THESE DE DOCTORAT DE L'ETABLISSEMENT UNIVERSITE BOURGOGNE FRANCHE-COMTE

PREPAREE A Universite de Bourgogne

Ecole doctorale n°85937

Sciences Pour l'Ingénieur et Microtechniques

Doctorat en Informatique

Par

JALEW Esubalew Alemneh

Fog Computing based Traffic Safety for Connected Vulnerable Road Users

Thèse présentée et soutenue **au laboratoire DRIVE à Nevers**, le **25 Octobre 2019**

Composition du Jury :

Rami Langar	Professeur, Université Paris-Est Marne-la-Vallée, Marne-la-Vallée, France	Rapporteur
Marcelo Dias de Amorim	Directeur de Recherche CNRS,Université Pierre et Marie Curie, aris, France	Rapporteur
Lynda Mokdad	Professeur, Université de Paris 12, France	Examinateur
Khaled Boussetta	Professeur, Maitre de conférences HDR, Université de Paris 13, Villetaneuse, France	Examinateur
Sidi Mohammed Senouci	Directeur de thèse, Professeur, Université de Bourgogne, Nevers, France	Directeur de thèse
Tesfa Tegegne	Directeur du centre de recherche ICT4DA, Université Bahir Dar, Éthiopie	Codirecteur de thèse
Philippe Brunet	Maitre de conférences (MCF), Université de Bourgogne, Nevers, France	Encadrant
Laurent Mussot	R & D Engineer, Orange Labs, Chatillon	(Invited)

Title: Fog Computing-based Traffic Safety for Connected Vulnerable Road Users

Keywords: Traffic safety, Vulnerable road users, Fog computing, Position accuracy and sampling rate, Energy efficiency, Trust management and Security

Abstract: Annually, millions of people die and many more sustain non-fatal injuries because of road traffic accidents. Despite multitude of countermeasures, the number of the causalities and disabilities are increasing each year causing grinding social, economic, and health problems. Due to their high volume and lack of protective-shells, more than half of road traffic deaths are imputed to vulnerable road users (VRUs) that include pedestrians, cyclists and motorcyclists. Mobile devices combined with fog computing can provide short-term feasible solutions to protect VRUs by predicting collusions and warning users of an imminent traffic accident. Mobile devices' ubiquity and high computational capabilities make the devices an important components of traffic safety solutions. Fog computing has features that suits to traffic safety applications as it is an extension of cloud computing that brings down computing, storage, and network services to the proximity of the end users. Therefore, in this thesis, we propose an infrastructure-less traffic safety architecture (PV-Alert) that depends only on VRUs' and drivers' mobile devices besides the fog computing concept. The mobile devices are responsible to extract their position and other related data and to send cooperative awareness messages to a nearby fog server. The fog server estimates collision using a collision prediction algorithm and sends an alert message, if an about-to-occur collision is predicted. Evaluation results shows that the proposed architecture is able to render alerts in real-time and outperforms other related road safety architectures in terms of reliability, scalability and latency.

However, before deploying this architecture, the challenges pertaining to weaknesses of its important ingredients should be treated prudently. The first challenge is related to the positions read by mobile devices, which are not accurate and do not meet the maximum position sampling rate of traffic safety applications. Moreover, continuous and high rate position sampling drains mobile devices battery quickly. From fog computing's point of view, it confronts a new challenge related to privacy and security in addition to those assumed from cloud computing. For the aforementioned challenges, we have proposed new solutions: (i) To improve GPS accuracy, we have proposed an efficient and effective two-stage map matching algorithm. In the first stage, GPS readings obtained from smartphones are passed through Kalman filter to smooth outlier readings. In the second stage, the smoothed positions are mapped to road segments using online time warping algorithm. (ii) position sampling frequency requirement is fulfilled by an energy-efficient location prediction system that fuses GPS and inertial sensors' data. (iii) For energy efficiency, we proposed an energy efficient fuzzy logic-based adaptive beaconing rate management that ensures safety of VRUs. (iv) finally, privacy and security issues are addressed indirectly using a trust management system. The two-way subjective logic-based trust management system enables fog clients to evaluate the trust level of fog servers before awarding the service and allows the servers to check out the trustworthiness of the service demanders. We have therefore been able to show in this thesis that the use of ubiquitous mobile devices combined with the Fog Computing concept has great potential to improve road safety and more specifically to reduce the excessive number of road accidents involving vulnerable road users.

Titre : Assurer la sécurité des usagers vulnérables de la route connectés grâce à leur Smartphones et au concept de *Fog Computing*

Mots clés : sécurité routière, usagers vulnérables de la route, *fog computing*, précision de position géographique et taux d'échantillonnage, efficacité énergétique, gestion de confiance et sécurité

Résumé : Chaque année, des millions de personnes meurent et beaucoup d'autres subissent des séquelles graves à la suite d'accidents de la route. Malgré une multitude d'initiatives, le nombre de cas mortels et d'accidents graves augmente chaque année en engendrant des problèmes préoccupants à la fois sociaux, économiques et sanitaires. En raison de leur nombre élevé et de l'absence de protection personnelle, plus de la moitié de ces décès concerne les usagers vulnérables (en anglais, *vulnerable road users* - VRU) regroupant les piétons, cyclistes et motocyclistes. Les appareils mobiles, combinés à la technologie de *Fog Computing (ou informatique géodistribuée, ou même informatique en brouillard)*, représentent une solution réaliste à court terme pour les protéger en les avertissant de l'imminence d'un accident de circulation. L'omniprésence des appareils mobiles et leurs capacités de calcul élevées font de ces appareils un élément important à considérer dans les solutions de sécurité routière. Le *Fog Computing* offre des fonctionnalités adaptées aux applications de sécurité routière, puisqu'il s'agit d'une extension du *Cloud Computing* permettant de rapprocher les services informatiques, le stockage et le réseau au plus près des utilisateurs finaux. Par conséquent, dans cette thèse, nous proposons une architecture réseau sans infrastructure supplémentaire (*PV-Alert*) pour des fins de sécurité routière et reposant uniquement sur les appareils mobiles des VRU et des conducteurs sur la route avec l'aide du concept de *Fog Computing*. Les données géographiques et cinématiques de ces appareils sont collectées et envoyées périodiquement au serveur *fog* situé à proximité. Le serveur *fog* traite ces données en exécutant un algorithme de calcul de risque d'accident de circulation et renvoie des notifications en cas d'accident imminent. L'évaluation de cette architecture montre qu'elle est capable de générer des alertes en temps réel et qu'elle est plus performante que d'autres architectures en termes de fiabilité, d'évolutivité et de latence.

Chaque année, des millions de personnes meurent et beaucoup d'autres subissent des séquelles graves à la suite d'accidents de la route. Malgré une multitude d'initiatives, le nombre de cas mortels et d'accidents graves augmente chaque année en engendrant des problèmes préoccupants à la fois sociaux, économiques et sanitaires. En raison de leur nombre élevé et de l'absence de protection personnelle, plus de la moitié de ces décès concerne les usagers vulnérables (en anglais, *vulnerable road users* - VRU) regroupant les piétons, cyclistes et motocyclistes. Les appareils mobiles, combinés à la technologie de *Fog Computing (ou informatique géodistribuée, ou même informatique en brouillard)*, représentent une solution réaliste à court terme pour les protéger en les avertissant de l'imminence d'un accident de circulation. L'omniprésence des appareils mobiles et leurs capacités de calcul élevées font de ces appareils un élément important à considérer dans les solutions de sécurité routière. Le *Fog Computing* offre des fonctionnalités adaptées aux applications de sécurité routière, puisqu'il s'agit d'une extension du *Cloud Computing* permettant de rapprocher les services informatiques, le stockage et le réseau au plus près des utilisateurs finaux. Par conséquent, dans cette thèse, nous proposons une architecture réseau sans infrastructure supplémentaire (*PV-Alert*) pour des fins de sécurité routière et reposant uniquement sur les appareils mobiles des VRU et des conducteurs sur la route avec l'aide du concept de *Fog Computing*. Les données géographiques et cinématiques de ces appareils sont collectées et envoyées périodiquement au serveur *fog* situé à proximité. Le serveur *fog* traite ces données en exécutant un algorithme de calcul de risque d'accident de circulation et renvoie des notifications en cas d'accident imminent. L'évaluation de cette architecture montre qu'elle est capable de générer des alertes en temps réel et qu'elle est plus performante que d'autres architectures en termes de fiabilité, d'évolutivité et de latence.

UBFC UNIVERSITE BOURGOGNE FRANCHE-COMTE

Université Bourgogne Franche-Comté
32, avenue de l'Observatoire
25000 Besançon

ACKNOWLEDGMENT

Throughout my PhD study I have received a great deal of support and assistance. First and foremost, I would like to express my profound gratitude to Professor Sidi-Mohammed SENOUCI, for his permanent support, scientific guidance, patience, constant optimism, enthusiasm and sympathy all over this long walk. My research would have been impossible without his invaluable encouragements as well as careful and well-timed feedbacks. Thank you, Prof!

I am grateful to my co-supervisor Dr. Philippe Brunet for his guidance and supervision that helped me to produce quality research outputs. I am very glad and thankful for having met and worked with Dr. Philippe. I am also grateful to my local co-supervisor Dr. Tesfa Tegegne from Bahir Dar university for his valuable supervision. Moreover, I am grateful to Dr. Mohamed-Ayoub MESSOUS for his guidance and support on part of my research works.

I would further like to thank all the jury members, Rami Langar, Marcelo Dias de Amorim, Lynda Mokdad, Khaled Boussetta and Laurent Mussot, for their participation in my PhD defense and for their kind and motivating comments.

My deepest thanks to my friends and colleagues, all teams of DRIVE Laboratory and all employees of ISAT especially Martine AIMÉ, Corinne GRALHIEN, Dr. El-Hassane AGLZIM and Regis for their unreserved and kind supports despite the language barrier.

I thank Ministry of Education of Federal Democratic Republic of Ethiopia, embassy of France in Addis Abeba and Campus France for sponsoring my study.

I wish to express my love and my gratitude to my family and friends back home for their appreciated support, and encouragement. Especially, I profoundly thank my father for his unfailing emotional support and for his constant source of inspiration. I am also deeply thankful to Sileshi and Gideon for helping in proofreading this dissertation.

Last but for sure not least, I would like to thank my soul mate, my dearest wife and devoted mother, Birtukan, for understanding and for standing with me throughout the toughest moments of my life. Her countless sacrifice, extreme support, never-ending patience, and inspiration was in the end what made this dissertation possible. Moreover, I would like to thank her for taking such good care of our children.

Finally, I would like to dedicate this work to my lovely two children, Bisrat and Fanuta, who are the pride and joy of my life. I can see from our phone conversation how much you both miss me when I am away for the study and your dad misses you more. I love you more than anything and I appreciate all your patience.

TABLE OF CONTENT

1

INTRODUCTION

1.1/ CONTEXT AND MOTIVATION

Road traffic injuries are reasons for many deaths globally. According to World Health Organization's 2015 Global status report on road safety, 1.2 million people die because of road traffic injuries each year [1]. As it is shown in the subsequent reports of the organization, this number has kept increasing each year. For example, the 2018's report of the organization shows that the number of traffic injury deaths has elevated to 1.35 million [2]. Based on the global road safety status reports, traffic injury is the leading cause of death in children and adults under 30 years causing grinding social, economic and health problems. Due to their high volumes and negligence of road traffic designs, vulnerable road users (VRUs) which could be pedestrians, cyclists and Powered Two-Wheelers (PTWs) accounts for more than half of the fatalities. Over the past few decades, the rate of traffic accidents and fatalities has gone down considerably, but the decrease in traffic accident injuries for VRUs is low [1], [2], [3]. Due to the lack of protective "shells" or safety features, pedestrians are more vulnerable to traffic accidents than other groups of VRUs. These accidents often result in severe injuries if not deaths. For instance, it has been estimated that pedestrians are 284 times more likely to be killed or injured in a traffic collision than motorists [4].

Root causes of high traffic accidents include poor safety standards, lack of law enforcement, rapid urbanization, driving under the influence of alcohol and drugs, failure to wear seat-belts and helmets as well as people driving fatigued [2]. Moreover, the increasing use of mobile phones and other portable devices globally has become a new cause of traffic accidents nowadays because of many types of distractions they brought [5], [6], [7]. Drivers and VRUs use their phones for talking, texting, and listening to music while driving and walking. This results in an inattention which eventually becomes the reason for many traffic accidents [8], [9]. Traffic accident injuries and fatalities have an immense impact on the physical, mental, and health issues of individuals as well as financial and social consequences for individuals and their families [10]. At the national level, economic developments of low- and middle-income countries is being hampered by traffic accidents. It cost governments approximately 3% of their Gross Domestic Product (GDP) [1].

Various accident protection mechanisms have been applied to minimize traffic accidents. Increasing visibility of roads and planning bumpers to reduce their speed are among passive measures for VRUs traffic accident reduction. Automatic braking is no more limited to luxury cars. Many contemporary vehicles are fitted with this feature for mitigation of forward-collisions. Moreover, passive measures like educating traffic safety and setting strict law enforcement are also among the most crucial VRU traffic accident prevention mechanisms. In recent days, active traffic accident protection steps that involve road user detection, collision prediction, alerting and collision avoidance have got a lot of attention. However, the problem is still apparent, and traffic accidents have continued to be reasons for deaths of many people. Those who didn't die of traffic accidents suffer permanent physical and mental consequences, among others.

1.2/ OPPORTUNITIES AND CHALLENGES

Omnipresent mobile devices can help to avoid traffic accidents on VRUs instead of becoming sources of road traffic injuries. The number of smartphones is increasing at a very high rate. It is predicted that the number of the handheld device users will clinch to 2.87 billion in 2020 [11], [12]. Because of affordable prices, versatile services, and high computation, storage, and communication capacity smartphones are owned by many road users including drivers. The staggering increase in their capability is further enhanced by their sensing potential, which is another feature that makes the devices more intelligent and essential part of everyday life. Though the number of sensors may vary from one smartphone to the other, typical smartphone contains accelerometer, a digital compass, a gyroscope, a GPS, quad microphones, dual cameras, near-field communication, a barometer, light, proximity, and temperature sensors [13]. Therefore, mobile devices combined with fog computing, which is a computing paradigm suitable for latency-sensitive applications, can provide feasible solutions to protect VRUs by predicting collusions and warning them of an imminent traffic accident in real-time.

Fog computing is an extension of cloud computing that brings down computing, storage, and network services to the proximity of users' arena with the objective of reduction of latency. It is a decentralized computing infrastructure with the following defining characteristics: low latency, location awareness, wide-spread geographical distribution, mobility support, existence of very large number of nodes, heterogeneity and predominance role of wireless access [14]. The attractive properties of fog computing make it an ideal technology for Intelligent Transportation Systems (ITS) and other applications that require real-time responses.

Pulling characteristics of fog computing and an increase in number as well as in the capacity of mobile devices pave a way to create novel active road safety applications. The main roles of mobile devices in active traffic safety measures that conglomerate mobile devices and fog computing are: (i)

extracting position including the direction of movement and speed of drivers and VRUs, (ii) sending Cooperative Awareness Message (CAM) to a nearby fog server, and (iii) receiving a warning message sent from the fog server. VRUs are connected to fog servers using a wireless communication that could be either Wi-Fi or Long-Term Evolution (LTE) connection. When a fog server receives the data, it estimates collisions using collision prediction algorithm. If an about-to-occur collision is predicted, the fog server sends a Decentralized Environmental Notification Message (DENM) to both VRUs and drivers. Cloud servers may also be involved in the solution to store the data which is no more important for the real-time traffic accident prediction. The data is helpful for farther traffic analysis.

The interplay between fog nodes and smartphones will prevent traffic accidents that might happen otherwise. However, before actualizing such remedies, challenges that are associated with smartphones and fog computing need immediate attentions. The most important ones are briefed below:

- *GPS Position Inaccuracy* – GPS positions sent to fog servers to predict collisions must be as accurate as possible. Minor GPS inaccuracy may result in an inaccurate or incorrect prediction. Incorrect predictions in their turn will most probably become reasons for traffic injuries. According to [15] longitudinal and latitudinal inaccuracy of GPS positions read by mobile devices is more than 4m. Because of their small size, smartphones contain miniature GPS chipsets which have limited capability to get accurate GPS fixes. The problem is worsened by subjection of the devices to non-ideal environments that compromise sensor accuracy and reliability. Noise, interferences, weather conditions, obstructions of satellite signals by big buildings and trees are among factors that contribute to the degradation of the accuracy of positions read by smartphones. Thus, it is mandatory to smooth GPS readings obtained from smartphones and improve the accuracy of locations to precisely predict and eventually avoid traffic accidents.

- *Insufficient Position Sampling Frequency* – European Telecommunication Standard Institute (ETSI) standardized time intervals of CAM generations for collision risk notifications systems. If a VRU is in the less risky region, the CAM can be sent every 1s but if the VRU is in high-risk region, 10 beacons need to be sent to a fog server every second. This implies GPS fixes have to be read in the interval of 0.1s to 1s. However, investigations made by [16] depict that smartphones can't support such high rate location sampling demand of traffic safety applications. In addition to the factors that affect GPS accuracy, the position sampling frequency of smartphones is affected by factors ranging from location method used to the hardware make of the mobile phone and operating system installed. The promises of using mobile device for traffic safety applications can only be materialized if they are able to meet the application's position sampling rate requirement.

- *High Energy Consumption* - not only smartphones have limited battery capacity due to their size and

weight constraints but also, they are among the most energy-hungry devices due to the number of services they support. High GPS sampling demands of traffic safety applications intensify the energy desire of mobile devices. Based on the experiment conducted in [17], a smartphone battery that could last for 95 hours with normal use is depleted in only 11 hours when the device is used to run traffic safety application. Mobile devices of drivers can get continuous power supply from the vehicles, but this is not true for handheld devices owned by VRUs. Therefore, the high energy consumption of smartphones is one of the hinderance to use the mobile devices for traffic safety applications.

- *Privacy and Security in Fog Computing* - fog computing comes with plenty of striking features. However, it is not a panacea. It faces new privacy and security challenges besides those inherited from cloud computing. The challenges are attributed to its distributed architecture and flexibility of deployment [18], [19]. Fog servers can be accessed easily by adversaries due to their geo-distributiveness and proximity to end users. Fog nodes can join or leave fog environment at any time, and they are usually from different manufacturers. Fog nodes are usually donated or rented by individuals, and fog networks are operated and maintained by different providers or individuals independently. These all leave security and privacy holes in the system. Imposing security mechanisms in fog computing is challenging, just like other distributed environments. Traditional security mechanisms like authentication and access control can't be applied readily due to the absence of universally unifying entity. Privacy and security issues in fog computing are one of the issues that need measures to increase the acceptability of the computing paradigm for traffic safety applications.

- *Offloading Trajectory Data among Fog Nodes* – road users and vehicles are mobile over many fog servers' coverage areas. Therefore, as the VRUs move from one fog node coverage area to another, their historical trajectories have to be passed for better accuracy of traffic accident estimations. Moreover, there may be a need to move some road users' position data to nearby fog nodes to distribute loads among fog nodes.

Unless the challenges pointed out above are addressed, it is less likely to get the full advantages of fog computing-based traffic safety applications that rely on mobile devices.

1.3/ THESIS OUTLINE AND CONTRIBUTIONS

As indicated in Figure 1.1, this thesis is structured into six main chapters, excluding introduction and conclusion chapters. The chapters can be organized into two groups. The first group, which comprises of chapter 2 and chapter 3, involves reviews of up-to-dated related works to traffic safety measures for

VRUs and proposition of an infrastructure-less collision prediction solution that employs smartphones and the emerging fog computing paradigm. Before deploying the architecture in real environments, challenges that affect the service provided by the architecture have to be addressed: mobile devices GPS fixes accuracy, high energy consumption, insufficient application sampling period, as well as privacy and security issues in relation to fog computing. The second group, which contains the remaining chapters from chapter 4 to chapter 7, deals with the solutions proposed to the challenges pertaining to mobile devices and fog computing. The summaries of contributions of the chapters are discussed below.

Chapter 2 - Background and State of the Art - this chapter presents the survey made on the context of this thesis's topics. Traffic accident problems and the most prominent solutions are discussed. Three main topics are included in the chapter. Contemporary passive and active road traffic safety solutions are discussed, in the second part, next to a section that introduces the chapter. Opportunities and challenges of connecting vulnerable road users to vehicles using their mobile devices to safeguard them from traffic accidents are explained in the third part. The last section is dedicated to fog computing, and its challenges and potential applications for road traffic safety solutions.

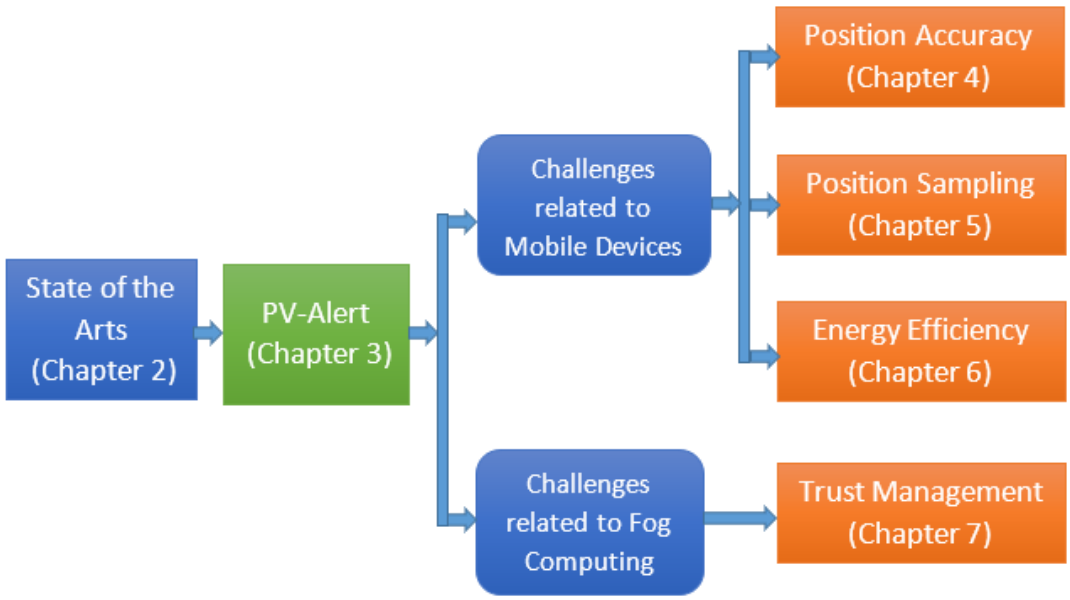


Figure 1.1: Organization of the Thesis

Chapter 3 - PV-Alert: A Fog Computing based Architecture for Safeguarding Connected Vulnerable Road Users - the first contribution of this thesis is traffic safety architecture to protect VRUs. The architecture is presented in this chapter. The two main components of the architecture that we have named PV-Alert are fog computing environment and mobile devices owned by VRUs and drivers. The devices are connected to fog servers with wireless connection media like Wi-Fi or LTE.

Fog servers are in charge of running VRU collision detection algorithms from the geolocation and other related information sent from mobile devices of connected VRUs and drivers. The servers also send alert messages to both drivers and VRUs if there is any anticipated accident. The analytical and empirical performance comparisons of the architecture to other mobile device-based traffic safety architectures are presented along with the criteria we have defined. Finally, experimental evaluation of the architecture is discussed.

Chapter 4 - PV-Alert: Meeting Position Accuracy Requirement – before deploying PV-Alert in a real environment, challenges related to the main components of the architecture have to be addressed. This chapter deals with one of the challenges pertaining to mobile devices. GPS positions accuracy of mobile devices remains insufficient for a lot of location-based applications, especially traffic safety ones. After reviewing related works, an experiment made to check the GPS accuracy of the current smartphones is given. Next, a new algorithm which is able to improve smartphones GPS accuracy for vulnerable road users' traffic safety to alleviate the problem is conferred. The solution is a two-stage algorithm in which GPS readings obtained from smartphones are passed through Kalman filter to smooth deviated reading, in the first stage. In the second stage, an adaptive online time warping based map matching algorithm is applied to map the improved new locations to corresponding road segments. The incremental alignment is made in a real time based on two similarity metrics: distance and direction difference. Then, the comparison made to different online time warping variants with the naïve dynamic time warping algorithm in terms of accuracy and response time is discussed. GPS trajectories collected from smartphones and reference points extracted from road network data are used for the evaluation.

Chapter 5 - PV-Alert: Meeting High Position Sampling Requirement – the solution proposed to meet high position sampling demand of mobile devices is discussed here. Traffic safety applications demand very high position sampling to safeguard VRUs - that is CAM has to be sent to fog server every 0.1s if the VRU is in high traffic risk regions. The investigation conducted to verify if different location methods of current mobile devices meet the maximum sampling rate of requirement is presented. Next, an energy efficient position prediction method that fuses GPS and Inertial Navigation Systems (INS) sensors data to estimate pedestrians' positions at a high rate is provided. INS based dead reckoning is performed to extrapolate positions from last known location when GPS reading is unavailable. When GPS fix is realized, the reading is used to correct dead reckoning parameters in addition to serving as the location fix. Finally, discussions are made on the evaluation results of the proposed algorithm and energy efficiency of different GPS and INS data sampling rates and conclusions are drawn.

Chapter 6 - PV-Alert: Achieving Energy-Efficiency by Adapting Beaconing Rate – discusses a measure taken to tackle high energy demand of mobile devices while using them for traffic safety applications. High beaconing rate of location and other associated data from mobile devices to fog

servers drain mobile devices' energy rapidly. A fuzzy logic-based adaptive beaconing rate management that ensures the safety of pedestrians from traffic accidents while minimizing the energy consumption of the mobile devices is discussed in this chapter. It also explains evaluations made on risk prediction accuracy of the fuzzy logic-based system, which is conducted by comparing its output with the risk level prediction algorithm that relies on minimum distance for information exchange to predict the likelihood of accidents. Then, the energy efficiency evaluation of the adaptive beaconing rate management is presented.

Chapter 7 - PV-Alert: Trust Management – in this chapter, a challenge on PV-Alert which is inherited from fog computing is discoursed. Some of its features and flexibility of deployments make fog computing susceptible to security and privacy attacks. The two-way subjective logic-based trust management system that solves information security and user privacy is covered. Topics related to trust management like trust metrics, and trust-based attacks and their proposed solutions are also discussed. Finally, the performance evaluation of the solution proposed and comparative analysis made are presented, and conclusions are given.

Chapter 8 - Conclusions and Perspectives - this chapter presents the conclusion, discusses the research and practical implications of the thesis and outlines the potential future research directions related to the use of mobile devices and fog computing to improve traffic safety.

2

BACKGROUND AND STATES OF THE ART

2.1/ INTRODUCTION

A road traffic accident is defined as an event, such as a car crash or collision, which occurs on the road and results in death or personal injury or property damage in direct relation to the operation of a vehicle in motion [10]. Every day more than 3,700 people or one person every 25 seconds die because of road traffic accidents [2]. Road traffic injuries recently have become the eighth cause of death worldwide. The injuries and disabilities induced by traffic accidents annually are tallied by tens of millions, and this number is increasing year by year. Even though low and middle-income countries have a low ratio of vehicles per inhabitants, they suffer most of the traffic accidents due to lack of infrastructures, poor enforcement of traffic safety regulations, poor access to health services, etc. Even in the European Union which has some of the safest roads in the world, traffic accidents claim over 25,000 lives every year, and many more are seriously injured [20]. VRUs account most of the traffic accidents figures mentioned. According to European Commission's ITS directive, VRU represents non-motorized road users, such as pedestrians, cyclists, motor-cyclists and persons with disabilities or reduced mobility and orientation (ability to know where one is and where he wants to go). Generally, road users who have a high fatality percentage and are supposed to be given special consideration in road safety policies are stated as VRUs.

Road traffic accidents induce health, economical and societal impacts to direct participants of the accidents as well as their families and the country at large. Road users who survive traffic accidents sustain long-lasting mental and physical health problems. Moreover, after road traffic accident injuries, overall quality of life of individuals is significantly reduced in comparison with the general population norm [21]. Quality of life is the standard of health, comfort, and happiness experienced by an individual or a group in relation to their goals, expectations, standards and concerns. A recent report released by World Bank [22], has shown that many countries can achieve substantial long-term income gains by reducing road traffic deaths and injuries. The finding states that national income growth can be boosted by plummeting road traffic injuries. This is an acceptable conclusion since road traffic injuries cost about 3% of most countries' GDP.

Speeding, drinking and driving, taking psychoactive substances and driving, nonuse or incorrect use of helmets, seat-belts, and child restraints, and distraction are the main cause for road traffic injuries. High speed of vehicles is the reason for the majority of traffic accident deaths. Based on [2], a 1% increase in average speed increases fatal crash risk by 4%. That is why France has introduced a reform on a speed limit that reduced from 90km/h to 80km/h on all two-lane highways [23]. An increased blood alcohol concentration increases traffic accident rates. Hence, drinking and driving is banned by many countries in the world. Though wearing helmets have proved advantages to reduce the risk of death and severe injuries, only a few countries have drafted motorcycle helmet laws. According to [24], distracted driving is the most common cause of road accidents in the United States. While distraction of drives may be caused by various reasons, talking on a cell phone and texting messages are the most common ones. Besides drivers, mobile devices-based distraction profoundly reduces VRUs safety, especially pedestrians [8]. Mismanaged over-usage of mobile devices puts pedestrians in the risk of road traffic accidents.

To address the problems mentioned above, many active and passive safety systems are proposed. Mobile devices are becoming important components of many active safety solutions. In fact, mobile devices bring both opportunities and challenges with them. As stated earlier, one of the challenges associated with the devices is the distraction of both drivers, pedestrians and other road users, making them the cause of many road traffic accidents. However, this challenge could be avoided by integrating the devices in traffic safety systems. Therefore, we argue that the wide existence of mobile devices coalesced with their increased computing, storage, network, and sensing capabilities make them good candidates to many applications including traffic safety ones. Stringent latency requirements of traffic safety applications can be dealt with using a new computing paradigm that brings cloud capabilities down to the ground close to end users. This paradigm is called fog computing and it has advantages like low latency, location awareness, and improved quality of services for real-time applications [14]. Traffic safety applications can use mobile devices to perceive VRUs' and drivers' environment using their onboard sensors, to report these data (e.g. position for road safety applications) to a fog server, and to receive feedbacks (e.g. alert message) when the fog server predicts an imminent collision.

The rest of this chapter is organized as follows. In section 2.2, we review state-of-the-art passive and active road safety measures that are proposed to minimize traffic accidents. Requirements of VRU devices that connect VRUs, either directly or indirectly, to vehicles are discussed in section 2.3. The emerging computing paradigm, fog computing, whose characteristics make it suitable for traffic safety applications is presented in section 2.4. In the last two sections summary and conclusion are provided.

2.2/ ROAD SAFETY MEASURES

Albeit road traffic accidents are both predictable and preventable, they are daily events [25], [26]. People make mistakes that result in crashes, and human beings' body has a limited physical capability to endure the crash forces. Hence, millions of lives are lost yearly. Many countermeasures have been taken to reduce road traffic accidents. The importance of inclusion of road safety and viable transport targets in the sustainable development goals are well understood by many countries [26]. Furthermore, seeing the current impact of road accidents on public health, organizations like United Nations has taken several initiatives. The Decade of Action for Road Safety 2011–2020 [27] is one of such efforts that have created extensive activities around all over the world. Some of the intervention as stated in [27] are: effective speed management by police and through the use of traffic-calming measures, improving the safety features of vehicles, promoting public transport, setting and enforcing laws requiring the use of seat-belts, helmets and child restraints, setting and enforcing blood alcohol concentration limits for drivers, and improving post-crash care for victims of road crashes.

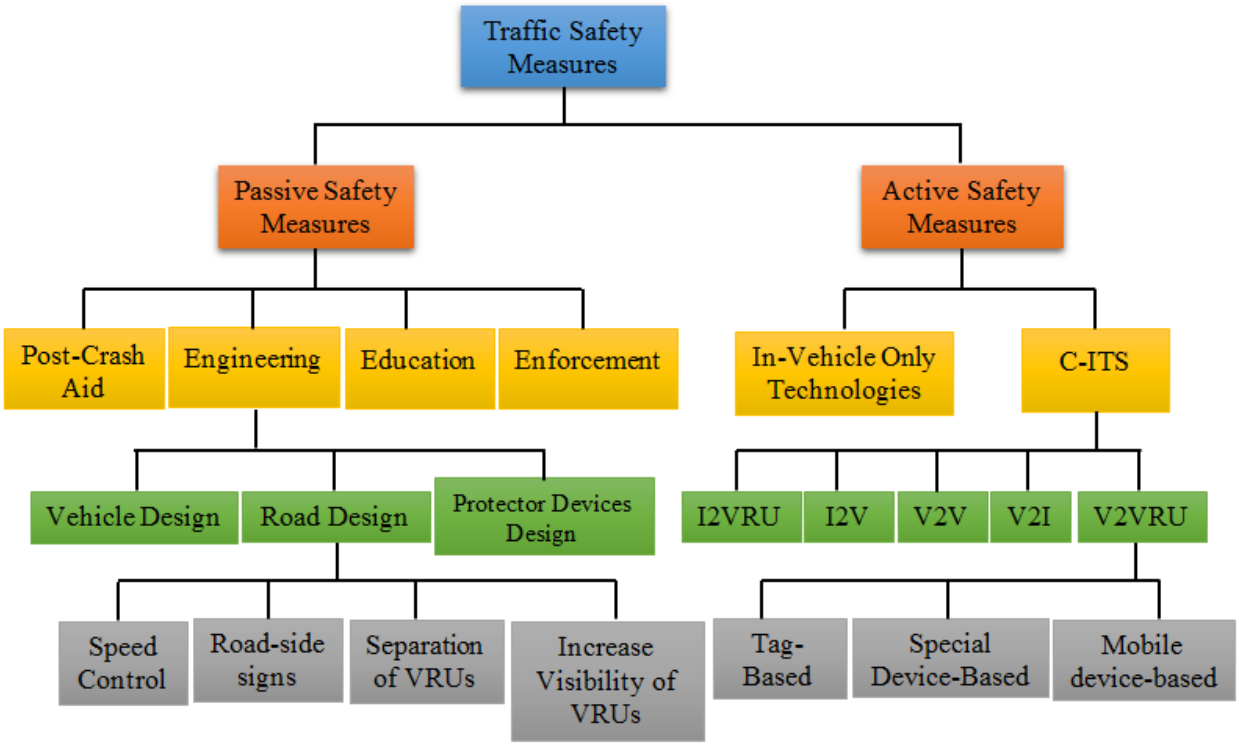


Figure 2.1: Traffic safety measures

Despite the various attempts to improve road safety, traffic accidents remain one of the main causes of premature deaths and injuries, especially for VRUs. In fact, many reports have shown that on average, 73% of people killed on city streets are unprotected road users like pedestrians, cyclists and

motorcyclists [2], [28]. This figure is not surprising since VRUs account for most of the traffic in high-density cities. Therefore, taking measures to reduce road traffic deaths is imperative.

As depicted in Figure 2.1, road safety measures are often categorized broadly into two as passive, and active. Details of the road safety measures focusing on VRUs are discussed in the upcoming subsections.

2.2.1. PASSIVE SAFETY SYSTEMS

Passive safety systems are used to minimize the impact caused on occupants at the time of the accident. They are not put into action before the occurrence of the accident. However, during the accident or time of impact, they become active to minimize or avoid the risk of injury on road users. Many crucial factors affect the severity of VRU's crash in traffic accidents. Vehicle design, its frontal aggressiveness, road and pavement layout, legislation like speed limitations, bicyclist's helmet are some of the examples [29]. Passive safety measures include wearing seat belts, the inclusion of air-bags in a vehicle, improving the design of vehicles to reduce impact, etc. Moreover, passive safety measures also include pre-crash preventive actions and post-crash aids to rescue road users [30]. As illustrated in Figure 2.1, passive safety systems can be further categorized into four classes: engineering, education, law enforcement, and post-crash aid [30], [31]. In the following paragraphs, we describe these four classes of passive safety measures.

The vast majority of passive safety systems are part of engineering, which involves vehicles design, roads design, and design of protector devices that shield road users from accidents. The objective of vehicle design is to minimize road traffic injuries to the lowest possible state. For example, to protect VRUs, vehicles' front- end geometry needs to be designed by taking the parameters that reduce the crash effect [32], [33]. Automotive crash boxes should be developed from lightweight materials such as aluminum and composites to reduce the effect of a crash [34]. Automotive crash box is a component installed at the front end of a car to enhance safety features by absorbing crash energy. A serious brain injury that could have resulted from a hit by a vehicle's front bumper can be minimized by designing flexible car body [35].

Accident protector devices include, among others, airbags and seat belts to protect passengers, and helmets to protect cyclists and motor-cyclists [36]. Recently, vehicles with pedestrian airbags have been designed by Volvo [37] to take traffic safety to the next level. The external airbag which is mounted on the front end of a vehicle is designed to guard pedestrians in case of a forward impact with a car. Road design involves providing a separate path for VRUs, managing vehicle's speed using bumps and increasing visibility and conspicuity of VRUs [25]. On-road and road-side signs, as well as qwick kurb

(traffic channelization device), are other examples that should be included in road design to maximize road safety.

Education on safety awareness for all ages is another passive safety measure that reduces accidents by brings behavioral changes. It enables road users and drivers to know all traffic rules and to be disciplined while walking and driving. Law enforcement refers to penalize drivers and VRUs that violate traffic rules. It ensures the compliance of road users to laws, regulations, standards, and policies. Education and enforcement are closely linked measures. We have to first create awareness and understand the traffic rules to enforce traffic rules and regulations [38].

Even though all the above measures are engaged to avoid accidents, the accidents happen unfortunately. Once the accident encounters, what can be done is striving to save the lives of the crash victims. This passive safety is called post-crash aid. Post-crash aid is very time-sensitive: an injured person whose life could have been saved may die due to a short delay. The reason for dramatically higher fatality rates in low- and middle-income countries is a lack of well-developed and organized emergency care systems to treat severe injuries. According to [39], 500,000 road traffic fatalities could have been averted every year, if fatality rates of high-income countries from severe injury were the same as in low- and middle-income countries. To reduce deaths due to severe traffic injuries, organized and integrated pre-hospital and facility-based emergency care system have to be developed, training has to be provided to all frontline basic emergency care personnel, and promotion of community first responder training has to be made [26].

Passive safety systems have confirmed significant benefits to reduce VRUs injuries. However, passive safety methods are constrained by human intelligence (to thoroughly understand and apply trainings provided) and the laws of physics (strength of accident shields) in terms of their capability to reduce collision energy and thus injury level [40]. Moreover, most passive safety countermeasures are mostly irreversible (can't be used again) and hence are more costly. The reasons mentioned above and the advancement made in passive safety systems over the years have shifted ITS researcher's attention to active safety. The next subsection reviews state of the art works on active safety measures.

2.2.2. ACTIVE SAFETY SYSTEMS

The objective of active safety solutions is to prevent an accident from occurrence [30]. The solution stays active the entire mobility periods of road users. Active safety systems use sensors to detect and monitor the movement of the road users to trigger countermeasures that are able to avoid or mitigate collisions in case of a foreseen danger [41]. As illustrated in Figure 2.2, there are three stages in accident prevention process using active safety mechanisms: road users' detection, collision prediction, and road users' notification or intervening on behalf of drivers.

Figure 2.2: Stages of active safety process

Active safety measures can be generally classified into two classes: in-vehicle only technologies and Cooperative ITS (C-ITS) systems. In-vehicle technologies are installed only in the vehicle to automatically control the vehicle ahead of an accident. So, systems in the vehicle are in charge of predicting collisions and taking counter actions. Autonomous Emergency Braking (AEB) systems, evasive steering, intelligent speed adaptation and other automatic driver assistant systems are some examples of in-vehicle technologies. In [40] an active safety system that has the capability to decide, whether to perform automatic braking or evasive steering at relatively high vehicle speeds (up to 50 km/h) is proposed. The decision is taken in split of seconds. The evaluation made on the potential effectiveness of AEB in pedestrian protection in [41] has shown that such systems have high places in accidents detection and avoidance. Intelligent Speed Adaptation (ISA) is a viable measure since the speeding of vehicles is the leading cause of road accidents. ISA is defined in [42] as "*the generic name for advanced systems in which the vehicle knows the speed limit and is capable of using that information to give feedback to the driver or limit maximum speed*". ISA has a large probability to reduce accidents and the severity of collisions drastically. The problem with active safety systems that rely on technologies deployed in vehicles is that as most of the cars currently are not equipped with the solutions, it is not practical for application in the present day. In fact, most vehicles are not designed for such remedy. Furthermore, road user detection mechanisms rely on cameras, infrared, radar, and tags which are highly affected by Line of Sight (LOS) and environmental conditions.

C-ITS is an active safety measure that brings vehicles and other road users together to make interactions to eliminate or reduce road traffic accidents [43]. This paves a way to create brand-new approaches for ensuring road safety. The intention of C-ITS is to apply a technological revolution in traffic management systems. Communication in C-ITS could be made among vehicles, infrastructures and VRUs. Vehicle-to-Vehicle (V2V), Vehicles-to-Infrastructure (V2I), Vehicle-to-VRUs (V2VRU) which contains Vehicle-to-Pedestrian (V2P), and Infrastructure-to-VRU (I2VRU) communications are some examples of the interactions. C-ITS minimizes human role (human beings naturally make mistakes) in the process of traffic management and, accordingly, strengthens the level of road safety and transport efficiency of the road network [43]. Therefore, vehicles or road side infrastructures like Road Side Units (RSU) and central servers are responsible to detect, anticipate collisions, and warn road users. For instance, in an active safety system called Intersection Safety, RSU has the role to detect VRUs crossing or coming to an intersection via radar or camera, assessing the risk of an accident, and sending

an alert message of an imminent collision to nearby drivers and VRUs via wireless communication [44]. In this system, on-board unit of the vehicle informs a driver about an accident whereas VRUs are informed by the RSU via blinking lights. Suchlike safety mechanisms are not scalable since infrastructure-based safety techniques are very costly.

VRUs are incorporated into C-ITS relatively recently. In [45], the authors propose an architecture to integrate VRUs with C-ITS systems and discuss the requirements of VRU devices that connect them to the infrastructures. Moreover, they discussed challenges to meet technical requirements of VRU devices. The challenges explained includes sensor accuracy, power consumption, context sensitivity, channel congestion, privacy, and security of messages. The vitality of standardizing message exchanges between VRUs and other road users and infrastructures are also pointed out. More details on requirements VRU devices should possess are discussed in section 2.3.

Based on the type of VRU device, V2VRU active safety mechanism can be categorized into three classes: tag-based, special dedicated device based, and mobile device based. In tag-based systems, VRUs carry tags that communicate with vehicles (or possibly with road side infrastructures) through RFIDs, infrareds, harmonic radars, passive transponders, etc. Pedestrian detection and warning system called i-tag is introduced in [46] to reduce risk of collision between vehicle operators and pedestrian staff in workplaces. Some of the reasons for the collision are fatigue, non-compliance with safe operating procedures and poor visibility. The maximum detection capability of this device is 9m. In Ko-TAG system [47], VRUs carry a transponder which is a small wearable device, and cars transmit a coded radio signal. Based on radio signal propagation between the two, vehicle to VRU distance is estimated and a warning is sent accordingly. An RFID-based device with a standalone radio unit that interacts with intelligent bus stops is developed for children, in a research project named SafeWay2School [48]. Drivers of the buses are notified of VRUs in the proximity with flashing lights. Tag-based safety systems require VRUs to carry additional electronic devices though they already have mobile devices such as smartphones with various capabilities. Moreover, short coverage ranges of tag-based systems are not suitable for fast-moving traffic.

Dedicated VRU devices are suggested for cyclists [49] and motorcyclists [50], [51]. The two wheelers can be equipped with dedicated C-ITS devices which are activated only when motion is detected to transmit personal safety messages. The messages should contain position and context information, and it should be compliant with standardized in-vehicle and roadside C-ITS equipment.

Handheld devices owned by VRUs are the third group of apparatus to enable vehicles to VRUs interaction for traffic safety and other ITS applications. Due to their high computation capability and pervasiveness, mobile devices are the most acceptable and widely used VRU device. Smartphone based V2VRU C-ITS communication can be formed in two different ways [45]: (i) by transmitting signals

from handheld devices to a receiver in a vehicle periodically over Bluetooth Low Energy (BLE), Wi-Fi or cellular radio (ii) by transmitting location data to a car as CAM or as standard messages over Wi-Fi or cellular connections. Usually, in the first case, direct V2VRU communication is made without the involvement of any intermediate infrastructure. The receiver (a communication device) in the vehicle is in charge of localizing the VRUs. Direct mode of communication is suitable for traffic safety systems since it has very low communication latency. However, it has the following drawbacks [52]. Firstly, its range of communication is constrained by the type of the technology used. Secondly, it has deployment challenges as it requires the devices that participate in the communication be furnished with the same type of communication technology. Thirdly, resource constrained devices are responsible to process messages received from VRUs to spot the VRUs and to predict collisions.

To overcome the drawbacks of direct communication, many solutions that involve intermediate infrastructures to establish communication between vehicles and VRUs are proposed [53], [54], [55], [56]. In this scenario, a central processing unit takes information from VRUs and vehicles to monitor the movement of road users, and to predict an imminent accident. The advantages of indirect mode of communication over the direct mode are: (i) communicating devices can have different communication technologies, (ii) a central infrastructure usually have high processing power and can be a non-dedicated unit like cloud or fog server, and (iii) safety applications cover large geographical area using a multi-hop communication. However, transmitting messages to infrastructure nodes may introduce high communication latency. Traffic safety applications are highly latency-sensitive applications. Therefore, infrastructure systems that suit for low-latency applications need to be chosen. For instance, edge servers of a deployed edge computing environment can be used for traffic safety systems as the computing paradigm is avowed for delay-sensitive applications. In addition to infrastructures, mobile devices used as VRU devices need to be inspected. Accuracy of positions obtained from mobile devices as well as low-frequency position sampling and high energy consumption of the devices are among the challenges that need immediate attention. The following section goes in details with mobile devices as VRU devices for safety applications.

2.3/ CONNECTED VULNERABLE ROAD USERS' SAFETY

To avoid traffic accidents and possibly for other ITS applications, VRUs need to get connected to the infrastructure and/or vehicles. Here, the infrastructure which usually runs safety application can be a central server like cloud server or other edge servers, RSU, Traffic Management Center (TMC), etc. The well-studied concept of connected vehicles refers to connecting vehicles to other vehicles, networks, applications, and services. Vehicles are connected using the available/embedded devices in the vehicle and different communication technologies to improve vehicle safety and to improve vehicle efficiency

and commute times [57]. Analogically, connected VRUs are VRUs that are connected to vehicles directly or using an intermediate infrastructure to send position and other information that is used to predict and avert collisions. To create the connections, the VRUs use wireless communication technologies which are supported by their carried devices and infrastructure. Various communication technologies can be used in V2VRUs systems: cellular, Wi-Fi, and Bluetooth are some examples. VRU-carried devices such as dedicated devices, tags or mobile devices can be used as VRU devices. However, in recent traffic safety proposals, mobile devices are widely opted as VRU devices due to their omnipresence, and high computation, storage, communication and sensing capabilities. For instance, among 28 V2VRU systems investigated in a survey conducted in [52], 23 of them have used smartphones as a VRU device. An example of connected VRU is shown in Figure 2.3.

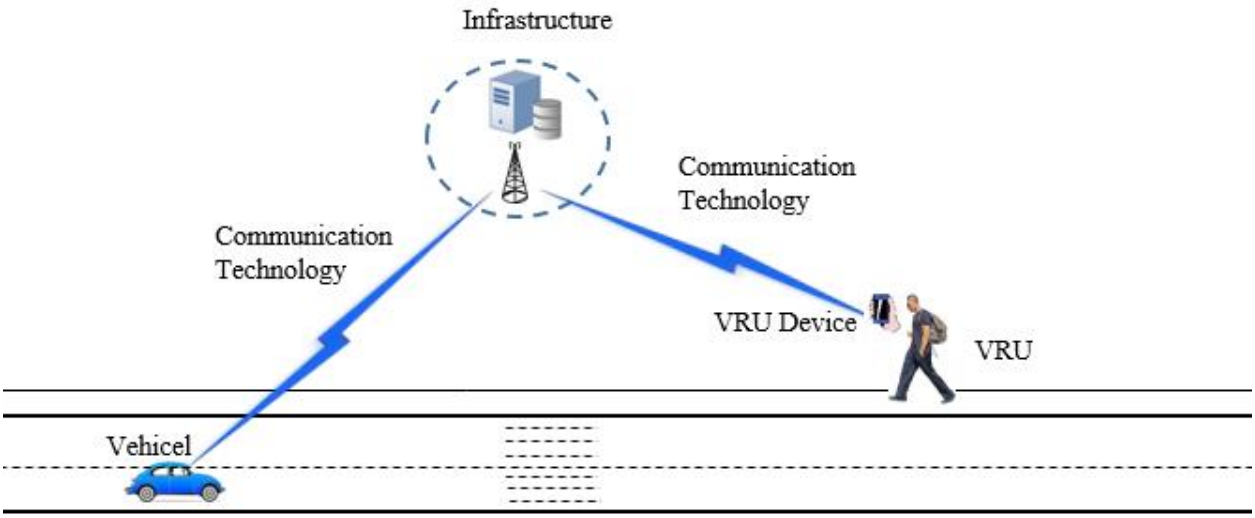


Figure 2.3: A connected VRU through an infrastructure

Creating a connection between vehicles and VRUs doesn't suffice to protect VRUs from traffic accidents. Safety critical systems demand strict requirements that can be attributed to VRU devices and the other components involved in the connection. In addition to computation, storage, and communication competencies, VRU devices need to extract accurate position at a very high sampling frequency. Their battery should also last long enough to provide the service continuously for the entire mobility period of the VRU. If collision prediction algorithms run on an infrastructure, the infrastructure should own a high computational capacity to execute VRU collision risk algorithm and send warning messages with the lower delay. This delay is also impacted by the used communication technology and the capacities of the VRU device. Communication technology also influences the range of communication. Other relevant requirements for traffic safety applications embrace reliability and scalability.

Mobile devices are recommended as VRU devices by many scholars for their wide existence and increased computing capacities. However, to keep the devices' involvement in traffic safety applications, their limitations that hinder meeting the requirements of such applications need to be addressed. Some important V2VRU requirements are summarized in Figure 2.4. Components of V2VRU communication that influence the requirements are also shown in the figure. In subsequent subsections of this section, we deliberate up-to-date efforts made to address each of the requirements.

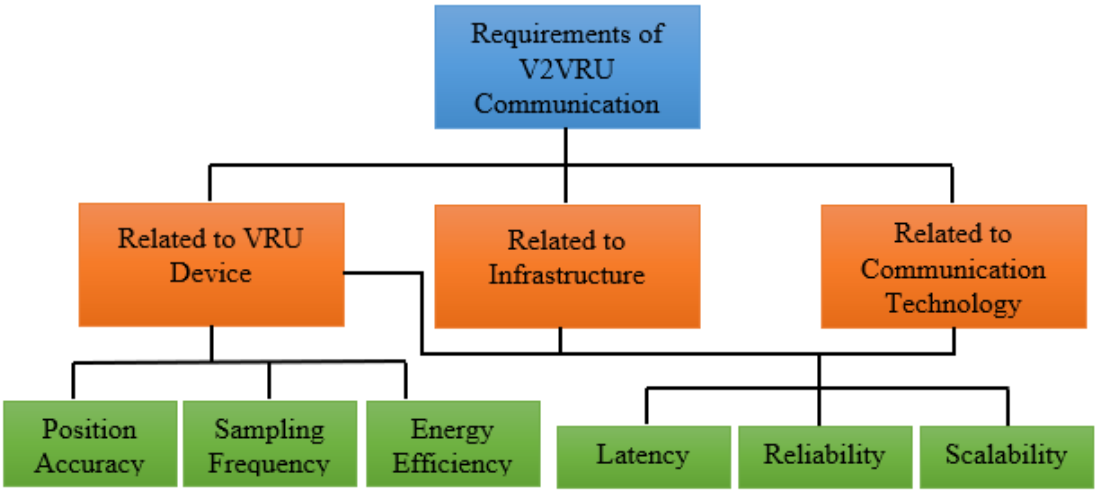


Figure 2.4: Some requirements of V2VRU communication for safety applications

2.3.1. POSITION ACCURACY REQUIREMENT

According to ETSI's technical specification which identified by *ETSI TS 101539–1*, vehicle traffic safety applications necessitate a position accuracy of 1m [58]. VRU safety applications should have at least 0.5m position accuracy to distinguish VRUs on roads and walkways [59]. Since small imprecision of the position may lead to wrong position prediction, which eventually results in a collision, various researches were conducted to improve the accuracy of the position read from VRU devices, especially smartphones. However, experiments have revealed that GPS accuracy of mobile devices is 10m for [60], 5m for [61], and 3m for [62]. In urban environments, the error may go as far as 40m [63]. The size of the devices, weather conditions, obstructions, noise, and interference are the main factors that contribute to the inaccuracy of GPS readings of mobile devices.

Various efforts from attaching external receivers like Global Navigation Satellite System (GNSS) on mobile devices [64] to the application of optimal estimators like Kalman filter [65] are suggested to improve the accuracy of smartphones. Although attaching external hardware to mobile devices may enable to achieve centimeter-level position accuracy, it hinders the mobility of the devices and makes the device inconvenient for handling. Software-based improvement techniques are unable to achieve position accuracies of even 3m in the handheld devices. According to [66], 1meter position accuracy can

be achieved by using data from the GLONASS and BeiDou satellites in addition to GPS. But still, this value does not meet safety applications position accuracy requirement.

2.3.2. POSITION SAMPLING REQUIREMENT

VRU collision prediction algorithms require VRUs' and vehicles' geographical data at a very high refresh rate to thwart VRU to vehicle conflicts. For instance, according to ETSI, the time interval between CAMs for collision risk warning systems must be between 100ms to 1s. This shows that the position sampled frequency needs to be 10Hz for VRU in high traffic risk area. However, experiments have shown that the maximum sample rate of modern mobile devices' GPS sensors is 1Hz whatever location methods of the mobile device are used [17], [67].

Position sampling frequency requirement can be achieved by integrating a GPS sensor and inertial sensor data. In [65], the authors demonstrate that the position sampling rate of a smartphone is able to be increased with the pedestrian dead reckoning algorithm that uses inertial and GPS sensor data. However, due to accumulated inertial sensor errors, the prediction accuracy decreases over a long prediction period making the system effective only for short-term predictions. Moreover, high-energy consumption of high-rate inertial sensor data sampling of mobile devices [67], [68] is not addressed.

2.3.3. ENERGY EFFICIENCY REQUIREMENT

Continuous position sampling and communication with a central infrastructure drain the battery of energy-constrained mobile devices quickly. To whatever degree smartphones position are accurate or the sampling rate is increased, unless the devices serve for long time periods, they will not be reliable means to protect VRUs from accidents. Many solutions proposed to save energy of smartphones involve adjusting sampling periods of the device, integrating auxiliary location methods, and performing adaptive communication to the vehicle through an infrastructure.

In [69], by using auxiliary location methods together with a GPS sensor, the authors show that up to 27% energy saving is achieved. According to [70], adaptive GPS sampling is able to reduce power consumption by 45%. A relaxed sampling of inertial sensors is able to reduce energy consumption by 22% in [68] and by 25% in [71]. According to [72], applying adaptive beaconing schemes based on the traffic risk level of pedestrian, introduced only 13% additional energy consumption in two simulation hours. In [73], an energy efficient communication scheme that relies on the grouping of VRUs based on their geographical locations to exchange safety messages between vehicles and mobile device owners is presented. The method involves establishing a Wi-Fi Direct communication among group members. An elected Peer-to-Peer (P2P) group owner acts on behalf of many P2P clients. It sends position and other information to a central server and propagates messages sent from the server to clients. Energy saving of smartphones can also be achieved by offloading computation to other devices. In [74], offloading

context information collected by smartphones to an edge server rather than executing in the devices is also used to increase the energy efficiency of the devices. A robust mobile device energy saving solution that works across all the processes from extracting positions to communication is vital.

2.3.4. COMMUNICATION TECHNOLOGIES

Many types of communication technologies can be used to connect VRUs to infrastructures and vehicles: 802.11p, Cellular, and Wi-Fi, being the most common ones. The type of technology used affects the range of communication and other characteristics like latency.

802.11p is a modification of the well-known IEEE 802.11 standard to include Wireless Access in Vehicular Environments (WAVE) for vehicular communication. It is the foundation for Dedicated Short-Range Communications (DSRC) protocol. DSRC is primarily designed for communication of vehicles in ITS with other vehicles or with infrastructures. Hence, its application in V2V communication is studied intensively. 802.11p is also root standard of ITS-5G. ITS-5G is a wireless short-range communication technology designed by ETSI to transport small data volumes at extremely high speed in V2V communications [75]. Even though 802.11p allows reliable, long-range (1km) and real-time exchange of safety information even at a very high vehicular mobility conditions, it doesn't come with VRU devices. [76] and [62] have shown that the technology can be integrated with smartphones, but mobile devices are yet to come with 802.11p. In [76], DSRC is conjugated with Wi-Fi Direct for vehicle to VRU communications. However, since DSRC is designed for vehicles and VRUs' movement dynamics, and crash situations are dissimilar from VRUs, the protocol needs modification. Even though current smartphones do not come with 802.11p, its features make the technology a promising contender for V2VRU communication in the future.

Bagheri et al. [53], suggested cellular networks for VRU safety applications since they have high mobility support, high bit-rate, long communication range as well as reduced user adoption costs and high market penetration time. [54], [72], and [77] have also proposed cellular technology for vehicles to road users' communications. LTE is undertaking standardization to support V2P functionalities as one part of the general Vehicle-to-Everything (V2X) schema [78]. Even though its attractive features make cellular technology convenient for V2VRU communication, the latency of the cellular networks humpers its suitability for VRU safety systems. However, the evolution of cellular technology to LTE and LTE Direct and further to 5G makes the technology a promising candidate for traffic safety applications [79].

Wi-Fi is the most experimented communication technology for V2VRU communications. In [65], smartphones are used to integrate VRUs into Car-to-Everything (Car2X) communication via WLAN 802.11 b/g. The applicability of Wi-Fi to create V2P communications for a pedestrian safety system is

studied by Anaya et al., [60]. Other works also have recommended Wi-Fi for VRU safety [79], [80], [81], [82], and [83]. Wi-Fi Direct has been proposed to exchange safety messages between vehicles and mobile devices of VRUs [73]. Wi-Fi Direct is a standard Wi-Fi which enables direct connection of devices with each other without requiring a wireless access point. Wi-Fi is a good candidate for VRU safety applications in urban environments due to its wide existence and its support for slow moving traffic. Some traffic safety proposals use both Wi-Fi and cellular technologies [55] for VRU traffic safety.

Other communication technologies for V2VRU interactions contain Bluetooth, 700 MHz ITS Band, and 802.15.4. A Bluetooth-based traffic safety system that can spot cyclists and PTWs in the range of 5m is proposed in [84]. However, the limited range of communication makes it useful only in restricted crash scenarios. In [85], 700MHz ITS Band is developed for V2V, I2V and V2P communications. However, the solution is mere experimental. IEEE802.15.4 based low power pedestrian safety system which can cover up to 80m of communication range is presented in [86]. IEEE802.15.4 based technology may be suitable in cases where notification of only vehicles (as it is installed only vehicles) is proved to avoid a collision.

In this section, we have discussed VRU device requirements and available communication technologies for the vehicle to VRU communication. Another component in V2VRU communication is an infrastructure that facilitates indirect communication between the two parties. The next section discusses fog computing which is a good enabler of the stated communications.

2.4/ FOG COMPUTING

An immense number of physical devices all over the world are connected to the Internet, creating the Internet of Things (IoT) paradigm. According to McKinsey [87], one trillion IoT devices are expected to be deployed by 2025. They also estimated the potential economic impact of IoT to dash to 11 trillion USD per year, accounting 11% of the world economy by the same year. The IoT devices generate an enormous volume and variety of data at high velocity resulting in big data. For instance, an electronic health track record system of a patient contains various wearable devices and sensors that produce an ocean of distinct types of data. Cloud computing's high-performance and storage capacity leverage processing and reposition of these data. However, transporting the data to far-situated cloud servers takes up a large amount of bandwidth. Hence, cloud computing is not suitable for real-time analytics and decision making. The problems mentioned above are alleviated by bringing data processing and storage down to the proximity of data production sites. The viability of the solution is founded on the fact that

processing, storage, and networking capabilities of the current edge devices are improved from time to time. One of such solutions is *fog computing*, aka *fogging*.

Fog computing stretches computing, storage, communication, and networking services down to the fringes of the network to reduce latency, decrease bandwidth, and increase reliability [14]. The technology has attracted considerable attention in academics and industry in short period of time. Establishment of consortiums like OpenFog [88] by hi-tech giant companies and renowned academic institutions to define an architecture for fog computing and to build operational models and testbeds is one of the indications of the wide acceptance of the computing paradigm. The upcoming subsections discuss fog computing's architecture, features, applications, and challenges in relation to its usage in traffic safety applications.

2.4.1. FOG COMPUTING ARCHITECTURE

As depicted in Figure 2.5, a fog computing architecture is composed of three main components: IoT or end devices, fog servers, and cloud servers. Fog servers are fog nodes which provide services to fog clients, which are service requests [19], [89]. Fog servers can be set-top-boxes, access points, road-side units, cellular base stations, gateways, routers, etc., while end devices like smartphones, sensors, smart watches, vehicles, cameras, etc., represent the fog clients [89], [90]. Fog servers may be arranged in layers (usually in 2 or 3 layers) and a fog server can be a single device, or it may comprise of multiple devices integrated as one fog node [90]. Fog servers can make horizontal communication with each other [91], making the computing paradigm scalable. The paradigm shift of distributed computing from cloud computing to fog computing doesn't mean fog computing is a replacement for cloud computing. Rather, the two computing paradigms work together by performing important interplays between them to provide services to end users with desired quality. End devices and fog layer communicate through Local Area Network (LAN) while communication between the IoT devices and cloud layer can be done either through the fog or without fog over the Wide Area Network (WAN) [92].

Fogging contains a very large number of geo-distributed fog clients which are responsible for real-time computation, storage, and sensing the environment. These resources-constrained devices send data to fog servers for analysis [93]. The fog servers process the data and give responses quickly. Their proximity to end users enables fast response. If the processing of the data requires either a large processing capacity or a non-delay sensitive response, the fog servers offload the computation to the cloud. Not only fog clients but also fog servers have limited storage capacity to store all the data. Therefore, the processed data which is not supposed to stay at the edge is sent to the cloud periodically.

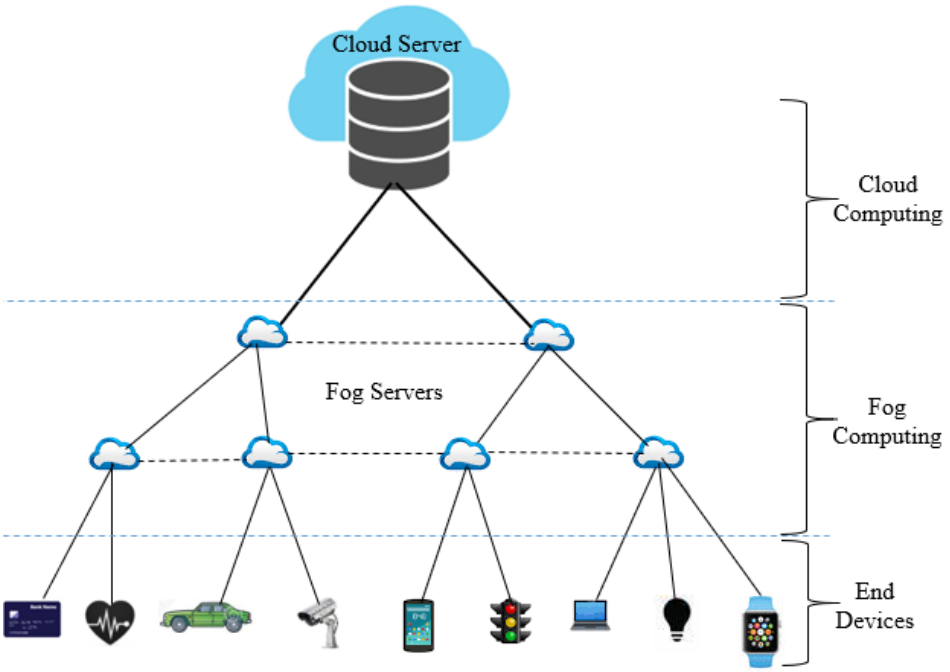


Figure 2.5: Architecture of Fog Computing

2.4.2. FOG COMPUTING FEATURES

Fog computing has multitude of advantages that make the technology attractive [94], [95] for traffic safety and other latency-sensitive applications. Important characteristics of fog computing are:

- *Reduction of Network Traffic and Low Latency:* massive amount of unprocessed data produced by low-level devices is not supposed to be transported far-situated servers. Fog servers process and filter the data drastically reducing the amount of data that is sent to cloud servers. Applications like safety, e-health, gaming, augmented reality, antilock brakes on a vehicle, etc. require real-time data processing. The proximity of fog servers to end users is vital to meet latency requirements of such applications.
- *Geo-distribution and Location Awareness*: fog computing is not centralized, like cloud computing. Instead, it can be deployed anywhere and can provide distributed services and applications. Hence, fog computing supports location awareness, i.e. fog nodes can be deployed in diverse locations.
- *Support for Mobility:* mobile devices can move from place to place without interruption from fog enabled services.
- *Scalability*: fog computing is a multilayered distributed environment which can work with an increasing number of end devices. Intercommunication among fog servers increases the scalability of the service they provide.

- *Heterogeneity*: fog servers and clients are from different manufacturers and they come with different forms. But fogging is made to work on different platforms.
- *Interoperability*: heterogeneous devices need the cooperation of different providers. Fog nodes can interoperate and work with various domains and across different service providers.
- *Reliability*: as a failure of a single node doesn't affect the operation of the entire fog environment, fog computing is more reliable than centralized computing paradigms.
- *Real-time Interactions*, *a Predominance of Wireless Access*, *Support for Online Analytics* and *Interplay with the Cloud*, are other advantages of fog computing

2.4.3. FOG COMPUTING APPLICATIONS

Since its introduction in 2012 by CISCO, fog computing has been proposed for many applications. As it keeps data and computation at the edge near to end users, it has become a source of a new breed of applications and services [96]. Therefore, by exploiting the characteristics of fog computing, many novel IoT applications and services have been suggested. Traffic safety application [56], e-Health [97], web content delivery [98], augmented reality [99], and big data analysis [100] are some of the applications that suit fog computing. Below, we discuss applications of fog computing in the domain of ITS.

[14] and [96] have discussed some fog computing application for connected/smart vehicles. Congestion mitigation, parking facility management, traffic light scheduling, precaution sharing, traffic information sharing, etc. are some examples of such applications. Mobility support, location awareness, geo-distribution all over the city and road-sides, the predominance of wireless access and support of real-time interaction are among the number of features that makes fogging the idyllic environment to provide various smart connected vehicle services in safety, traffic optimization, infotainment and other ITS applications. TABLE 2.1 summarizes some recent fog computing based ITS applications.

TABLE 2.1. SELECTED APPLICATIONS OF FOG COMPUTING IN ITS

Application	Architecture	Fog Servers	Fog Clients	Among fog nodes Communication	Reference, year
Finding a parking space	Three-tier fogging architecture with two fog layers	RSU and other servers	Vehicles	Wireless and wired (to connect to cloud)	[101], 2015
Moving and Parking vehicles analysis	Vehicle to infrastructure and vehicular ad hoc network	Vehicles and mobile devices	RSU and other sensors	wireless	[102], 2016
Vehicular data	Conventional	RSU,	Vehicles	Wireless and wired	[103], 2017

scheduling	three-tier fogging architecture	Base Stations		(to connect to cloud)	
Offloading for real-time traffic management	Conventional three-tier fogging architecture	Cloudlets and RSUs	Vehicles	Wireless and Wired	[104], 2018
Mobility-based geographical migration model for computing resources	Conventional three-tier fogging architecture	Vehicles, base stations, and other servers	Vehicles	Wireless and wired (to connect to cloud)	[105], 2019

Fog computing's suitability for road traffic safety applications is stated in [14], [94]. A smart traffic light can gather information from VRUs and vehicles, estimate collisions from the distance and speed of VRUs, and dispatch warning messages [14]. But this solution is limited to regions where traffic lights are available. An increasing number of traffic accidents and a need to provide computational services to road users have motivated authors of [94] to propose a new cloud computing model which includes fog servers. The model can also be used for detection and resolution of undesirable traffic situations like congestions. Traffic safety applications should provide fast, scalable and reliable services. Moreover, they need to work in a heterogenous environment, making interoperability also one of the crucial attributes. Fog computing needs to be exploited intensively for traffic safety applications as it comes with the characteristics that fit the requirements of traffic safety applications.

2.4.4. PRIVACY AND SECURITY IN FOG COMPUTING

Fogging extends the cloud adjacent to IoT devices (fog nodes) which generate the data. The fog nodes can be deployed anywhere in a network edge where network connection can be made with other nodes and up to the cloud. They may be placed in remote locations where rigorous surveillance and protection is not possible. In addition to sensing and processing the collected data, fog nodes are responsible for storing the data at the edge of the network. Despite proven advantages, fog computing has challenges that arise from its way of deployment and distributed nature. Fog computing has the following issues: network management, placement of servers, delay of computation due to data aggregation, energy consumption, privacy, and security. The devices heterogeneity, combined with distributiveness of fog nodes brings new challenges for the network management [96]. Finding the right place for fog servers such that they can provide maximum services to end users is another problem [106]. Aggregation of data from multiple fog nodes (especially on multilayered fog layers) may introduce long delays [107]. Energy consumption of mobile devices increases since fog computing allows usage of the devices for many applications [108]. Privacy and security are fogging's apparent and most discussed challenges [18], [19], [108], [109], [110], [111]. Majority of the publications explain

challenges and imperativeness of ensuring privacy and security issues on fog computing rather than giving particular solutions.

The physical location of fog nodes in the vicinity of end users make the technology prone to traditional attacks like eavesdropping, data hijack, etc. [109], [110], [111]. Moreover, fog nodes are manufactured by various distinct companies, are maintained and managed by different individuals and may be built by adversaries. They may also join or leave the fog layer any time posing service interruption problems. Devices in fog computing may also be resource-constrained to perform complicated procedures that confirm security [18]. Besides, the distributed architecture introduces new security and privacy risk in addition to those inherited from cloud computing. Because of the reasons pointed above, guaranteeing security and privacy in a fog computing environment is challenging. Yet, there are some research works that have proposed solutions to tackle the challenges. TABLE 2.2 summarizes challenges to apply security and privacy techniques and the solutions proposed for fog computing environments.

TABLE 2.2. CHALLENGES AND PROPOSED SOLUTION FOR SECURITY AND PRIVACY TECHNIQUES IN FOG COMPUTING

Security and Privacy Technique	Challenges and Solutions
Authentication	**Challenges:** IoT devices have limited computation resources to execute cryptographic operations. **Solutions:** According to [112], fog servers can be used for authentication. A public key infrastructure-based authentication protocol is suggested in [110]. However, [19] questions usage of public key infrastructure-based authentication in fogging due to the resource limitation.
Access Control	**Challenges:** Secure collaboration and interoperability between the heterogeneous resources are mandatory to fulfill the security and privacy technique [109]. **Solutions:** a policy-based resource access control is proposed in [113]. A comprehensive review of access control in fog computing is provided in [114].
Trust	**Challenges:** Lack of central entity to manage trust, malfunctioning or change of behavior of fog nodes and trust's requirement of ensuring service reliability are some challenges for trust management [109], [110]. **Solutions:** Many works are proposed for trust management in the IoT environment [115] and cloud computing [116]. A broker-based trust evaluation framework for fog service allocation is proposed in [117]. However, malfunctioning of the broker results in a complete cessation of the trust management system.
Network Security	**Challenges:** The predominance of wireless networks in fog computing implies

	that it is highly susceptible to jamming attacks, sniffer attacks, etc. [19], [109]. **Solutions:** In general schema, [118] recommended separation of normal data traffic from the network management traffic. However, it incurs a heavy burden to network management since the number of fog nodes is usually huge. In relation to fog networking, to avoid heavy roadside sensors and single point of failure as well as to detect malicious vehicles, a secure intelligent traffic light control system for Vehicular ad hoc Network (VANET) is proposed in [119]. [120] proposed fog computing-based face identification and resolution framework to ensure the identity consistency of humans in physical space and cyber space.
Rogue Node Detection	**Challenges:** A rogue node may be injected or built up in fog networks. This makes the environment vulnerable to attacks like man-in-the-middle attacks. Dynamic environment and change of behavior of fog nodes make it hard to maintain a blacklist of rogue nodes. The complexity of trust management in various scenarios makes rogue node detection in IoT systems difficult [112]. **Solutions:** a framework that detects a rogue access points in Wi-Fi networks is suggested in [121].
Intrusion Detection	**Challenges:** In fog computing, intrusion can be detected by monitoring and analyzing log file, access control policies and user login information [19]. However, the low latency requirement of fog-applications creates many challenges in intrusion detection [109]. **Solutions:** Bearing in mind the resource limitations of IoT devices, a lightweight intrusion detection system is proposed in [122].
Secure Data storage and processing	**Challenges:** the data stored in fog nodes is easily physically accessible. Offloading sensitive data from one node to another may put data privacy at risk. That is ensuring data integrity and unauthorized access is challenging. Low-latency demands, supporting dynamic operation, dealing with the interplay between fog and cloud, and resources limitation of fog devices are reasons for challenges to ensure data storage and processing security [19]. **Solutions**: A privacy-preserving data transmission protocol that meets data confidentiality and integrity, mutual authentication, anonymity, and key escrow resilience is proposed in [123]. A data security storage model to realize the integration of storage and security management in large-scale IoT application for fog model is presented in [124].
End User Privacy	**Challenges:** Fog nodes being in the vicinity of end users puts identity, usage and location privacy in danger [110]. Geo-distribution, location awareness and increased communication make imposing privacy a difficult process. **Solutions:** A secure positioning protocol with location privacy is presented in [125]. However, the solution has limitations for applications that demand high

	position accuracy and high rate location sampling. Lack of trusted party in fogging complicates the implementation of private usage. For identity privacy, privacy-preserving methods mentioned in [126] can be used. However, anonymization of user information for each task request may incur computational burden [127].

Fog computing has a wide acceptance in academia and industry due to its characteristics that suit many application requirements. However, some challenges have become obstacles to rejoice the benefits. Security and privacy are among those challenges that require immediate attention. Because of this, solutions are being proposed at a rapid pace. However, the problem is far from being solved in its entirety. In fact, some literature has explicitly stated the difficulty of ensuring security and especially privacy in fog environments. For instance, Mithun et al [110] stated that "*how to provide the location and identity privacy for fog computing is a challenging issue*". Jianbing et al [18] asserted that "*unfortunately, it is of difficulty to protect users' locations in fog computing*". According to [128], fog node faces new challenges in addition to those inherited from cloud computing due to its architecture and unattended and remotely operated fogs.

However, we believe that trust management is one of the ways to tackle the problems of security and privacy in fog computing. Trust management ensures user privacy and information security. It is also related to reliability, integrity, dependability, and ability to perform a service. Trust management allows autonomous connections establishment between fog servers and resource-constrained IoT devices. Moreover, trust management is known to be effective in the detection of misbehaving nodes in a network.

2.5/ SUMMARY AND DISCUSSIONS

Road accidents are causing unacceptably high death toll all over the world even though the geographic spread of the losses is not uniform. A very high proportion of traffic deaths is among pedestrians, cyclists, and PTWs due to their high volume and lack of protections. Even though road safety doesn't get attention it deserves, many passive and active road safety measures have been proposed. Road safety solutions that use both passive and active safety solutions have high chance of reducing road accidents. Active safety measures have capabilities to thwart an about-to-occur accident by predicting the accidents, and warning road users. To detect potentially dangerous conditions of VRUs, active safety systems should understand the road scene using VRU devices. VRUs should share their position and context information obtained using their devices to avoid traffic accidents, and possibly for other ITS applications. VRU devices can be tags, dedicated devices or mobile devices like

smartphones. However, since many users own mobile devices with high computation, storage, communication, and sensing capacities, they are ideal candidates to function as VRU devices.

VRU devices enable to create a connection between road users and vehicles using various communication technologies. However, the devices must fulfill position accuracy and sampling rate requirements of traffic safety applications. The applications require centimeter level position accuracy to save road users from accidents. However, current mobile devices GPS readings are far from that figure. Hence, various hardware and software-based accuracy improvement methods are proposed. Because their small size and hardware limitations, hardware-based solutions of improving GPS accuracy of mobile devices are not promising. Instead, the position accuracy of mobile devices can be improved using algorithms like map matching algorithms. Regarding the position sampling frequency, a VRU in high traffic safety regions needs to beacon his position data 10 times in a second, which is not satisfied by current mobile devices. The fusion of data obtained from inertial sensors with GPS data is a feasible solution to cope with high sampling demand of road safety applications. Nevertheless, high rate position sampling and communication with vehicles results in high energy consumption of the handheld devices. To solve this problem situation adaptive position sampling and communication based on road accident risk-level of road users is helpful.

V2VRUs connection between vehicles and VRUs can be realized either directly or indirectly through infrastructures. Infrastructure can be RSU, TMC, central server, etc. Indirect connection using infrastructures have advantages over direct communication. Some of the advantages are heterogeneity (devices that support different communication technology can communicate with each other), the burden of running the VRU collision prediction algorithm and message management can be handled by the infrastructure. It also enables the safety mechanism to cover large geographical area using multi-hop communications. However, the involvement of infrastructures has an effect on response time, reliability, and scalability of the application. Hence, the infrastructure must satisfy these and other characteristics of road safety solutions.

Fog computing, which is a newly introduced distributed computing paradigm is an excellent contender to serve as infrastructure in active safety systems. Fog computing extends cloud computing closer to user arena so that end users can benefit from computation, storage, and communication services provided at the edge of networking. It has advantages like low latency, geo-distribution, location awareness, mobility support, predominant wireless communication, heterogeneity, interoperability, and scalability, all of which are vital for safety critical systems. Therefore, in addition to traffic safety systems, it is being proposed for emergency warning systems, e-Health systems, and so on. However, its proximity to the end users access area makes the fogging vulnerable to security and privacy attacks, among others. Moreover, fog nodes come from different vendors, are contributed and managed by different individuals, and they can join or leave the network anytime. Some solutions are

proposed to solve different security and privacy aspects, but the problem is still apparent and requires a lot of effort to be safe from such attacks. Trust management-based solution is promising to address privacy and security challenges in fog computing. In this type of remedies, fog nodes establish the connection to only trustworthy nodes i.e. they avoid connection to untrusted nodes.

2.6/ CONCLUSIONS

Throughout this chapter, we gave an overview on road traffic injuries, road safety measures, connected VRUs, and on fog computing. We have also discussed recent works in relation to the aforementioned topics and the challenges which yet require attention. We began the chapter by presenting the extent of road accident damages in human life. Next, the proposed passive and active safety measures to alleviate the problem were discussed. Connecting VRUs with vehicles to exchange personal safety messages is elaborated. VRU needs to have portable VRU devices to create a connection through several options of wireless communication technologies. Furthermore, the requirements of VRU devices used in active road safety systems and the efforts made to meet the demands as well as open issues are explained. An emerging fog computing paradigm which has enormous potential for road safety architectures is presented. Emphasis is given to architecture, features, and application of the technology. Moreover, the privacy and security challenges of fog computing are discussed. Before we provide the conclusion of the chapter, a summarized discussion is given.

The subsequent chapters present the main contributions of this thesis. To reduce high fatalities of VRUs, we have proposed a fog computing-based road safety architecture that exploits omnipresent mobile devices as VRU devices. The next chapter discusses this architecture. Following chapters deal with challenges pertaining to mobile devices and fog computing to meet requirements of road safety applications.

3

PV-ALERT: A FOG COMPUTING BASED ARCHITECTURE FOR SAFEGUARDING VULNERABLE ROAD USERS

3.1/ INTRODUCTION AND PROBLEM STATEMENT

As it has been stated in previous chapters, road traffic injuries are globally one of the leading causes of death [1]. The number of road traffic deaths because of traffic injuries exceeds deaths caused by HIV/ AIDS, tuberculosis, and diarrhea combined. More than half of those deaths are attributed to VRUs. Even though traffic accidents and fatalities have decreased greatly over the past few decades, the decrease of fatalities among VRUs is much less than all other road users [3], [20]. Because of the lack of protective "shells" or safety features, pedestrians are more vulnerable to traffic accidents than other groups of road users. Pedestrian accidents occur in roads where LOS are affected, road intersections, straight roads, and even in pedestrian crossings in both urban and rural areas. As distracted driving is the main contributor to traffic accidents, many countries banned drivers from using mobile phones during driving. In recent days, inattention and distracted walking like talking and walking, listening to music or texting have become an emerging problem to pedestrians due to an exponential growth of the use of mobile phones and other smartphones worldwide [5], [6], [7]. This chapter aims to take advantage of the pervasive existence of mobile devices to propose traffic safety architecture that helps to protect VRUs instead of becoming a reason for their death.

To assuage road traffic accidents, many passive and active protection mechanisms have been proposed. Passive safety systems include measures that could be categorized into 'three Es': engineering, education, and enforcement [31]. Providing a wide flat area for slower moving traffic, designing bumpers, increasing visibility of roads, educating traffic safety, and setting strict law enforcement are some examples of passive traffic accident protections. Active VRU protection measure involves VRU detection, collision prediction, warning, automatic braking, and collision avoidance [129]. There are situations where traffic accidents cannot be avoided. However, the application of both passive and active protection mechanisms is crucial to minimize the number of traffic accidents. Many studies on active traffic accident protection mechanisms are conducted to precaution pedestrians and other VRUs. Most of

these works are infrastructure-based, which depends on sensors, cameras, radio tags, road-side units, etc. Contemporary researches on VRU safety rely on handheld devices of road users' together with state-of-the-art technologies to warn them about traffic accidents [53], [54], [55], [60], [77], [130]. However, still most of these works rely on infrastructures RSU, TMC and Human-Machine Interfaces (HMI) for vehicle to VRU communication and some of them are not reliable, others are not scalable or have high latency.

In this chapter we present a fog computing-based architecture proposed to protect VRUs from traffic accidents using ubiquitous mobile devices. Many VRUs have their own handheld devices like smartphones, and the devices nowadays are outfitted with advanced onboard GPS sensors that can detect their position. The devices support broadband Internet connections to connect to servers that predict accidents. Since fog computing extends cloud computing down to users' arena to proximate computing, storage, and network services to end users, it is suitable for latency sensitive applications. The decentralized computing infrastructure has essential characteristics like low latency, location awareness, wide-spread geographical distribution, mobility support, the existence of a very large number of nodes and predominancy of wireless access [14], making it ideal for traffic safety applications. The potential of fog computing for ITS is advocated in the literature including [14], [102] and [131]. Currently, the majority of researches in fog computing involves defining the computing paradigm, lucubrating its characteristics and its relation with other related technologies, proposing networking and reference architectures, as well as suggesting application scenarios where it is the best fit.

The proposed architecture is an infrastructure-less[1] solution which uses VRUs' and drivers' mobile devices crowd sensed data to detect their geographical locations and fog nodes to predict a collision risk, and send warning, if there is imminent accident. VRUs' and vehicles' GPS readings that includes speed and direction are periodically sent to the fog node through wireless connections from the devices. Fog node (or fog server) intakes the readings and executes VRU traffic collision prediction algorithm. If there is any imminent collision, it sends warning messages to both VRUs and drivers. The three-tier fog-node based architecture exploits the enabling characteristics of fog computing and has the capability to detect traffic accidents accurately and send warnings in real time. The comparison of the architecture with other smartphone-based solutions using evaluation criteria we have defined, shows that the new architecture surpasses others in terms of scalability, reliability, and performance. Moreover, extensive performance evaluations of the architectures in a simulated environment indicate that the architecture fulfills latency and packet delivery ratio requirements of safety applications.

[1] The architecture does not need any additional and newly installed infrastructures (e.g. road side units) than those already available for other purposes

The remainder of this chapter is organized as follows. Section 3.2 elucidates summary of related works. In section 3.4, we detail the proposed architecture and the algorithm defined for traffic collision prediction. Section 3.5 presents performance evaluation results and comparison of the new architecture with other related architectures. Finally, conclusions are drawn in section 3.6.

3.2/ RELATED WORKS

Even though traffic accidents and fatalities have decreased in the past few decades, the problem still needs attention, especially for VRUs. To reduce traffic fatalities and accidents, various researches are conducted, and many solutions are proposed, ranging from design enhancements in infrastructure and vehicles to application of cutting-edge technologies for VRUs collision detection and prevention. As stated earlier, traffic safety measures can be passive or active. Passive safety encompasses safety countermeasures to mitigate the consequences of an accident as much as possible once it happens, such as seat belts, air-bags, and strong body structures. However, active safety measures includes systems that use an understanding of the state of the vehicle to avoid or minimize the effects of a crash, such as a brake assist, electronic stability control system, advanced driver assistance systems [55], [132]. Safety measures may be related to vehicles, VRUs, or road infrastructures. Some examples of passive and active safety measures and literature that deals with the measures are recapped in TABLE 3.1.

TABLE 3.1. EXAMPLES OF PASSIVE AND ACTIVE VRU SAFETY MEASURES

Passive safety measures	Active Safety measures
Pedestrian Airbag System [133]	Special pedestrian traffic lights [134]
Proper usage of Seat Belts [135]	Intelligent Vehicle Speed Controller [136]
Automatic in-vehicle emergency call service (e.g. eCall) [137]	Navigation Systems [138]
Padding to reduce injuries in automobile accidents [139]	Automatic Emergency braking [40]
Intelligent restraint Systems [140]	Adaptive light control [141]
Using Helmets [142]	Motorbikes and cyclist's detection and warning system using V2X Communications [84]

Studies in traffic safety solution may be grouped in both active and passive types. For instance, [143] proposed a new approach using state-of-the-art numerical technologies for VRUs' safety enhancement. The solution can detect VRUs and provide data to active safety systems to protect accidents, and in case of an unavoidable accident it puts passive safety structures and systems into operation to mitigate the collision effect. Other studies consider all types of VRUs: an urban VRU classification framework using local feature descriptors and hidden Markov model has been proposed by [144] to detect and classify pedestrians, bicyclists and PTWs. Though the focus is on pedestrian safety, our architecture can also entertain all types of VRUs as long as the VRUs are equipped with mobile devices.

Literature on passive pedestrian protection systems and the earlier works on active pedestrian protection systems that require cameras, infrared, radar, tags, and image processing are discussed in detail in [129]. To protect distracted users, recently, many solutions have also been proposed, including designing special traffic lights [134]. The solution, which is named *the +Lichtlijn* is linked to existing traffic lights and emits lighting strip in the pavement. Pedestrian detection mechanisms mentioned above require infrastructures, are profoundly affected by weather and do not work if the pedestrian is not in LOS or in situations where visibility is limited. Therefore, researches that depend on V2P communication technologies to overcome these problems have got attention. Smartphones which are becoming causes of many traffic accidents are being used for safeguarding VRUs instead. Because of their sensing and communication capabilities, they become feasible for VRUs active safety [15]. Smartphone based systems are important to protect VRUs whose line of vision is affected by buildings, trees, parked cars, and other hindrances.

V2P communication prototype has been developed using the 3G cellular network and WLAN to deter possible collisions by giving an alarm to both pedestrians and vehicles [77]. The authors have developed an algorithm that estimates the collision risk between pedestrians and vehicles and tested the prototype at T intersection. However, due to the absence of dedicated central servers, the system is not scalable to be applied in different road scenarios and to accommodate increased number of road users. In another similar work [60], vehicles directly alert pedestrians their existence in close distance using Wi-Fi technology. This work has revealed minimum information exchange distance based on the communication technologies used and claimed that Wi-Fi could satisfy the application requirements. Minimum information exchange distance is the minimum distance vehicles, and pedestrians have to exchange information to avoid accidents. Nevertheless, as there is no central server that manages messages sent to pedestrians, there is a possibility of message overloading. In another research [55], a pedestrian safety concept based on pedestrian detection, filtering supported by personal profiles and context awareness, prediction calculation, communication, and warning has been demonstrated. However, the solution looks impractical as most of the pedestrians may be strangers. In this work, an assessment has been made on different architectures comprising different combinations of cellular and ad hoc networks.

Albeit the main focus of [53] is on energy management of smartphones while using them for pedestrian road safety, the authors have proposed a method which assists the development of V2P road safety applications without requiring any infrastructure unless existing ones like a central cloud server, mobile devices and cellular connectivity of vehicles. They also argued that cellular networks are best fits for pedestrian safety applications due to high mobility support, high bit-rate, large communication range, and high capacity as well as reduced user adoption costs and market penetration time. However, cloud computing-based applications are not suitable for low latency applications. In an architecture proposed

in [54], the information generated by vehicles' and cyclist's mobile devices is sent over heterogeneous communication architecture and processed in a central cloud server which generates messages that are shown on the drivers' and cyclists' HMI. The proposed C-ITS allows the use of vehicles as mobile sensors that share their positions, speed, and direction in the form of floating car data with the VRUs warning each other about their locations so that they can take appropriate maneuver to avoid collisions. The system is primarily designed for cyclists, and it relies on infrastructures like RSUs, TMCs and HMIs.

The summary smartphones based VRU traffic safety proposals in terms of communication mode, communication technology, VRU type addressed, and whether the alerts are sent to VRU only, or to driver too are shown in TABLE 3.2. Communication mode, could be direct, indirect with the assistance of infrastructure (shown in bracket) or hybrid.

TABLE 3.2. SUMMARY OF TRAFFIC SAFETY WORKS FOR VRU

Reference	Communication Mode	Communication Technology	VRU Type	Alert sent to
Hernandez-Jayo et al. [54]	Indirect (Central Server)	Cellular, 802.11P	Cyclist	Cyclist
Anaya et al. [60]	Direct	Wi-Fi	pedestrian	Pedestrian
Bagheri et al. [53]	Indirect (cloud server)	Cellular	Pedestrian	-
David and Flach [55]	Hybrid (Central Server)	Cellular, Wi-Fi	Pedestrian	-
Sugimoto et al. [77]	Hybrid (Central Server)	Cellular, Wi-Fi	Pedestrian, Cyclist	VRUs and drivers

Our work differs from works mentioned above in the fact that it is based on a fog computing architecture to take advantage of geographically distributed fog servers to collect crowd sensed data from VRUs and vehicles, predict collision risk and dispatch warning messages to road users and drivers. As mobiles have limited capacity, scalable architecture with low latency is mandatory. The proposed architecture which is named PV-Alert (Pedestrian-Vehicle Alert, as the architecture is tested mainly for pedestrians) meets these characteristics and doesn't require special infrastructures except existing ones (users' smartphones, wireless connections, and fog computing environment).

3.3/ PROPOSED ARCHITECTURE AND ALGORITHM DESCRIPTION

In this section we first present the proposed architecture and its components. Next, a description of the VRU collision prediction algorithm including its flow chart is outlined.

3.3.1. PV-ALERT ARCHITECTURE

PV-Alert is the architecture that relies on only existing infrastructures, mainly fog computing environment and smartphones, Figure 3.1. The architecture has three layers: perception layer (or user

layer), fog layer, and cloud layer. The detail description of the layers is presented in the following paragraphs.

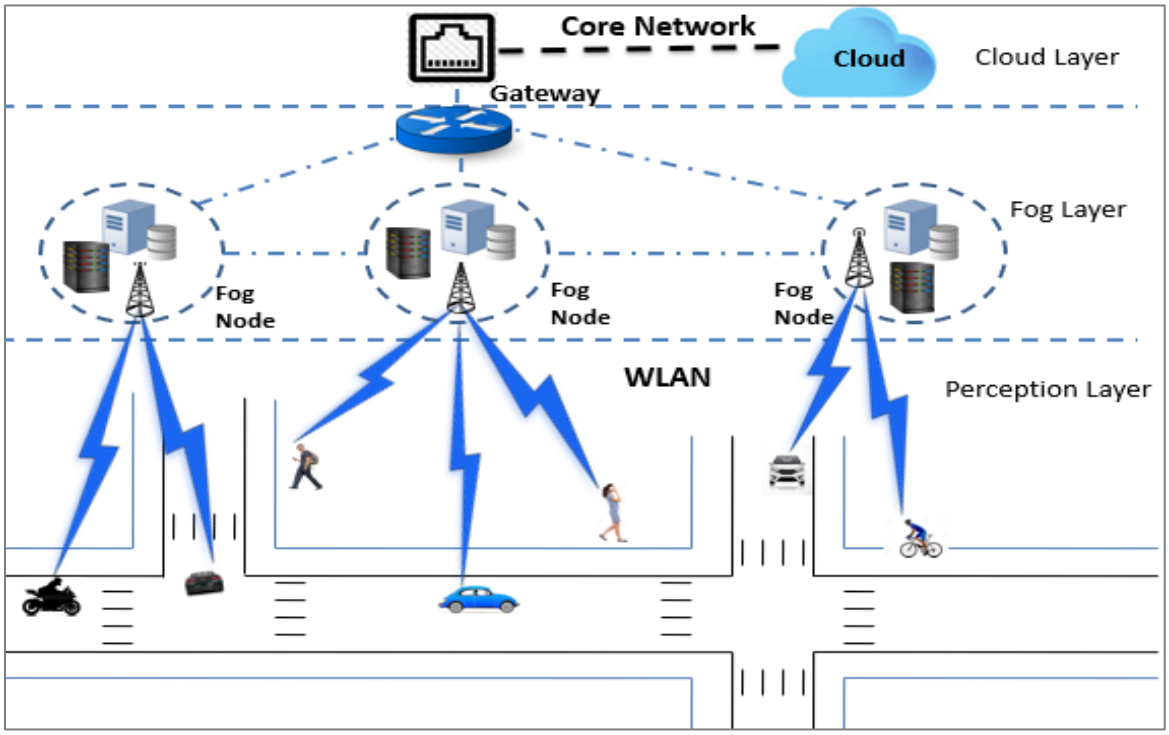


Figure.3.1: PV-Alert – the VRU safety architecture

- *User layer* or *perception layer* refers to road users and their associated mobile devices. This layer is responsible to perceive and send positions of VRUs and vehicles in terms of latitude, longitude, velocity, bearing, and other associated data. It also receives alert messages sent from fog nodes. At this stage, just like [55] and [130], we assume that the position information read by smartphones of VRUs and drivers has enough precision for traffic safety applications. Of course, chapter 4 deals with an improvement of GPS accuracy since positions read by smartphones are inaccurate [145] and VRU safety systems require very accurate GPS readings. After appending time stamp, the CAM is sent to the nearby fog node periodically. If there are more than one fog nodes in proximity, the load situation, quality of service or other parameters can be taken into consideration for node selection. Note that the minimum CAM frequency for traffic safety applications is set to be 1Hz by ETSI [59]. If the traffic risk level of VRU is higher, the frequency of sending CAM must increase accordingly. On the other hand, if VRUs are in less traffic risk regions, smaller frequency of messaging can be applied to save energy consumption of smartphones and bandwidth of the network. For instance, even though the owners of the mobile devices are near roads, their mobiles send data to the fog node only when there is any potential risk of collision and when they are in motion. Furthermore, VRUs who are

moving away from vehicle roads and which are not in the proximity of roads are excluded from sending the CAM. It is the duty of collision prediction algorithm which runs in fog server to recognize such situations and instruct the smartphones to switch frequency of beaconing CAM. See chapter 6 for more on collision risk level based adaptive beaconing rate management.

- *Fog Layer* is another important layer of PV-Alert which mainly contains *Fog nodes*. The fog node may be either a single device like a gateway, switch, router, access point, or group of devices working together. The responsibility of this layer is receiving CAM messages sent from connected VRUs and executing collision prediction algorithm. If any risk of collision is anticipated, the node sends DENM in real time to both VRU and driver as accidents are usually due to driver's error and/or VRUs' inattention or destruction. Moreover, fog nodes perform perturbation and aggregation of the collected data before sending it to the cloud for user privacy and data security. Fog nodes can communicate with each other. This makes the computing paradigm scalable and reliable. Moreover, a fog layer is usually arranged in two or three layers.
- The third layer comprises a *cloud server*. Its responsibility is performing aggregated analysis on data received from fog nodes for further use in traffic analysis and decision making.

Edge location of fog nodes in bus stations, supermarkets, and road side buildings make fog computing an ideal solution for latency-sensitive applications like traffic safety [14]. Fog nodes may be connected to smartphones using WLAN, which could be Wi-Fi, cellular networks including LTE, WiMAX, etc. The nodes are extended to the cloud server using core networks. The length of the road segment covered by a single fog node varies from hundreds of meters to kilometers depending on the communication technology used. The next section details the collision detection algorithm for VRUs.

3.3.2. COLLISION PREDICTION ALGORITHM DESCRIPTION

In PV-Alert, CAM messages sent from drivers' and VRUs mobile devices are processed by fog servers to predict collisions. Road user collision prediction algorithm is helpful to predict collisions and send alerts to VRUs and drivers. The algorithm is deployed in fog nodes and can be applied to any road scenario. Its flowchart is shown in Figure 3.2.

In the initialization step, VRUs' and drivers' mobile devices are subscribed or connected to the server. Smartphones send their sensed CAM data to the server periodically. For optimization purpose, VRUs moving away from road segments, far away from road segments and those at rest send their position data at long intervals. Those who are in no danger of traffic accidents are inactivated.

The succeeding step identifies intersecting VRUs and vehicles using the sensed data, road information and the source, destination as well as path of each vehicle. Intersecting VRUs and vehicles are those which cross each other with possible collision risks. If we consider a traffic scenario shown in

Figure 3.3, Vehicle V1 is expected to intersect only road user VRU1 since VRU2 is moving away from the vehicle and VRU3 is too far from the Vehicle. In this way, intersecting road users can be obtained for each vehicle to VRU combination.

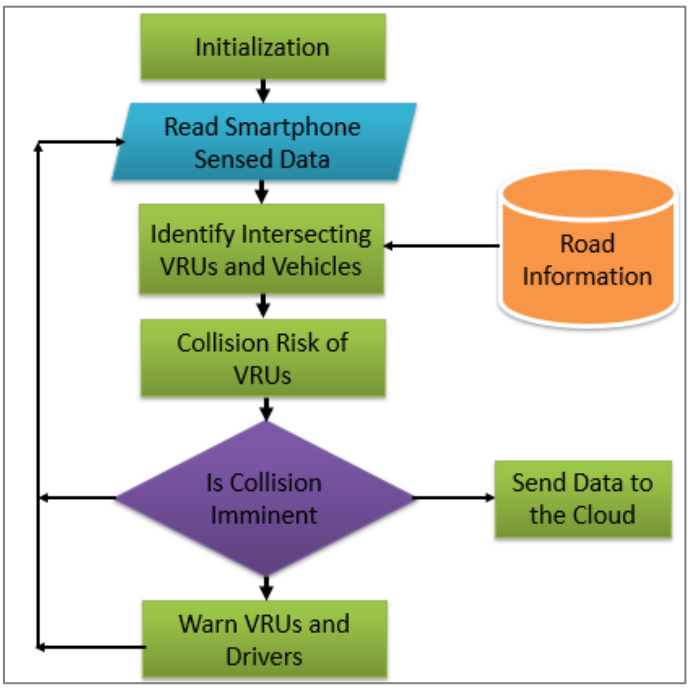


Figure 3.2: Flowchart of VRU collision prediction algorithm

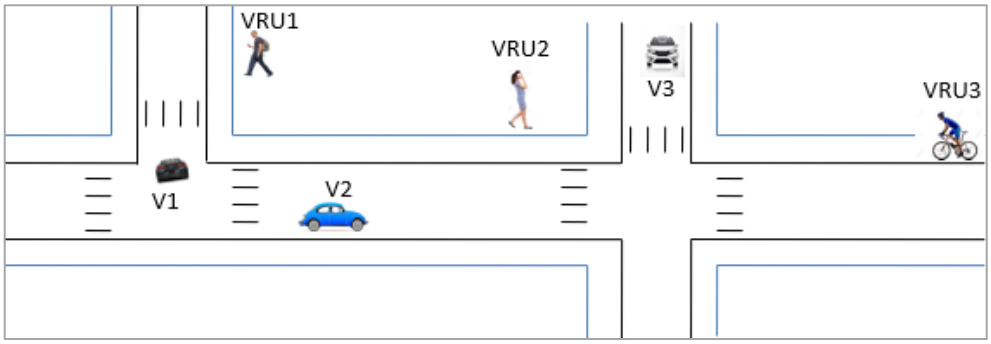


Figure 3.3: Identifying intersecting VRUs and vehicles

The most essential module is a collision risk prediction module. This module estimates potential dangers of the collisions between road users, and vehicles at a particular instant of time. For this purpose, minimum information exchange distance (D_{min}) is computed using the equation obtained from [60]:

$$D_{min} = V_{veh} * (t_p + t_r + t_{tx} + t_c) + GPS_{err-veh} + GPS_{err-VRU} \quad (3.1)$$

Where V_{veh} is the velocity of a vehicle; t_p is the perception time, and it is 0.83s [60]; t_r is the reaction time, and it is 0.17s for audio alerts [146]; t_{tx} is the transmission delay; t_c is the computation time of algorithm, and $GPS_{err-veh}$ and $GPS_{err-VRU}$ are GPS errors of vehicles and VRU locations.

Next, the actual distance from the vehicle to VRU crossing in the road is calculated. The actual distance is simply calculated using distance formula as locations of the two parties are known and as we have a database storing road information. Based on D_{min} and actual distance, it can be determined whether there is an imminent collision or not. If the actual distance is less than D_{min}, then the VRU is in a collision risk region, and a warning message is sent to both driver and the road user. If a VRU is in more than one collision risk regions of vehicles, then a warning message management module takes care of multiple messages to avoid messages overload. The algorithm runs indefinitely in iteration within the fog node. To evaluate the architecture, the algorithm is implemented and installed in a fog server. Details of performance evaluation of the PV-Alert are described in the following subsection.

3.4/ PERFORMANCE EVALUATION AND DISCUSSION

In this section, we first give an analytical comparison of PV-Alert with other similar smartphone based VRU safety architectures. Simulation setup and the considered road scenario are then discussed. Performance evaluation results are presented at the end of this section.

3.4.1. ANALYTICAL COMPARISON

Various smartphone-based architectures have been proposed since today's mobile devices have many capabilities in addition to their primary purpose. Comparison of different architectural approaches utilizing ad hoc and/or cellular technologies and different processing setups (i.e., location of filtering process) has been made by Klaus David et al. in [55] using criteria like energy consumption, time agility, reliability, cost and ease of management. In this subsection we present a similar analytical study that compares PV-Alert with other smartphone-based traffic safety architectures using our new comparison criteria.

Generally, smartphone-based traffic safety architecture can be categorized into two classes: architectures that use only the handheld devices with no central server and architectures that use the smartphones and some kind of central server or infrastructure. In the former case, vehicles and pedestrians directly communicate with each other [60]. This implies that the collision prediction algorithm runs on the mobile devices. In the latter case, the mobile devices are primarily responsible to send CAM to the central server and to receive DENM or warning message dispatched from the server. So, the prediction algorithm runs on the central server. Further classification can be made on the second group based on whether a central server is a cloud server [53], [54] an ordinary server [55], [77], [130], or a fog server (PV-Alert). Hence, we propose to classify smartphone-based architectures into four

categories: mobile-to-mobile (M2M), mobile-to-cloud (M2C), mobile-to-ordinary server (M2OS), and mobile-to-fog node (M2FN). M2OS differs from M2FN in that the former has a standalone server that has no capability to communicate with neighboring servers. The architectures are compared in terms of energy saving, latency, reliability, scalability, computational capability, and message management. The comparison metrics are briefly defined below.

- *Energy saving* - is the ability of an architecture to assist mobile devices to save their energy.
- *Latency* - as defined in [55], is concerned with how much time the system has between sensing and reaction. Round trip time, connection establishment time, and VRU collision prediction algorithm processing time have important contributions for the latency.
- *Reliability* - An architecture is said to be *reliable* if the failure of some of its component does not lead to the cessation of the entire system.
- *Scalability* of an architecture is its ability to cope and perform as an application of the system expands to city wide scale beyond road segments.
- *Computational capability* refers to the capability of the server to run collision prediction algorithm efficiently.
- *Message management* is about handling multiple warning messages for a VRU or a driver. That is, if a VRU is in collision risk area of multiple vehicles, he may receive multiple warning messages causing a message overloading. But for optimum safety of the road user and proper use of resources, VRUs should receive one message that indicates multiple collision risks.

TABLE 3.3. COMPARISON OF DIFFERENT TRAFFIC SAFETY ARCHITECTURES

Architecture	M2M	M2C	M2OS	M2FN
Energy Saving	-	+	+	+
Latency	+	-	+	+
Reliability	+	-	-	+
Scalability	-	+	-	+
Computational Capability	-	+	+	+
Message Management	-	+	+	+

As shown in TABLE 3.3, architectures are ranked as + (for high) if the architecture meets the criteria or – (for low) otherwise for each criterion. Architectures involving only mobile devices (M2M) have the shortest latency and the failure of one or more mobile devices will not affect the entire system. However, it has high energy consumption, low computational capability, limited scalability, and is subject to message overloading. Architectures with a central server (M2C, M2OS, and M2FN) enable mobile devices to save their energy (since collision detection algorithm runs on the servers with

continuous power supply), have a high computational capacity, and can centrally manage warning messages. Reliability of M2C and M2OS are low since the failure of a centralized server leads to total stoppage of the system. Fog node and cloud server-based systems have high scalability due to geo-distribution and high computational capacity, respectively. Therefore, from this comparison, we can conclude that a fog-based architecture is the best fit for VRU safety applications as it is more reliable, scalable, and has low latency.

To reinforce analytical comparison results, we have made an empirical performance comparison on selected architectures from each of the four categories. As shown in Figure 3.4, mobile to mobile architecture proposed in [77] has a delay of 20ms for V2P communication when wireless LAN is used. Average round trip time of bike and vehicle reception delays of mobile to cloud architecture is about 281ms [54]. In mobile to ordinary server architecture proposed by [55], the latency of 100ms is registered when, by then latest cellular network, high speed packet access network is used. Mobile to fog node (i.e. PV-Alert) architecture has a maximum round trip delay of 60ms, see section 3.4.3, making it the second-best time. However, with other attractive characteristics of fog-based architecture, it is the best choice for VRU safety applications. In addendum, we can infer that fog computing is a promising computing paradigm for other ITS applications.

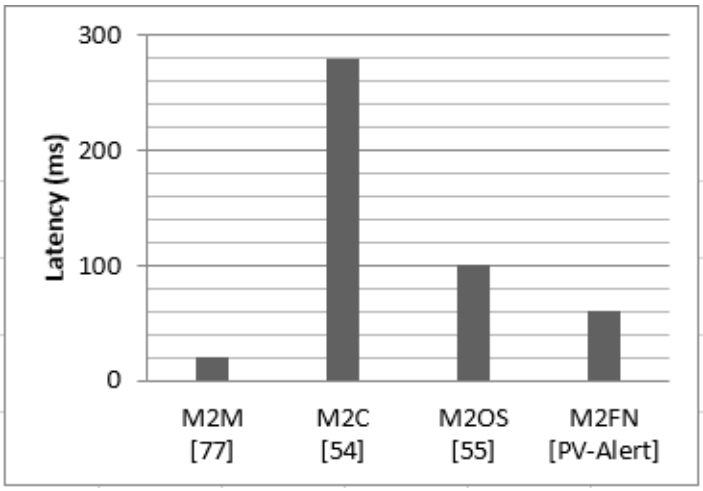


Figure 3.4: Latency of different smartphone-based VRU safety architectures

3.4.2. SIMULATION SETUP AND SCENARIOS

Before deploying the proposed architecture in a real environment, testing the system in a simulated environment is vital. The purpose of simulations in this research is to check if PV-Alert is feasible and fulfills the constraints enacted by ETSI for traffic collision warning VRU applications. The main objective of our research is to enable drivers & VRUs avoid collisions by notifying each of them

through their mobile devices. Mobile devices could communicate with the fog node using Wi-Fi, WiMAX or cellular connections like LTE. Different works already show that both Wi-Fi [60] and cellular [53], [147] connections can be used for traffic safety applications. Hence, our simulations are done for Wi-Fi and LTE. The fog node is placed in the proximity of an access point and an eNodeB for Wi-Fi and LTE, respectively. Our simulation is different from evaluations of other similar works in that our tests include a large number of VRUs (i.e., pedestrians) and vehicles. Such simulations are very important, since it is very difficult to run on a real environment. The two-performance metrics considered to evaluate the architecture are:

- *Round Trip Delay Time (RTD)* – the time period from sending CAM beacon to the fog node to receiving a warning message in case of an anticipated accident. It is computed using the following formula:

$$RTD = T_{sp-fn} + T_c + T_{fn-sp} \tag{3.2}$$

  Where,
  - T_{sp-fn} is end-to-end delay from smartphones to fog node,
  - $T_{fn-sp}$is end-to-end delay from fog node to smartphones,
  - T_c is computation time of the algorithm.

- *Packet Delivery Ratio (PDR)* – the average ratio of packets received by fog node and smartphones to the total packets sent to fog node (from smartphones) and to smartphones (from the fog node).

  We used the following equation to calculate PDR:

$$PDR = 100 * (\frac{1}{2} * \left(\frac{P_{Rec-sp}}{P_{Gen-fn}} + \frac{P_{Rec-fn}}{P_{Gen-sp}}\right)) \tag{3.3}$$

  Where,
  - P_{Gen-sp} is total number of packets generated by smartphones,
  - P_{Rec-sp} is total number of packets received by smartphones,
  - P_{Gen-fn} is total number of packets generated by fog node,
  - P_{Rec-sp} is total number of packets received by fog node.

PV-Alert is evaluated using discrete-event open network simulation environment ns-3 [148] and microscopic, multi-modal traffic simulation tool SUMO [149]. Both tools are most widely used since they are open source and are being actively supported. As depicted in TABLE 3.4, the simulation parameters are grouped into four: general parameters, parameters related to SUMO, and communication technology parameters for LTE and Wi-Fi. The size of the packet (i.e., CAM message) which is sent

every second for two minutes to the server is assumed to be 1KB. The speed of vehicles is taken to be between 10km/h to 80km/h while pedestrian speed is 5km/h. Furthermore, important parameters and respective values are displayed in TABLE 3.4.

TABLE 3.4. SIMULATION PARAMETERS

Parameter	Value
General Parameters	
Packet Size	1KB
Simulation Time	120s
CAM Frequency	1Hz
SUMO Parameters	
Vehicle Speed	10-80km/h
Pedestrian Speed	5km/h
Simulation Area	120mx60m(Wi-Fi) & 3000mx60m(LTE)
Scenario	Refer Figure 3. 5
LTE Parameters	
Propagation Loss model	Nakagami with Free Space path loss
Fading Model	Trace Fading Loss Model
Scheduler	Proportional Fair MAC Scheduler
TxPower(eNB)	25dB
TxPower (UE)	15dB
Downlink bandwidth	30MB
Uplink bandwidth	25MB
Wi-Fi Parameters	
Propagation Loss model	Nakagami chained with Log Distance
Bandwidth	20MHz
Frequency Band	5GHz
Client TxPower	16dB
Server TxPower	25dB

The road scenario considered is a two-lane straight road with many pedestrian roads crossing it, see Figure 3.5. The reason for why we have chosen this scenario is vehicles speed is high in a straight road and pedestrians coming out of smaller intersecting roads are highly susceptible to traffic accidents due to an affected line of vision, distraction, or inattention. Moreover, the severity of a straight road crash is 0.9 to 3.2 times more severe or fatal outcome than on non-straight roads [150]. Even though many studies focus on crossing roads [60] and T roads [77], the literature reveals that a high percentage of road accidents occur in straight roads; 89.8% [151], and 93% [152]. Pedestrian accidents are even common in pedestrian crossings [153], [154].

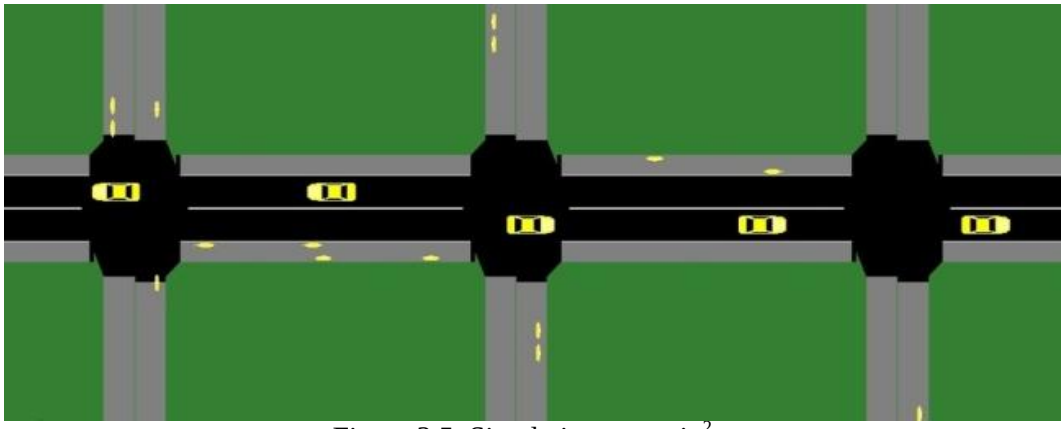


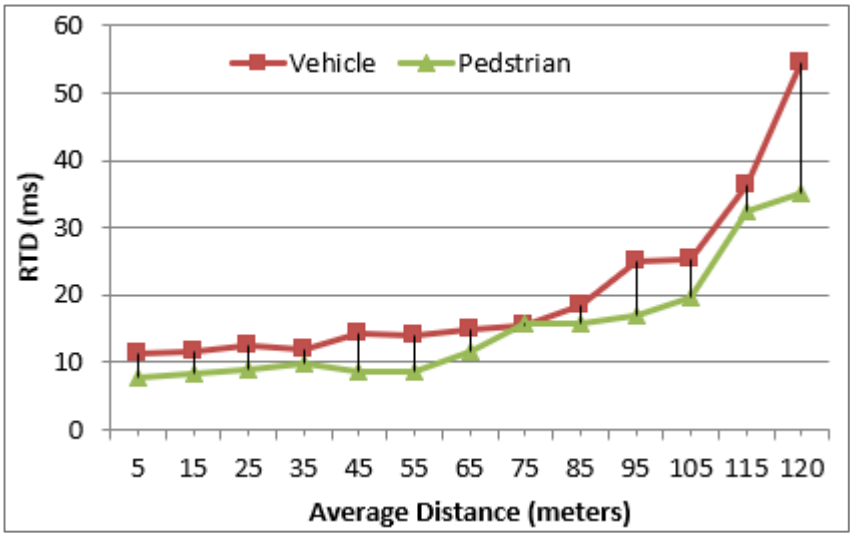
Figure 3.5: Simulation scenario[2]

3.4.3. RESULTS AND DISCUSSIONS

As mentioned before, the system is evaluated for both Wi-Fi (results shown in figures Figure 3.6 and Figure 3.7) and LTE (results shown in figures Figure 3.8 and Figure 3.9).

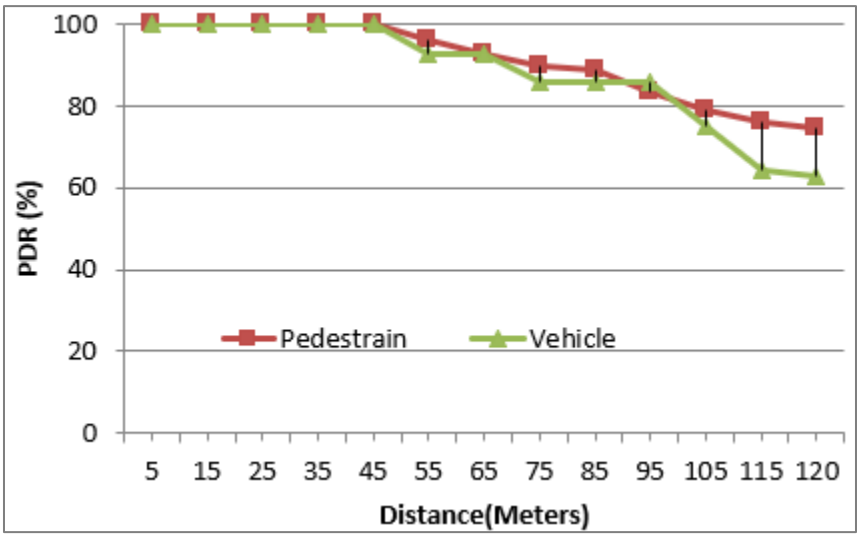
Figure3.6. a) shows how the delay is impacted by the distance between fog server and pedestrians or vehicles. We can notice that the RTD of both pedestrians and vehicles is under the maximum latency time (100ms) set by ETSI [59]. The difference between the two is due to their speed since slow-moving objects will have more chance to access the channel than faster ones.

Packet delivery ratio is also affected by the distance between the fog server and road users as well as speed, as shown in Figure 3.6. b). More than 80% of the packets sent are received as long as the distance of mobile devices is not more than 100m. Signal attenuation is the main reason for the dropping of PDR when the distance exceeds 100m.



[2]Smaller dots in the figure represents pedestrians

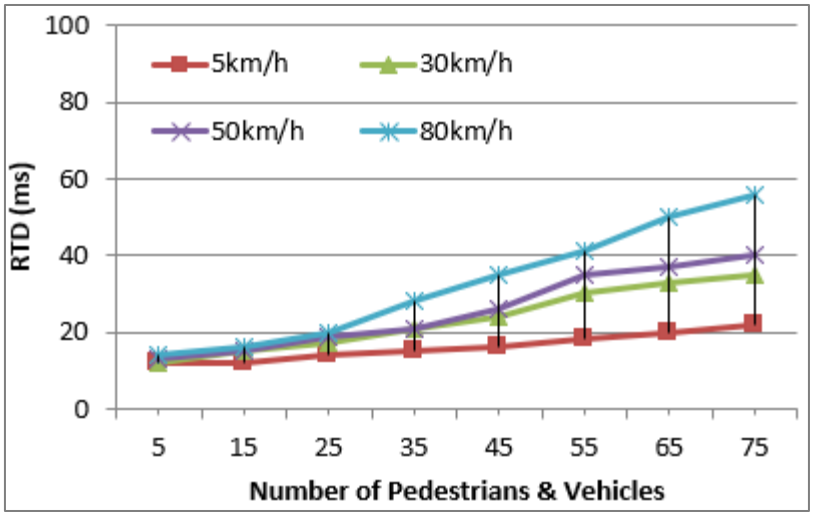
a)



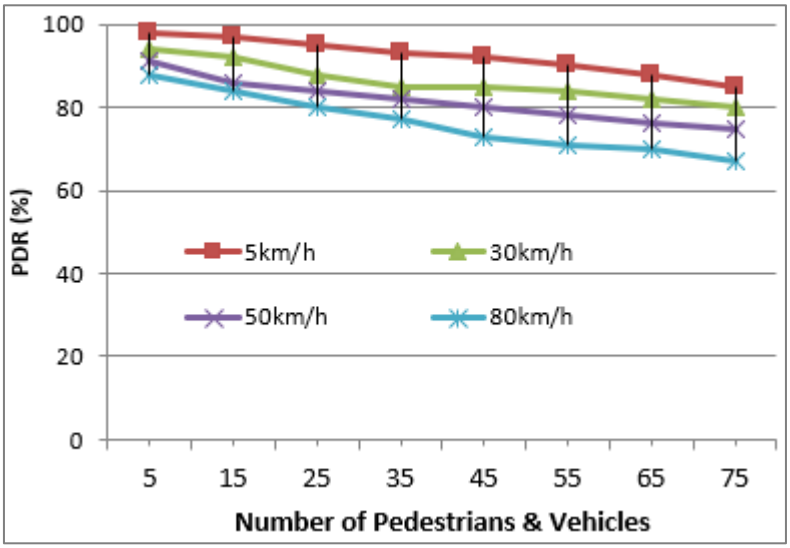
b)

Figure 3.6: RTD and PDR vs. Distance (Wi-Fi connection with the Fog node)

Figure 3.7 depicts the evaluation results of delay and PDR when the number of road users increase (of which approximately 50% pedestrians and 50% vehicles) and by varying the vehicles' speed to 30km/h, 50km/h, and 80km/h. As shown in Figure 3.7 a), the RTD increases as the number of road users and their speed increase, but the delay is still below the maximum expected latency time. The increase is due to the interference and congestion as multiple nodes contend to access the same medium. In Figure 3.7. b), we varied the vehicles' speed and raised the number of pedestrians and vehicles. For slow moving vehicles (30km/h), and pedestrians (5km/h) more than 80% PDR is well achieved till the number of nodes reach 70. However, PDR for fast-moving vehicles is low if the number of nodes exceeds 25. This is because fast-moving vehicles have less access to the medium and due to packet losses owing to interference. The results confirm that Wi-Fi has better performance in sparse networks, and it has limited mobility support [155].



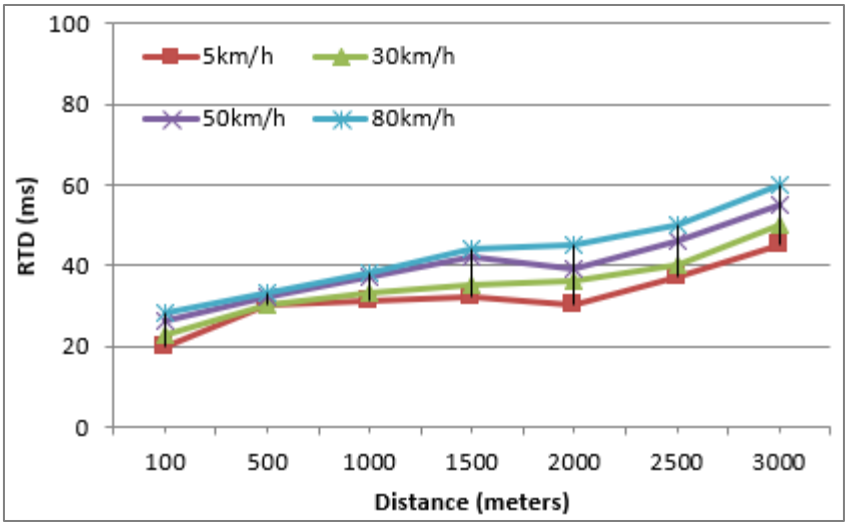
a)



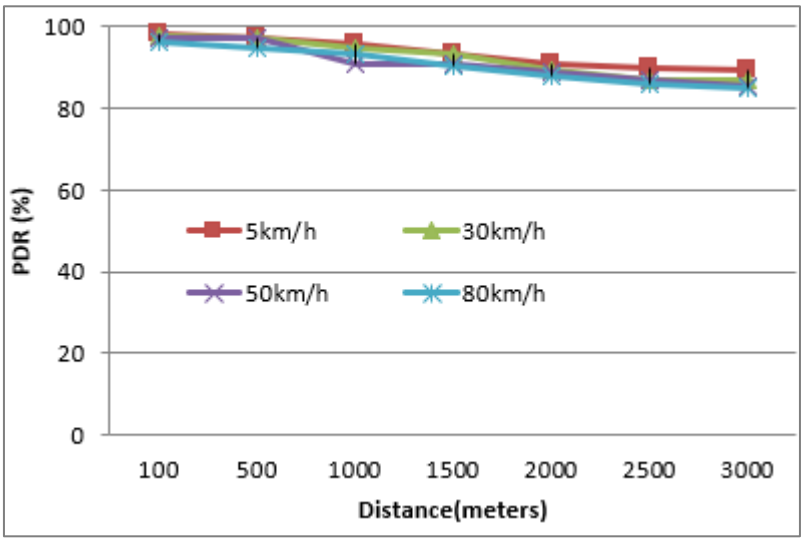
b)

Figure 3.7: RTD and PDR vs. Number of Vehicles and Pedestrians (Wi-Fi connection with the Fog node)

Experimental results of RTD and PDR when an LTE connection is used by smartphones to communicate with the fog node is given in Figure 3.8 and Figure 3.9. Round trip time delay increases from 20ms to 60ms as the nodes move away from the fog node, as shown in Figure 3.8 a). The delay fulfills the application requirement and we can notice that the difference between fast-moving vehicles and slow-moving vehicles is not significant due to high mobility support of LTE [155], [156]. The same is true for the PDR as shown in Figure 3.8 b); PDR exceeds 80% for all distances and the difference among vehicles moving at different speeds is insignificant. However, there is a minor decrease in PDR as speed and distance increase.



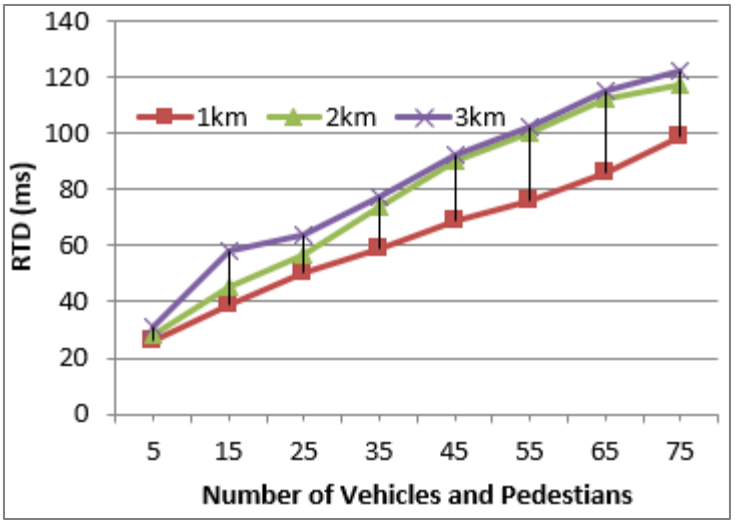
a)



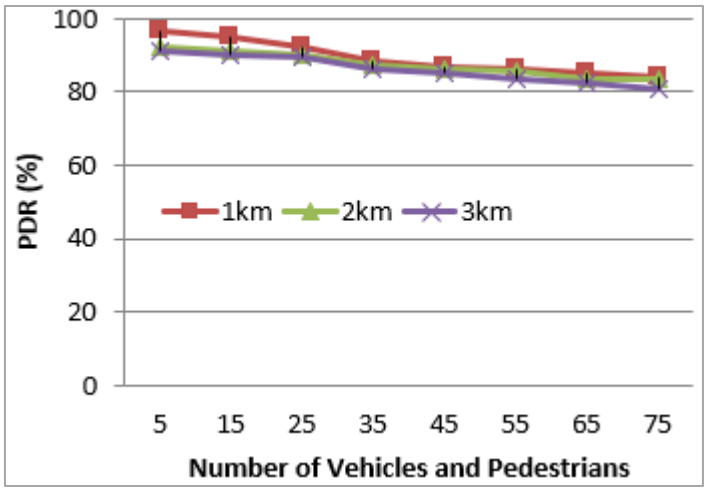
b)

Figure 3.8: RTD and PDR vs. Distance (LTE connection with the Fog node)

Figure 3.9 shows the impact of the number of vehicles and pedestrians on delay and packet delivery ratio at different distances. Due to the high mobility support of LTE, we have observed that the speed does not significantly impact on the delay and PDR. Therefore, the experiments are realized for different average distances and velocity of vehicles that does not exceed 80km/h in urban scenarios. At average distance of 1km, all delays of nodes are below the threshold value. However, as vehicles' and pedestrians' an average distance increase (2km and then 3km), the delay increases due to signal attenuation combined with network congestion. In Figure 3.9 a), if the number of vehicles is 55 or below, the system satisfies delay requirement at any distance. PDR is more affected by the number of nodes than distance, as depicted in Figure 3.9 b). The average PDR of uplink and downlink is above 80% for all the distances, though it gradually decreases as the number of nodes increases. Moreover, we have noticed that downlink PDR is higher than uplink due to downlink's higher bandwidth.



a)



b)

Figure 3.9: RTD and PDR vs. Number of Vehicles and Pedestrians (LTE connection with the Fog node)

From the simulation results, we conclude that the proposed fog-based architecture, PV-Alert, meets the constraints fixed by ETSI for safety applications regardless of the wireless communication technology (Wi-Fi or LTE) used between fog server and smartphones.

3.5/ CONCLUSIONS

High volumes of pedestrians, cyclists, and other VRUs have much higher casualty rates per mile; this is not surprising given their lack of protection from an accident. To alleviate the problem, we have proposed an architecture that exploits enabling features of the new computing paradigm named fog computing and the sensing capabilities of mobile devices to detect, warn, and safeguard the road users. Fog computing is a promising solution for problems that require low latency, high geographical distribution, high mobility support, location awareness, etc. In the proposed architecture (i.e. PV-Alert) VRUs are connected to fog servers using wireless transmission media through their smartphones to send

geographical awareness information to the servers and to receive warning messages in case of an imminent traffic accident. Collision risks are estimated using VRU collision prediction algorithm installed in fog servers. Analytical and performance comparisons of the architecture to other smartphone-based VRU safety architectures based on the criteria we defined shows that it has high scalability, reliability, and low latency. Moreover, the simulation results show that the proposed architecture is able to render alerts in real time whichever the wireless communication technology (Wi-Fi or LTE) used to connect the smartphones with fog nodes. That is, it can meet the maximum latency requirement enacted by ETSI for collision warning systems and the packet delivery ratio requirement of safety critical systems. The solution can be deployed quickly since it depends only on users' smartphones and doesn't require special infrastructure except for existing fog computing environment. Therefore, we conclude that fog computing is a feasible solution to safeguard connected VRUs from traffic accidents.

However, smartphones GPS fixes accuracy, high energy consumption, high position sampling period, as well as privacy and security issues in relation to fog computing, need to be addressed before deploying the application in the real environment. Chapter 4 discusses the solution proposed to improve the accuracy of GPS position fixes of smartphones. Insufficiency of the sampling frequency of the mobile device is dealt with in chapter 5. Chapter 6 explains the solutions proposed to tackle high energy consumption of mobile devices while using them for traffic safety. Data security and user privacy issues introduced due to fog computing are addressed using a two-way subjective logic-based trust management system, which is explained in chapter 7.

4

PV-ALERT: MEETING POSITION ACCURACY REQUIREMENT

4.1/ INTRODUCTION AND PROBLEM STATEMENT

The number of mobile device users is increasing from year to year due to their reduced price [11], [12]. The high penetration rate of the handheld devices and their increased capabilities to sense, compute, store, and communicate have made the devices important components of many applications. The mobile devices are equipped with GPS chipsets, multiple sensors, high storage capacities, fast processors, and multiple wireless communication interfaces. In light of this, mobile devices have become vital for location-based services to offer directions, targeted recommendations, or other location-specific information. Location data obtained from smartphones' GPS and motion sensors could also be used for ITS applications. In chapter 3, a fog-based active safety architecture to safeguard pedestrians and two-wheelers from traffic accidents is proposed. PV-Alert depends on GPS locations obtained from the mobile devices of drivers and VRUs [56].

Various other works in literature has investigated the potential of using smartphones as mobile sensors for active safety systems to protect VRUs [15], [61], [157], [158]. However, according to [15], GPS locations obtained from smartphones have 4.68m longitudinal and 6.83m latitudinal accuracy on average, and according to [61] the median horizontal error locations are found to be between 5.0m and 8.5m on average. These values are not sufficient for traffic safety applications. The experiments we conducted in urban and rural areas in different environment conditions also confirm this. In fact, there are several factors like weather conditions, obstructions, noise, and interferences that result in an inaccuracy of GPS readings by delaying GPS radio signals [159].

Attaching external GPS receivers like GNSS antenna to mobile devices enables to obtain centimeter accuracy [64]. But this will limit portability and create the devices usage inconvenience. Map matching is the most widely used techniques to correct the locations by matching to the road network. It is the process of correcting a sequence of real-world locations obtained from GPS readers by estimating the right road segments. Correlating the GPS points to road segments can be done either in post-processing mode or real-time mode [160]. Post-processing technique has complete knowledge of the user's

trajectory since actual mapping is performed after the user has completed his journey. It fits with non-time sensitive applications like mining historical trajectories of a large number of experienced taxi drivers to find the shortest routes between different origin-destination pairs at different times of day [160]. Real-time map matching, also named incremental or online map matching, involves assigning currently obtained user location immediately to the correct segment (hence its name). Real-time map matching is employed for applications that demand prompt alignment of user positions. Incremental map-matching algorithms have fast computation time, which usually trades with accuracy. The inaccuracy comes from the lack of global knowledge of the matching sequences [161]. However, the precision in online map matching can be soothed by adding constraints that lift the matching accuracy.

Map matching process employs various types of methods like Kalman filter, multiple hypothesis technique, chain code method, hidden Markova model, and fuzzy logic [160]. Dynamic Time Warping (DTW) algorithm, which involves measuring similarities between two time series sampled at equidistant points in time can also be used for map matching. The algorithm has been extensively applied in various disciplines including speech recognition, handwriting, and online signature matching, sign language and gestures recognition, etc. [162]. DTW is applicable only with the conditions that the complete sets of two time series are available. For applications which have incomplete time series, DTW needs to be adapted. Online Time Warping (OTW) is a modified version of DTW which is found by making several changes to align known time series with partially known ones in real-time [163].

In this chapter, we present a two-stage algorithm which performs incremental map matching to relate GPS points obtained from mobile devices of VRUs to a reference road segment. In the first stage, to improve the accuracy of matching by polishing outlier GPS points, Kalman filter is employed. In the second stage, OTW based map matching is applied to map GPS readings to reference data obtained from road networks using distance and direction difference similarity measures. Extensive evaluations have been made to assess the proposed algorithms in terms of accuracy and response time for three route trajectories of medium pedestrian walking distances.

The rest of the chapter is laid out as follows. Section 4.2 explains preliminary experiments made to check the accuracy of current smartphones, summarizes the literature on real-time map matching, and deals with the theoretical foundation of DTW and OTW. Section 4.3 discusses the proposed OTW based map matching algorithms. Evaluation setup and results are explained in section 4.4 and conclusions are given in section 4.5.

4.2/ BACKGROUND AND RELATED WORKS

An experiment conducted to evaluate accuracy of smartphones is presented, in this section. The purpose of the evaluation is to check if current smartphones are indeed inaccurate for traffic safety

applications. Then related works on map matching are discussed. Lastly, DTW and OTW are briefly introduced.

4.2.1. ACCURACY OF SMARTPHONES GPS READINGS

Results from early researches [15], [61] have shown that GPS readings have insufficient accuracy for location-based safety critical applications. We also have conducted an experiment to assess the accuracy of GPS read by present-day smartphones according to known geographical areas and under various reception conditions. We used an Android smartphone equipped with GPS on-board sensor, PC for recording exact positions from high precision real-time kinematics (RTK) receiver and a tape measure for measuring ground distances. The GPS readings are taken from an urban area which is surrounded by buildings and trees and relatively plain rural area in Nevers, France in two different weather conditions (sunny and cloudy days).

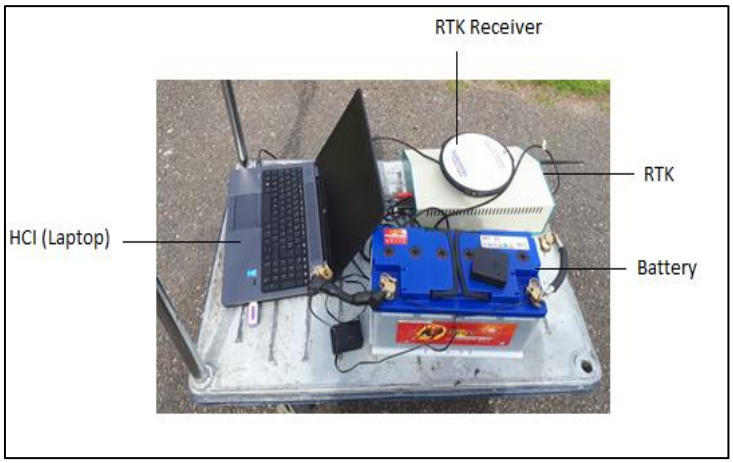
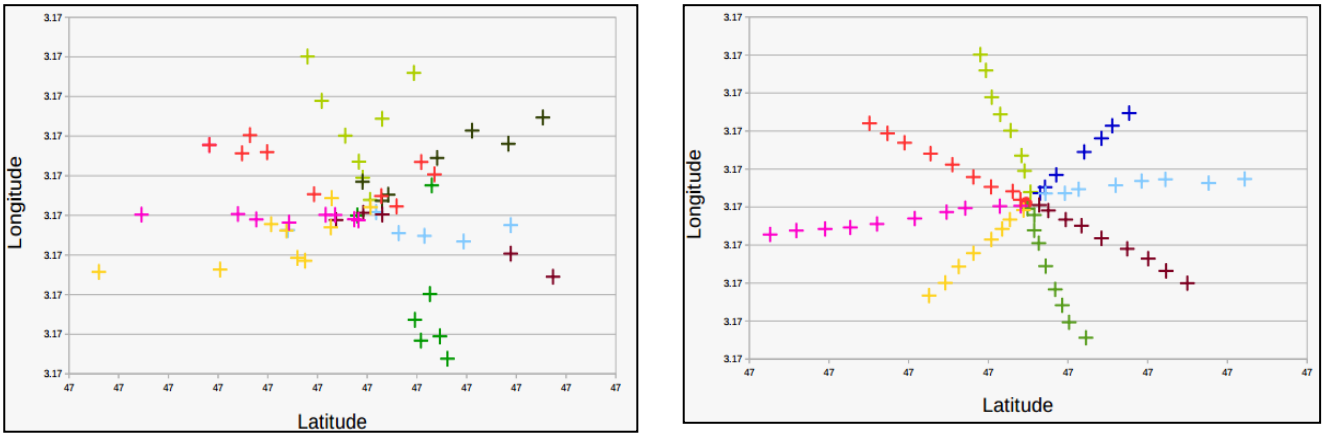


Figure 4.1: RTK receiver and associated equipment used in the experiment



a) b)

Figure 4.2: GPS readings for sunny day on urban area with a) Smartphone and b) RTK

During the measurement process, the RTK receiver's antenna was kept two meters above the ground to get accurate measurements. The mobile device used to get GPS readings is a Samsung, Model M-A520F. For each weather condition and area pair, we have taken 72 measurements starting from a center in eight different directions, each differing in 45°, at a 1-meter distance and then adding 3m to each of the previous measurements. The RTK and other equipment used, and the measurement results are shown in Figure 4.1. Smartphone and RTK readings for an urban area on a sunny day are displayed in Figure 4.2 a) and b), respectively.

TABLE 4.1 summarizes results of the measurements. The measurements taken on a sunny day in a rural area are most accurate and those taken on a cloudy day in an urban area are the least accurate. From the experiment, we can conclude that GPS readings obtained from the mobile devices have insufficient accuracy for traffic safety systems. Moreover, we have found that the readings are scattered, see Figure 4.2 a). So, smoothing the readings and improving the accuracy of locations to precisely predict and avoid traffic accidents is mandatory.

TABLE 4.1. GPS ACCURACY OF A SMARTPHONE AT DIFFERENT CONDITIONS

	Rural	**Urban**
Sunny Day	2 to 3 meters	2 to 6 meters
Cloudy Day	2 to 7 meters	3 to 9 meters

4.2.2. RELATED WORKS ON MAP MATCHING

Many ITS applications depend on location information obtained from mobile devices. Fleet management, route optimization, accident warning, and reporting are some of such applications [164]. Depending on the application, location accuracy and sampling frequency requirements, and even the type of location method may be different. Traffic safety applications require high accuracy and sampling rate. Though GPS readings of smartphones necessitate improvements, they can be used for safety applications. One way to improve GPS accuracy of the mobile devices is by using map matching.

Map matching algorithms take location readings from GPS or inertial sensors as input and identify the right road segment where the readings should belong. Various researches on map matching have been reported, and a detailed review can be obtained from [160] and [165]. Most of the researches reported on map matching are conducted for vehicular navigation systems. However, there are still some studies on VRU navigation systems, especially for pedestrians. These studies used various techniques starting from integrating GPS with other auxiliary techniques to advanced map matching to correct pedestrian locations. As per [166], correction of Dead Reckoning (DR) parameters, heading and step size, have improved DR-only based location accuracy. Their method is able to further increase the positioning accuracy when GPS signals are available. Different filters to GPS locations obtained from

inexpensive consumer-grade GPS receiver connected to a personal digital assistant is applied in [167]. Among the filters considered, map matching filter can significantly reduce GPS errors.

Ren et al. [168], in their successive studies, utilized various techniques for wheelchair and pedestrian navigation. They presented an efficient chain-code based map matching that looks at the trajectory of the data in addition to the current position [169]. A hidden-Markov model-based map matching algorithm proposed in [170] was able to outperform the chain-code based method in terms of correct segment identification. Fuzzy logic-based map matching is presented again by Ren et al., [171] to yield numerically accurate output from readings gathered in an urban environment. The algorithms just mentioned were tested in the sidewalk network on a university campus. In other recent researches, 3D map matching algorithms are proposed for urban canyon area [172], [173].

Most map matching algorithms presented in literature work in post-processing mode. However, there are still some real-time processing map matching algorithms [166], [174]. Bang et al. [174] reiterated how complex and detailed pedestrian network data are in comparison to vehicular datasets and presented a real-time pedestrian navigation system based on the Fréchet distance approach. The method was able to perform better than known vehicle map matching algorithms for the test data probed.

OTW is another approach that can be used for the map matching process. The approach is originated from DTW. DTW is an algorithm which is used to measure similarities between two time series. DTW is applied for pedestrian positioning using network map [175], but it performs in post-processing mode. The implementation of OTW algorithms in the area of live tracking of musical performance [163] and in streaming time series setting [176] have shown its efficiency and flexibility. To the best of our knowledge, this is the first work to propose OTW for location-based real-time map matching.

Dynamic Time Warping (DTW)

DTW is a time series matching technique that takes two time series and finds an optimal alignment between the two sequences under some restrictions [177], [178]. That is, given two time series $R = (r_1, r_2, \dots, r_N)$ of length $N \in \mathbb{N}$ and $G = (g_1, g_2, \dots, g_M)$ of length $M \in \mathbb{N}$, DTW compares the two series and gives optimal mapping among the values of R and G. Figure 4.3 illustrates the warping or alignment.

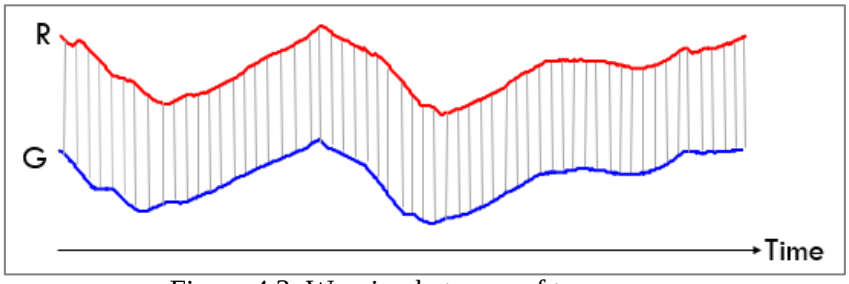


Figure 4.3: Warping between of two sequences

Suppose, the two sequences are taking values from feature space denoted by $\mathcal{Y}$. To compare the values of the two sequences, local cost measured has to be computed using equation 4.1:

$$\mathrm{d}: \mathcal{Y} \mathrm{X} \mathcal{Y} \rightarrow \mathbb{R} \geq 0 \tag{4.1}$$

Basically, d (r, g) measures the similarity between r$\in$ R and g$\in$ G, and it is small if the two values are similar and high otherwise. Computation of these measures using equation 4.2 for all pairs of values of the two sequences results in the local cost matrix.

$$d(r_i, g_j) = ||r_i - g_j|| \; ; \; \mathrm{i} \in [1 : \mathrm{N}]; \; \mathrm{j} \in [1 : \mathrm{M}] \tag{4.2}$$

The actual mapping is done using optimal global cost matrix D, which is calculated recursively using equation 4.3.

$$D\left(r_i, g_j\right) = d\left(r_i, g_j\right) + \min\{D\left(r_i, g_{j-1}\right), D\left(r_{i-1}, g_j\right), D\left(r_{i-1}, g_{j-1}\right)\} \tag{4.3}$$

After the optimal global cost matrix is populated, then, the next step is to find an alignment between R and G with minimal overall cost. This alignment path which is formally called warping path contains the sequence of points $p = (p_1, p_2, \ldots, p_k)$ with $p_1 = d(p_i, p_j) \in [1 : N] \times [1 : M]$ for $l \in [1 : K]$. The warping path must satisfy the following three restrictions:

- *Boundary Condition*: It must map the first two and the last two values of the sequences. That is $p_1 = (1, 1)$ and $p_k = (N, M)$.
- *Monotonicity condition:* The points must be time ordered. That is $n_1 \leq n_2 \leq \ldots \leq n_L$ & $m_1 \leq m_2 \leq \ldots \leq m_L$.
- *Step size condition:* The warping path cannot jump while aligning sequences. For any two consecutive points on warping path their positive difference must be (1, 1), (1, 0), or (0, 1).

Keeping the restrictions mentioned above, to find an optimal warping path, the sum of costs of all paths from $p_1 = (1, 1)$ to $p_l = (N, M)$ is computed and the one with minimum value is selected. However, this is computationally very costly, especially when the length of the two series is very large. Nevertheless, by applying dynamic programming, it can be figured out with the complexity of O (N.M). The algorithm runs recursively in reverse order starting from $p_k = (N, M)$ and stops in case (n, m) = (1, 1). There are plenty of modifications of DTW for various objectives. Improving response time and the accuracy of maping are examples of the objectives. Some are step size condition modification, biasing to a direction, applying global constraints and approximation [179], [180], [181], [182].

Online Time Warping (OTW)

OTW was introduced by Simon Dixon in [163] to align audio signals because of the inconvenience of DTW for real-time alignment. OTW acts on an incomplete time series (boundary condition doesn't hold), and the alignment is built incrementally starting from $p_{l+1} = (1, 1)$ in the forward direction as a value is read for incomplete time series, see Figure 4.4.

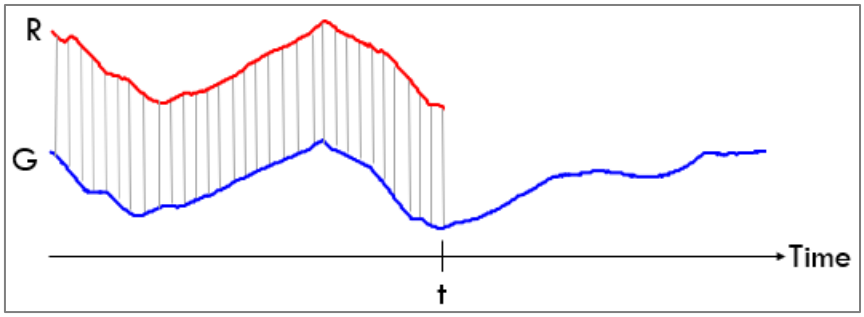


Figure 4.4: Online time warping of two sequences at time t. As the value of R is read at the next time, the warping is made accordingly

$$p_{l+1} = \min\{D(r_{i+1}, g_{j-1}), D(r_{i+1}, g_j), D(r_i, g_j)\} \quad (4.4)$$

Optimal warping path is computed using equation 4.4:

The algorithm is a greedy algorithm which has no global knowledge about the future. Just like DTW, OTW can be modified in different ways for better efficiency. The next section details the proposed two-stages algorithm composed of a smoothing GPS reading using Kalman filter and a map matching using the OTW algorithm.

4.3/ ONLINE TIME WARPING BASED MAP MATCHING ALGORITHM

The overall process of the algorithm is shown in Figure 4.5. The process starts with smoothing outlier GPS position readings by passing the readings to the Kalman filter. Then the improved points from pedestrian trajectory are mapped to points on ground truth trajectory using the OTW algorithm. The details of the processes are delineated underneath.

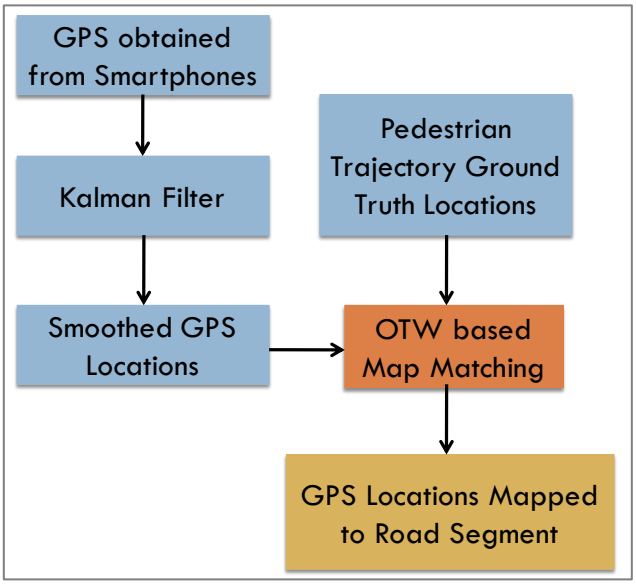


Figure 4.5: High level description of OTW based map matching algorithm.

4.3.1. 1ST STAGE: KALMAN FILTER

Kalman filter is a technique which takes a sequence of measures over time and previous estimations to find the most optimum averaging factor for each following state [183]. A simplified form of Kalman filter is expressed using equation 4.5.

$$Y_k = Y_{k-1} + K_k * (M_k - Y_{k-1}) \tag{4.5}$$

Where Y_k is the current estimation; K_k is Kalman gain; M_k is the measured value, and Y_{k-1} is the previous estimation. Kalman gain is an important parameter which determines whether to rely more on current measured value or previous estimation. At each step, Kalman gain is calculated by dividing error in estimate to the sum of errors in estimate and measurement. The technique has widespread applications in various areas, including GPS accuracy improvements [183], [184].

In this research, Kalman filter comes into action to smooth GPS read by smartphones by removing outliers to enhance matching accuracy of our algorithm. Android location providers give latitude, longitude as well as accuracy, among others. Even though a location can be represented by two numbers (latitude and longitude), instead of a covariance matrix, the accuracy in the Kalman filter can be measured by a single number. Hence, the new estimated latitude and longitude can be calculated using the set of Kalman filter-based formulas which are specified in a set of equations below.

$$\begin{aligned} Lat_t &= Lat_{t-1} + K * (Lat_m - Lat_{t-1}) \\ Lon_t &= Lon_{t-1} + K * (Lon_m - Lon_{t-1}) \\ K &= \frac{var}{var + acc^2} \\ var &= (1 - K) * var \end{aligned} \tag{4.6}$$

Where Lat_t and Lon_t are latitude and longitude estimate at time *t* respectively, while Lat_{t-1} and Lon_{t-1} are estimated at time *t-1*. Current measurements of latitude and longitude are represented by Lat_m and Lon_m. *K* is *Kalman gain* and *var* is variance, which evaluates the rate of accuracy degradation in the absence of any new location estimates and *acc* is the accuracy of GPS reading.

Figure 4.6: Smoothing of GPS reading by applying Kalman filter

The application of the above formulation of Kalman filter on a test data provided the output shown in Figure 4.6. The red line at the back are formed from the row outlier GPS readings and the blue line is made up of smoothed points. The matching accuracy of the algorithm improved by 12.59%.

4.3.2. 2ND STAGE: OTW ALGORITHM

A position obtained from GPS readers, and corrected using Kalman filter must be immediately mapped to correct road segment for reliable location service. OTW algorithm matches an incomplete set of location time series streamed from smartphones to the ground truth points extracted from the digital map. The feature spaces for OTW algorithm are the set of GPS readings expressed in terms of latitude and longitude. Local cost measure is great-circle distance calculated using the *Haversine formula*. The pseudo code of the main OTW algorithm is displayed in Algorithm 4.1, while TABLE 4.2 shows notations used in the algorithms.

OTW has two main steps - calculating the optimal global cost matrix for newly read GPS (steps 4 to 8 of Algorithm 4.1) and conducting the matching process (steps 10 to 30 of Algorithm 4.1). Optimal global cost is calculated in the same way as DTW using equation 4.3 except in OTW it is filled immediately after each point is read and smoothed by Kalman filter. The incremental matching process is quite different from naïve DTW. First of all, the matching is done in forward fashion in real-time. Secondly, the algorithm has limited knowledge about the future global cost matrix.

TABLE 4.2. LIST OF NOTATIONS

Notation	Description
$R = \{r_1 \ldots r_r \ldots r_n\}$	A time series of length n
$G = \{g_1 \ldots g_g \ldots\}$	An incomplete time series with unknown length except the first g_g
CM[n][m]	An n x m cumulative cost matrix used in OTW
r	Index of R and row index of cumulative cost matrix
g	Index of G and column index of cumulative cost matrix
W[2][n+m]	A warping path Matrix
k	Index of warping path Matrix
$\delta(\ )$	Cost between points of time series
getMinimum (r, g)	A function that returns the best match based on distance and direction difference
▷	Represent a comment line

Algorithm 4.1: OTW Algorithm (free or unconstrained)

Inputs: *$R = \{r_1 ... r_r ... r_n\}$, $G = \{g_1 ... g_g ...\}$*
Output: *W[2][n+m] populated with the mappings*
Steps:

```
1. Function Compute_Unconstrained_OTW(R, G)
2.   While there are more GPS readings
3.     ▷calculates local cost matrix for newly read GPS
4.     for  i = 0 to n
5.       gps = read_GPS
6.       gps = apply Kalman on gps
7        CM[r][g] = δ( gps, R[r]) + min{CM[j-1][g-1], CM[j-1][g], CM[j][g-1]}
8.     end for
9.     ▷Conduct the matching
10.    If r=0
11.      W[0][k] = 1 and W[1][k] = 1
12.    else
13.       min = getMinimum(r, g)
14.      If min = CM[r+1][g]
15.         W[0][k] = r+1 and W[1][k] = g
16.      else If min = CM[r+1][g-1]
17.        W[0][k] = r + 1, W[1][k] = g – 1, r = r+1 and k = k+1
18.        While true
19.          min = getMinimum(r, g)
20.          If min = CM[r+1][g]
21.            W[0][k] = r + 1, W[1][k] = g and exit inner while
22.          else If min =CM[r][g]
23             W[0][k]= r, W[1][k]=g, r=r-1 and exit inner while
24.          else If min =CM[r+1/[g-1]
25.            W[0][k] = r + 1and W[1][k] = g -1
26.          end IF
27.        end While
28.      else
29.          W[0][k] = r and W[1][] = g;
30.      End IF
31.      r = r + 1, k = k + 1, and g = g + 1;
32.  end While
33. end function
```

Optimal path selection formula depicted in equation 4.4 is used to find the minimum among the three candidate points; vertical (*CM[r+1][g-1]*), diagonal (*CM[r+1][g]*) and horizontal (*CM[r][g]*) points, see Figure 4.7. To decide the final mapping, the direction of GPS trajectory of VRU is compared with direction of the reference points. If *getMinimum(r, g)* function, which integrates the two metrics returns either right or diagonal cell, current matching is made and the next GPS is awaited to repeat the whole process. If the vertical cell is returned, the matching process is done again, steps 16-27 of Algorithm 4.1.

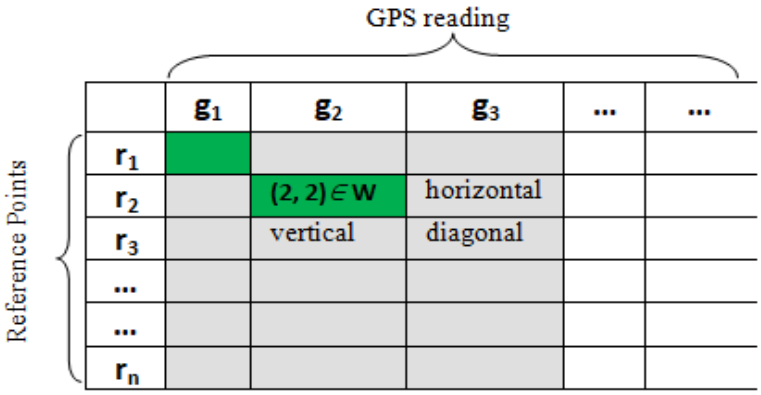


Figure 4.7: A snapshot of cost matrix of unconstrained/free OTW based mapping process. Suppose the algorithm has read g_3, and recently selected cell on warping path is (2, 2), then the next cell could be vertical (3, 2), horizontal (2, 3) or diagonal (3, 3).

If the reference point and a point on trajectory are in the same direction, then the direction difference will be between -90° and 90°. In this case, the mapping is done based on the result of distance. Otherwise, the next closest point is taken into attention, see Algorithm 4.2.

Algorithm 4.2: Get the best match (getMinimum*(r, g)* function)

Inputs

r, index value of reference datasets

g, index value of current GPS trajectory

Output:

Minimum of CM[r][g], CM[r+1][g], CM[r+1][g-1]

Steps:

```
1. function getMinimum(r, g)
2.    If angle_Difference(R[r+1], G[g-1]) ==[ -90, 90]
        and CM[r+1][g-1] == min{CM[r+1][g-1],
        CM[r+1][g], CM[r][g]}
3.      min = CM[r+1][g-1]
4.    Else If angle_Differnce (R[r], G[g])==[-90, 90] and
          CM[][g] == min{ CM[r+1][g], CM[r][g]}
5.        min = CM[r][g]
6.    Else
7.      min = CM[r+1][g]
8.   end IF
9. end function
```

Figure 4.8 shows the effect of direction on the choice of a non-closest point. Though point g_4 is closer in terms of distance to point r_4, the algorithm maps it to r_3 due to direction difference. This scenario happens when there are sharp turns, which are commonly observed in slow-moving VRUs.

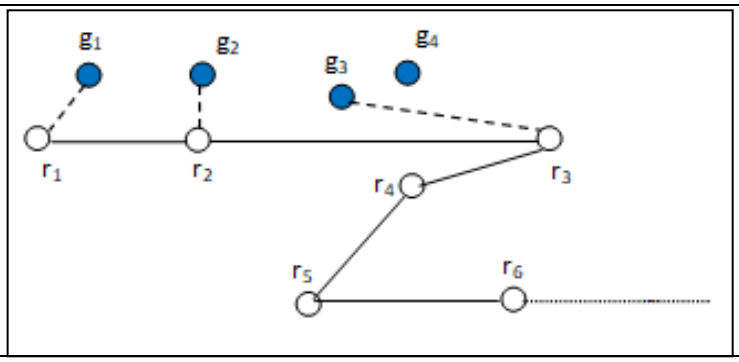


Figure 4.8: Effect of direction difference on selecting mapping points.

The blue shaded dotes are GPS readings from smartphones, while dots connected by lines are the reference points. The dotted lines indicate the mapping between GPS points and reference points.

4.3.3. VARIANTS OF OTW ALGORITHM

To reduce pathological matches and for a quick matching, free OTW can be modified in different ways. We have made three adjustments described which are: windowing, smoothing, and weighting.

1- OTW with Windowing: In this variant, the cost matrix is calculated only for the cells near the most recent cell on the warping path. in Figure 4.9, which shows cost matrix in the process of application of this algorithm, only shaded regions are considered in both cost matrix calculation and warping path computation.

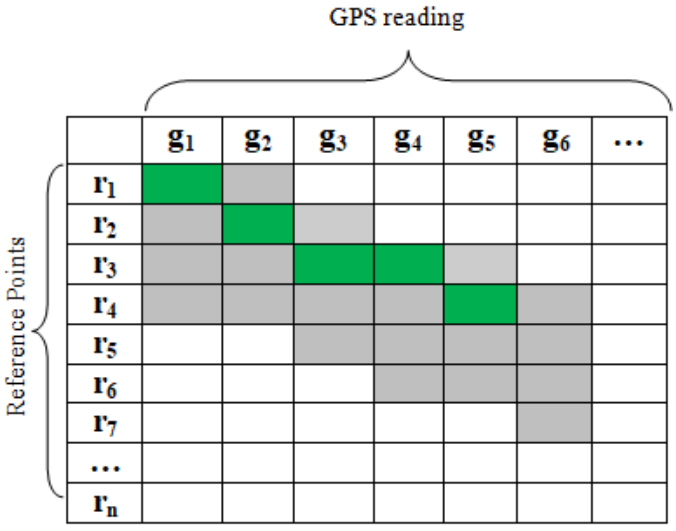


Figure 4.9: Cost matrix for OTW that has window size of 4 cells. Green colored cells are those included in warping path

2- OTW with Smoothing: Two approaches that can be taken to address greedy nature of OTW algorithms are making the alignment based on a limited view into the future if the application allows a certain amount of latency, and smoothing the sequence of alignment of points [163]. The first option is

not suitable for time sensitive applications. Smoothing applies normal DTW warping path computation in reverse order on the known section of the time series to correct the warping path periodically. It allows periodic correction of the warping path.

3- OTW with Weighting: Weighting refers to multiplying vertical, horizontal, or diagonal cell by some constants. Therefore, amending costing function stated in equation 4.3 gives the next one.

$$D\left(r_i, g_j\right) = d\left(r_i, g_j\right) + \min\{w_d * D\left(r_i, g_{j-1}\right), w_v * D\left(r_{i-1}, g_j\right), w_h * D\left(r_{i-1}, g_{j-1}\right)\} \quad (4.7)$$

Where, (w_d, w_v, w_h) refers to constants for diagonal, vertical, and horizontal biases. For non-biased DTW/OTW the biases are each equal to 1. These values can be changed whenever there is a need to penalize or favor movement in a particular direction. For instance, if the constants are changed to (1, 1.2, 1.2) the horizontal and vertical directions are penalized favoring diagonal movement.

4.4/ PERFORMANCE EVALUATION AND DISCUSSIONS

In this section we elaborate the data used to evaluate the algorithm, the metrics for evaluation and evaluation results.

4.4.1. DATA COLLECTION AND EVALUATION METRICS

The OTW algorithm proposed was tested using datasets taken from the suburban area of Bahir Dar city, Ethiopia. The 0.51km^2 area is usually crowded by mostly pedestrians due to the presence of bus stations and a university in a nearby. Ground truth datasets are obtained from OpenStreetMap [185]. The wiki world media is chosen because it is free and most popular web map source with acceptable positional accuracy [186], [187]. Three "short-range" routes with different level of complexity are chosen from the test site, and data collector with a Samsung mobile device (Model M-A520F) which reads GPS periodically walked along the center of the routes. The first route has only three turns while the second and third (is longer than route two) routes each have nine turns. TABLE 4.3 shows the details of the routes. Figure 4.10 displays the reference datasets together with the collected GPS datasets.

TABLE 4.3. DETAILS OF THE THREE ROUTES

Route ID	No. of GPS Points	Length (m)	Duration (s)	Average Speed (m/s)	Average Error (m)
Route 1	274	476.93	369.71	1.29	5.37
Route 2	453	780.52	696.89	1.12	7.89
Route 3	670	1194.22	884.61	1.35	6.01

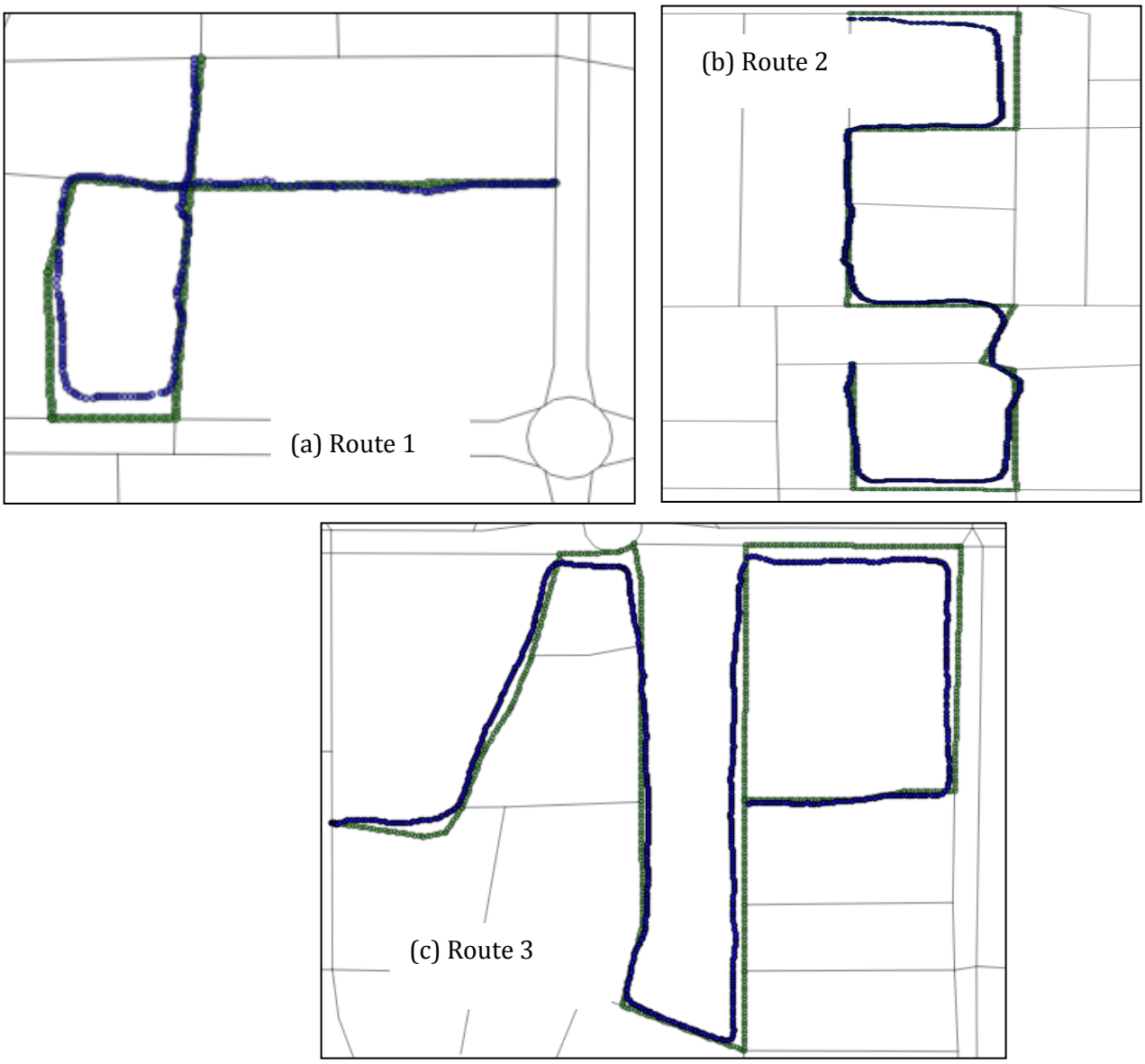


Figure 4.10: The three trajectories (blue) and corresponding ground truth datasets (green). The background lines are of the base map.

Two metrics are used to compare the performance of the algorithms using the datasets of the three trajectories.

- *Ratio of Correct Matches (RCM)* – is calculated by dividing the number of correct matches to total number of matched points. Wrong matches can be identified since we have ground truth map matching results which are computed based on Euclidian distance and heading of the GPS points manually taking into consideration the average error of each route once the complete dataset is obtained. The RCM is used to evaluate the accuracy of the map matching proposed.
- *Time Complexity* is the running time of the algorithms. It is evaluated in two different ways; running time in terms of Big O notation and empirical evaluation

4.4.2. PERFORMANCE RESULTS AND DISCUSSIONS

Free OTW is tested for Kalman filtered datasets (used by all other algorithms) and on raw datasets. For OTW with windowing, the window size is set to be 8% of the number of reference datasets and this size is proved to contain all points that could be read in the range of average error. OTW with weighting is used to slightly bias the warping path to diagonal by multiplying vertical and horizontal cells by 1.2 since the number of GPS points on the trajectory, and reference datasets are equal. For OTW with smoothing, we have configured our algorithm so that smoothing is performed after every fifteenth mappings. The values for windowing, weighting and smoothing can be varied based on the computation of the server that runs the algorithm and application requirements. As this algorithm is intended for VRU safety applications, we have applied point-to-point level map matching since position errors are first corrected by Kalman filter, and OTW algorithm is known to be fast.

As it can be seen in Figure 4.11, classical DTW has comparatively higher average accuracy for the selected routes though it is exceeded by OTW with weighting. OTW with windowing and the one with no constraints performed equally, as expected. Free OTW calculates cost matrix for all cells corresponding to the given GPS reading with no effect on accuracy. The application of free OTW on datasets which are not Kalman filtered depicts that Kalman filtering is indeed important since the worst RCM is recorded in this case. OTW algorithms that are amended by weighting and smoothing have better performance from other OTW variations.

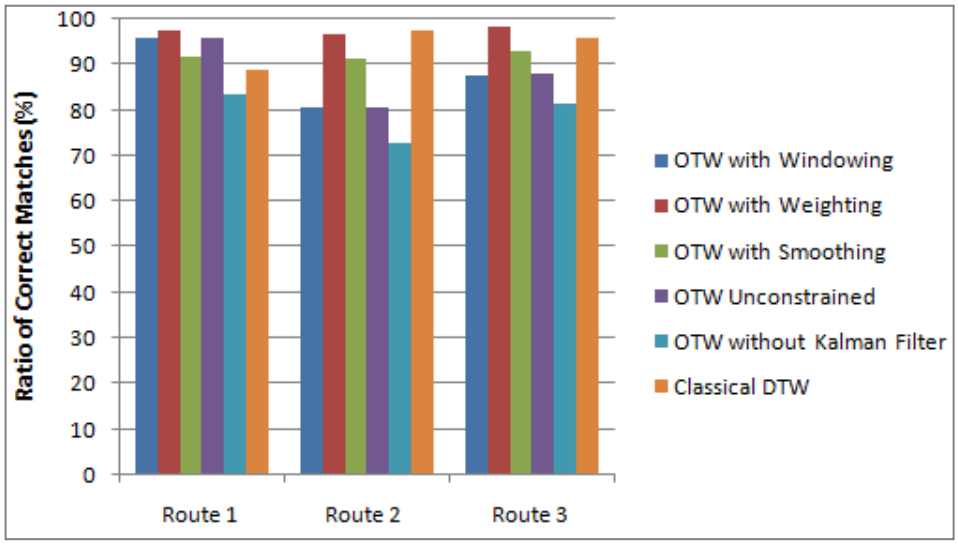


Figure4.11: Ratio of correct matches

Figure 4.12 shows the alignment for a section of Route 3 using DTW and OTW with weighting. DTW is susceptible to singularities [177]. Singularity is unreasonable alignments of a single point of one

time series to multiple points on the other time series, see encircled region in Figure 4.12 a). As it is shown in Figure 4.12 b), the application of OTW with weighting has reduced the problem.

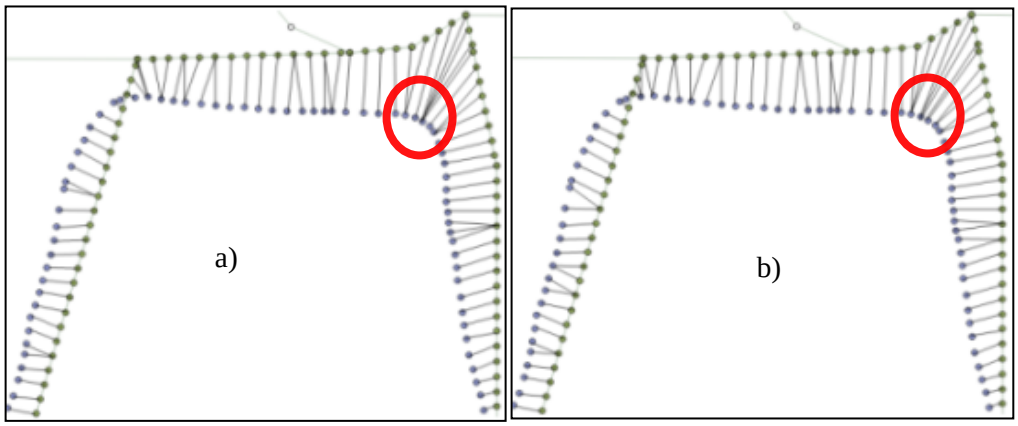


Figure 4.12: Comparison of alignment results found from (a) DTW and (b) OTW with weighting for portion of Route 3.

Running times of various algorithms where *n* and *m* are the number of trajectory and ground truth points are displayed in TABLE 4.4. OTW with windowing and weighting have constant complexity while free OTW and OTW that involves smoothing have linear running time. OTW with smoothing has the worst execution time if the smoothing is done every iteration. Classical DTW has quadratic execution time.

TABLE 4.4. BIG O NOTATIONS OF ALGORITHMS

OTW with				**Classical**
Window	***Weights***	***Smoothing***	***free***	**DTW**
O(1)	O(1)	O(n+m)	O(m)	O(n.m)

The proposed algorithms are implemented in Java and executed in a PC machine with an "Intel Core™ i7-6500U 2.50GHz" CPU. Empirical evaluation results are displayed in TABLE 4.5. To get a running time of the algorithms proposed, we ran each algorithm 1000 times for each dataset and recorded the average. All OTW algorithms except free OTW have very short average execution times, making them good candidates for real-time map matching. DTW is the slowest algorithm since the matching is done on complete datasets.

TABLE 4.5. ALGORITHMS EXECUTION TIME (MS)

Routes	**OTW with**				**Classical**
	Window	***Weights***	***Smoothing***	***free***	**DTW**
Route1	2.43	2.75	3.09	61.50	16574.72
Route 2	2.73	2.87	3.85	111.20	47225.87
Route 3	2.93	3.04	5.27	158.25	98065.04

4.5/ CONCLUSION

Nowadays, ITS rely on mobile devices due to their omnipresence, their high storage, and computational capacity, and their capability to sense users' positions. When smartphones are used for traffic safety applications, the positions sensed should be as accurate as possible to prevent traffic accidents. However, an experiment conducted by us, and the literature prove that GPS accuracy read by smartphones is limited. In this chapter, we have presented a new map matching algorithm that is based on online time warping to better map GPS read by smartphones of VRU to correct road networks. Online time warping, which is a special type of dynamic warping algorithm is used to align the two time series data in a real time.

Location data is first set to pass through Kalman filter to polish outlier readings. Then the online time warping based algorithm performs the matching process. Distance and direction differences are used to opt the matching point with reference points. That is a point nearest to reference point may not be selected as a match if the direction of the reference point and this point is not the same. Online time warping is presented in different forms by adding constraints like windowing, weighting, and smoothing. The algorithms are evaluated using a reference dataset obtained from a road network and a GPS reading collected using a smartphone. The ratio of correct matches and time complexity are the two metrics used for evaluation of the algorithms. The algorithms have better time complexity and comparable accuracy with standard dynamic warping algorithm. Therefore, we conclude that online time warping algorithm is a good candidate for applications that demand real-time map matching. PV-Alert is one of such applications.

The next chapter deals with position sampling frequency requirement of mobile devices to fulfill the promises of PV-Alert. Current mobile devices GPS position sampling rate is too sparse to meet the requirements of traffic safety applications. However, the problem is addressed by integrating inertial and GPS position data.

5

PV-ALERT: MEETING HIGH POSITION SAMPLING REQUIREMENT

5.1/ INTRODUCTION AND PROBLEM STATEMENT

Smartphones have become part of everyday life of human beings. They are used for gaming, navigation, monitoring environmental and traffic conditions, supervising the health of the owner, acting on our behalf, social networking, etc. [13], [188], [189]. In recent days, they have become important ingredients of ITS applications like traffic safety, infotainment, and traffic efficiency due to their wide existence and increased capability. An overwhelming increase in their computation, storage, and networking capabilities are further enhanced by their sensing potential, which is another feature that makes the devices more intelligent, and essential part of our life.

Though the number of sensors may vary from one smartphone to the other, typical smartphone contains an accelerometer, a digital compass, a gyroscope, a GPS, quad microphones, dual cameras, near-field communication, a barometer, light, proximity, and temperature sensors [13]. However, handheld devices are far from becoming apotheosis sensing devices. Producers of the devices purposefully make them compact and small so that they can fulfill user preferences more cheaply. Size reduction and subjection of the devices to non-ideal environments compromise the sensor accuracy and reliability highly, and this has become a hindrance to fulfill requirements of many applications. For instance, ETSI has enacted the maximum and the minimum time interval between beacon generations to be 1s and 0.1s, respectively for collision risk warning systems [59]. This implies that position sampling frequency should be 10Hz since location information is an integral part of CAM. Even though smartphone-based solutions are proposed for traffic safety by warning the about-to-occur collisions based on positions of vehicles and VRUs [54], [56], present mobiles devices' position sampling rate does not meet the maximum positions sampling frequency.

The maximum GPS sampling rate of mobile devices depend on factors like the location method, hardware implementation of the GPS module, the embedded GPS chipset, as well as the version and type of the operating system. A research conducted by Zhizhong et al., in 2013 [16] has indicated that maximum GPS sampling rate of smartphones is 1Hz [16]. We also conducted an experiment to verify

that the modern smartphones could meet high GPS sampling requirements of traffic safety applications. The experiment is discussed in the next couple of paragraphs.

The location methods supported by current android smartphones are: (i) Assisted-GPS (A-GPS), (ii) GPS only, and (iii) network (Wi-Fi and Mobile Internet). A-GPS, which is also termed high accuracy location method, uses GPS chip, and Wi-Fi, or cellular networks to accelerate the first fix acquisition. GPS only location method uses solely GPS chips and network location methods may depend on Wi-Fi, or cellular Internet connection. During the experiment, all applications, except the application for the experiment, were denied location access, and the mobile device was set to run only the default manufacturer processes. A Samsung smartphone (Model-SM-A520F) was used exclusively for this controlled experiment. An Android application was developed, which can read smartphone location at the highest possible frequency. By enabling each location methods turn by turn, the experiments were conducted in indoor and outdoor environments. Keeping the smartphone with the application running on front jacket pocket, one of the researchers walked for about an hour for each experiment. The application saves the following location data in a log file: system timestamp, latitude, longitude, accuracy, bearing, and speed. The average sampling period and the standard deviation of the values are presented in TABLE 5.1.

TABLE 5.1. AVERAGE LOCATION SAMPLING PERIOD OF DIFFERENT LOCATION METHODS

Location Method	Sampling Period (ms)	Standard Deviation
GPS-only	1003.84	108.97
A-GPS	1281.28	526.72
Mobile Internet	20521.42	975.30
Wi-Fi	20178 .13	1007.98

Even though the minimum GPS fix time is not meet by any of the location methods, the highest average GPS fix time interval is achieved by GPS only location system. Using this location method location updates can be obtained approximately every second. This value confirms the result obtained in [16]. Location obtained from mobile internet and Wi-Fi-based location methods' is too sparse for traffic safety applications. This is attributed to the low accuracy of network location method and slow movement of pedestrians since Android reports a new location if the new location fix is different from the last known location. A-GPS sampling rate is lower than GPS-only based location method as it uses network location methods when GPS fixes are not possible. The experiment reveals that GPS sampling rates of current smartphones do not satisfy the application requirement of traffic collision risk warning systems. Thus, location methods that can provide positions at higher rates should work together with GPS based location to meet high rate location demand of traffic safety applications.

Losses in connections and imperfect behavior of the data collection application further increase the sparseness of location data obtained from smartphones [189]. From these facts, it can be deduced that location updates of smartphones do not meet applications requirements of traffic safety systems. This is because pedestrians with maximum walking speed of 1.83m/s and running speed of 4.2m/s [41] could face traffic accidents in the time interval between two consecutive locations updates. Since vehicles' impact velocity could reach up to 80 km/h [190], the assertion is acceptable. Therefore, to keep mobile devices' involvement for traffic safety, a solution that uses inertial sensors to predict positions in case of unavailability of GPS location fixes is proposed. The method integrates GPS and low-cost inertial sensors to meet applications that require high position sampling.

Inertial sensors can be used to pinpoint the position of mobile device holders without the assistance of any external measurements like radios [191]. It is possible to extrapolate locations from reference points by calculating the travelled distance and direction of movement from inertial sensors data. INS sensors data can be sampled at a much higher frequency than a GPS sensor. However, high sampling rates of INS and GPS sensors are known to drain smartphone batteries rapidly. Therefore, applications that demand fast position sampling must address the issue of energy consumption in order not to exacerbate energy hungriness of mobile devices. This can be done by a slacked sampling of GPS and INS sensors data instead of sampling them at their fastest possible time. However, caution has to be taken not to harm the accuracy of position prediction by reducing the number of data points for estimation.

This chapter presents an energy efficient DR method proposed to estimate locations of VRUs, and particularly pedestrians. The novel INS and GPS sensors data fusion method enables to cope with high location sampling rate demands of traffic safety applications. Data are obtained from mobile devices of road users. The method doesn't depend on map information or movement history of pedestrians. It involves the estimation of displacement by using conventional kinematic equations from the distance and velocity of the pedestrian. GPS readings are used to correct dead reckoning parameters periodically in addition to serving as correct positions of pedestrian trajectory. Accelerometer and magnetometer are used to estimate the attitude of movement of the pedestrian. Intermediate positions estimated from displacement and heading are set to pass through Kalman filter for further improvement of the positions. The proposed position prediction method is applied to sampling rates which contributes to smartphones energy efficiency. The results show that with a small compromise of accuracy, a large amount of energy can be gained by relaxing sampling period of only INS sensors. This is because sparsening GPS positions is found to profoundly damage the position accuracy with very small energy gain.

The rest of the chapter is organized as follows. Section 5.2 summarizes related works in INS based dead reckoning and energy efficiency. Section 5.3 presents the details the implementation of the position prediction method. Section 5.4 is dedicated to discussions of the evaluation results made on the

proposed algorithm and energy efficiency of different GPS and INS data sampling rates. Finally, the conclusion is presented in section 5.5.

5.2/ RELATED WORKS

Traffic safety applications necessitate high rate position sampling to safeguard pedestrians and other VRUs from traffic accidents. Though mobile devices have been recommended for traffic safety applications as sources of geolocation of VRUs [54], [55], [56], [77], their position sampling rate is limited. Therefore, in situations when GPS reading is unavailable, or its accuracy is highly degraded, VRUs position must be dead reckoned using supplementary positioning systems. DR can be applied either in an offline mode [192], or in an online mode [193] based on the type of applications. Offline DR is used for post-processing of locations after collecting known locations. Online DR is suitable for real-time systems since estimation should be made immediately after a known location is captured. Most position estimation solutions proposed are either for vehicular navigation [193], [194], or for indoor pedestrian navigation [192], [195], [196]. To extrapolate the next positions from known GPS locations for VRU traffic safety, an online DR that can be applied in indoor or outdoor environments is required.

Some reasons for applying position prediction methods in navigation are related to energy saving by lowering sensor data sampling, absence of GPS location signals, and the need to improve location accuracy. Outdoor navigation systems that are used in open sky scenarios can use GPS based locations. However, to reduce smartphone energy consumption by lowering GPS sampling rate, GPS based localization can be supplemented by dead reckoning that involves low energy cost sensors [192], [193], [197]. INS sensors help to improve positioning reliability in situations where GPS location is not available due to obstruction of GPS satellites by high buildings, trees, etc. INS can also be integrated with GPS for best location accuracy [194] as both methods suffer from their own drawbacks. According to Zengshan Tian et al. in [198], navigation information obtained from the INS sensors is boasted with continuity, high data-updating rate, good short-term accuracy, and stability. INS sensors, in their research, are used to supplement GPS based positioning to fulfill higher location sampling rate requirements than the current mobile devices can support. The experiment they conducted has proved that the maximum GPS sampling rate is 1Hz, which is below the maximum sampling frequency enacted by ETSI. As mentioned earlier the same result is obtained by another group of researchers [16] and by the experiment we have conducted. The results of the test made on DR [198] shows that the accurate, reliable, and continuous localization and tracking can be provided. However, the DR relies on step detection and stride length estimation.

To predict position, the distance travelled, and the direction of movement needs to be known. Most dead reckoning solutions use an accelerometer to predict displacement by first detecting step events and estimating stride length [65], [195], [199]. A direction of movement is usually estimated from

magnetometer and gyroscope data, and position prediction is made after one or more strides. For applications that require very fast position predictions, multiple estimations must be made in a period of one stride. Therefore, step detection and stride length estimation-based position prediction do not fit for such applications.

Gathering GPS and INS sensor data at high data-updating rates is an energy-hungry process [16], [68], [69], [70], [71]. In [69] and [70], the authors have shown that sampling GPS at different sampling periods impact energy consumption. According to [16] and [68] normal INS data sampling consumes lesser battery power than fastest sampling. The energy hungriness of the different GPS and INS data samplings are at a very small sampling period is studied. The application of the position prediction method proposed on sensor data obtained by energy-efficient sampling periods demonstrates that a significant amount of energy can be saved with small effect on the accuracy of prediction. TABLE 5.2 summarizes some INS-based position prediction methods proposed in literature.

TABLE 5.2. EXAMPLE INS SENSOR BASED POSITION PREDICTION METHODS

Reference	Sensors Used	Prediction Basis	Proposed for	Indoor or Outdoor?	Reason for Prediction	Energy Efficient?
[192]	Accelerometer, Gyroscopes	Distance and direction	Pedestrian	Indoor	Absence of GPS Signals	No
[193]	Accelerometer, Magnetometer, GPS	Distance and direction	Vehicles	Outdoor	Energy Saving	Yes
[194]	GPS, Wheel Odometer, Compass, Gyroscopes, Accelerometer	Distance and direction	Vehicles	Outdoor	Location Accuracy Improvement	No (no mobile)
[200]	Magnetometer, Proximity sensor, Gyroscopes, Light Sensor, Accelerometer, Wireless connection	step events & stride length	Pedestrian	Outdoor	Location Accuracy Improvement	No
[195]	Accelerometer, Magnetometer, Gyroscopes	step events & direction	Pedestrian	Indoor	Absence of GPS Signals	No
[196]	Accelerometer,	step events & stride length	Pedestrian	Indoor	Location Accuracy Improvement	No
[198]	Accelerometer, Magnetometer, Gyroscopes	step events & stride length	Pedestrian	Outdoor	Location Accuracy Improvement	No
[199]	Accelerometer, Magnetometer, Gyroscopes	step events & stride length	Pedestrian	Indoor	Location Accuracy Improvement	No

[65]	GPS, Compass, Accelerometer, Gyroscopes	step events & stride length	Pedestrian	Outdoor	Location Accuracy Improvement & meet app requirements	No

Our position prediction method differs from the works listed above in that the main objective is to meet the position sampling requirement of mobile devices while using them for traffic safety applications. Moreover, the position prediction method is energy efficient.

5.3/ POSITION PREDICTION SYSTEM

The position prediction system proposed in this chapter is an online processing system implemented as an Android application. The system is aimed to extrapolate locations in a very short time interval (100ms) to meet application requirements of traffic safety applications as GPS based localization has a limited sampling frequency. A GPS fix gained every second is used as the correct location and to correct dead reckoning parameters for future predictions. If no new location is received from the satellite at a particular sampling period, dead reckoning based estimation is made using INS sensors data mainly accelerometer and magnetometer sensors. Major components of the system and flow among its constituents are shown in Figure 5.1.

The system has four groups of components. The sensors component contains the three main sensors used: GPS, accelerometer, and magnetometer sensors. The next components are sensor data filtering and processing components, and their roles are making the data ready for displacement and heading estimations. The third components calculate the distance travelled as well as direction of the travel. The last category is responsible for position prediction. The intermediate position is estimated from the distance travelled and the direction of movement. This position is passed through the Kalman filter to smooth outlier predictions. These components are detailed in subsequent sections.

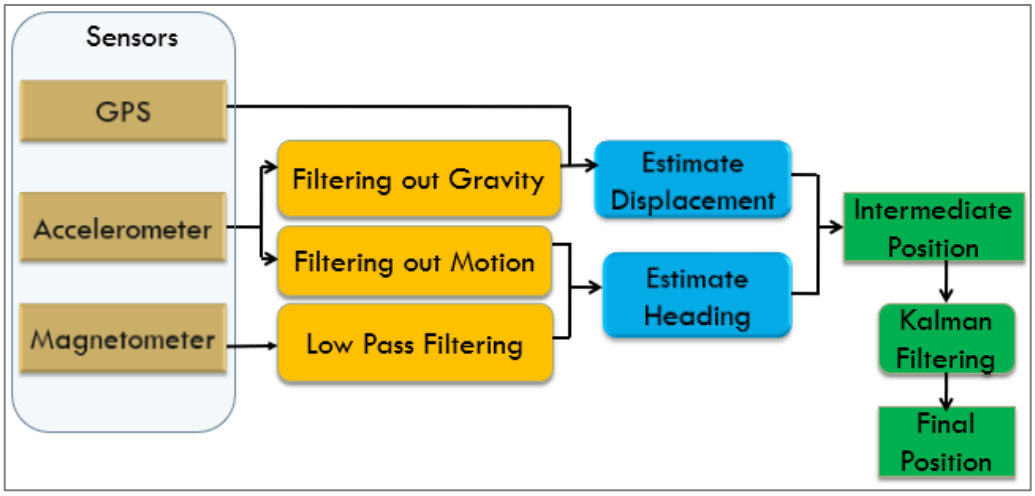


Figure 5.1: Component of the System for high position sampling system

Accelerometer and Magnetometer are the two inertial sensors explicitly used for position predictions in addition to the GPS sensor. The speed, which is one of the outputs of GPS readings, is used in displacement estimation by correcting velocity of the pedestrians obtained from the accelerometer as discussed in *Displacement Calculation* subsection below. Raw acceleration data is split into two by filtering out gravity and motion. This process results in linear acceleration and gravity virtual sensors. The two software-based sensors are synthesized through a combination of accelerometer input and gyroscope input. Since Android performs optimized filtering and sensor fusion processes by applying an Extended Kalman filter [201], the sensors' values from the Android are used directly. A magnetometer is employed to predict movement direction of smartphone holder. It is susceptible to working machines and metals in the vicinity as they result in high magnetic field strength. To remove the high-frequency noise from the output of the magnetometer, low-pass filtering has been applied. This process is intended to produce accurate and stable estimations by discarding unnecessary noise. After a repeated experiment in the test environment, it was found that at cutoff frequency f = 0.01Hz the heading result is more durable and accurate.

5.3.1. INTERMEDIATE AND FINAL POSITION PREDICTIONS

After pre-processing of the sensors data, the position is estimated by figuring out displacement and heading of the pedestrian. Linear acceleration obtained from the accelerometer is used together with the speed obtained from GPS to estimate displacement. The heading is computed from accelerometer without motion component and corrected magnetometer values. Once the two values are available, intermediate location result can be calculated using the following set of equations [195], [199].

$$X = X_0 + D * sin(\beta) \tag{5.1}$$

$$Y = Y_0 + D * cos(\beta)$$

Where (X_0, Y_0) and (X, Y) are initial and the intermediate positions, respectively, D is displacement, and β is heading, see Figure 5.2. The final position is obtained by passing intermediate position throw Kalman filter to improve the accuracy of prediction. Kalman filter equations presented in [202] are used since they have improved GPS accuracy by 12.59%. The detail of calculation of displacement and heading are presented beneath.

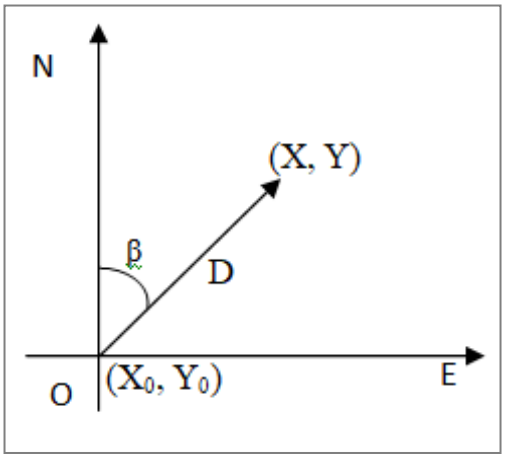


Figure 5.2: Calculating intermediate position (X, Y) from current position (X_0, Y_0) given distance traveled D and heading β

Displacement Calculation

Calculating displacement using inertial based pedestrian dead reckoning usually involves step detection and step length estimation [65], [195], [196], [198], [199], [200]. This method is not applicable if position estimation has to be made in a very short time interval since many predictions may be needed in a period of one stride which is 0.4m to 1.0m in length [195]. This is true for the application in consideration as position prediction has to be made every 0.1s. The conventional kinematics equations shown on equation 5.2 are used to calculate displacement.

$$V_t = V_0 + A_t * t \tag{5.2}$$

$$D_t = V_t * t + 0.5 * A_t * t^2$$

Where D_t, V_t, and A_t are displacement, velocity, and acceleration at time *t*, respectively; t is change in time; V_0 is the initial velocity. V_0 is set to 0 at the beginning. Velocity is calculated by integration of acceleration found from accelerometer without gravity. Since acceleration and velocity take vector values, integration is made for each axis. Due to accumulated error velocity extracted from linear acceleration tends to increase exponentially over a short period of time, see Figure 5.3. Therefore, velocity from GPS fixes is fused and used as initial velocity at each ground truth GPS fix. Let V^{gps} be

speed obtained from GPS, and β be heading, then X and Y components of initial velocities at ground truth point are computed using equation 5.3 [195].

$$V_{ox} = V^{gps} * \sin(\beta) \tag{5.3}$$

$$V_{oy} = V^{gps} * cos(\beta)$$

Only the velocity extracted from GPS fixes can't be used as it wouldn't capture frequent velocity changes of VRU as GPS are sampled every one second, and displacement is calculated every 0.1s.

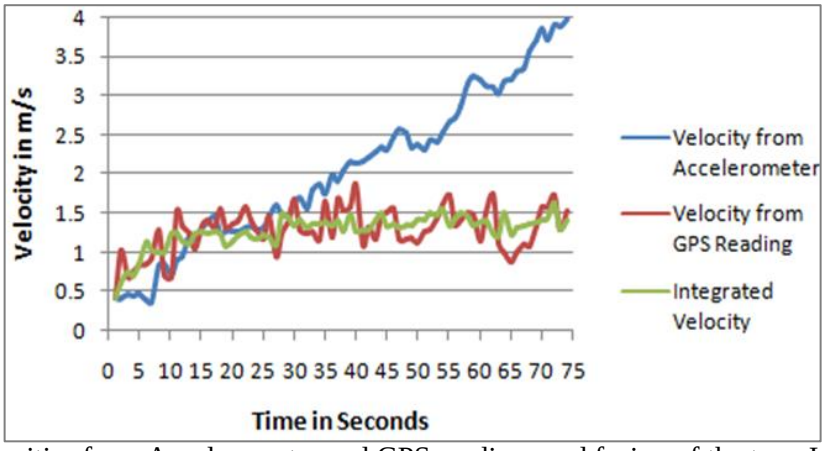


Figure 5.3: Velocities from Accelerometer and GPS readings and fusion of the two. Integrated velocity is more stable in comparison with velocity from the accelerometer. By taking this velocity the distance between two GPS fixes is found to be approximately the same as the sum of distances between GPS points

Heading Calculation

Heading is the deviation of the smartphone's Y-axis from magnetic north, measured clockwise in the East-North plane. Corrected values from the magnetometer and the gravity portion of the accelerometer are integrated to estimate the attitude angle of the smartphone [196]. From the two sets of values, a rotation matrix is produced to map points from the Local Coordinate System (LCS) to the Global Coordinate System (GCS) to resolve the random placement of smartphones. GCS is a real-world North-East-Gravity direction coordinate system. If R_t is the rotation matrix and γ is an azimuth which is the degrees east of magnetic north in LCS, then the orientation is converted to GCS using equation 5.4.

$$Y^{GCS} = R_t * \gamma^{LCS} \tag{5.4}$$

The actual heading of a user is forecasted by accounting declination angle. [192] and [196] can be referred for detail on heading estimation. Figure 5.4 displays a comparison of heading calculated using INS sensors and GPS bearing during a short trip in the test site. The test data is collected from a rectangular trajectory that takes 75 seconds to walk around. The result depicts that the two values are similar with only minor differences.

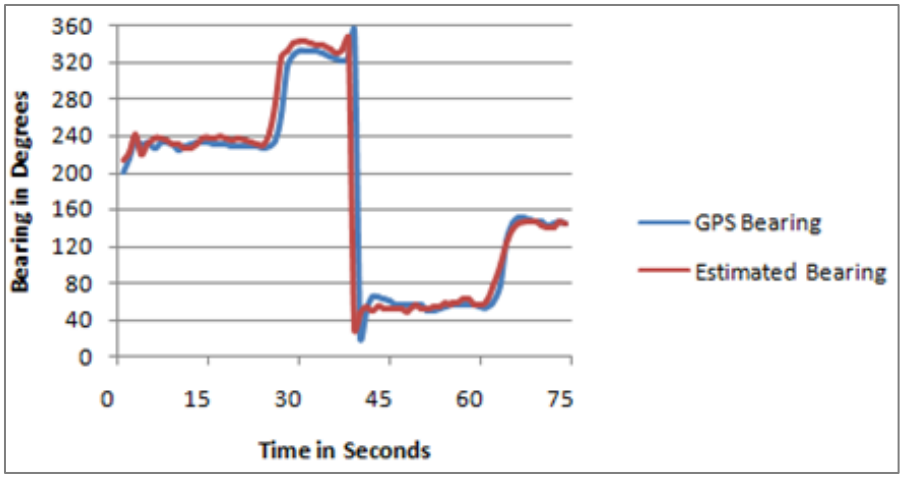


Figure 5.4: Comparison of heading estimation with ground truth GPS bearing

5.4/ PERFORMANCE EVALUATION AND DISCUSSIONS

In this section, the performance results of the proposed position prediction method are presented. Then, the energy consumption of various GPS and INS sampling rates are assessed. Finally, prediction exactitude of the proposed prediction method using various sampling methods that are found to enable obtrusive energy saving are evaluated.

5.4.1. PERFORMANCE OF THE POSITION PREDICTION MODEL

The position prediction system is tested with the data collected by a Samsung smartphone (Model-SM-A520F) with Android application that reads GPS points at the maximum possible sampling frequency in a plain area on a sunny day. The algorithm running on the smartphone calculates the displacement and heading angle and estimates locations at a 0.1s time interval. The accelerometer and the magnetometer were set to sample at a maximum rate, and average values are taken for the estimation period. Ground truth data is collected using the RTK position device (AsteRx4 OEM), which has centimeter-level accuracy. Two trajectories are conceived to test the proposed system. The first trajectory is a straight path with only one turn, while the second is a rectangular path with four turns. The proposed GPS and INS Sensor based Prediction (GISP) is compared in terms of the error in the distance of predicted points and deviation of heading from ground truth points of walking path of the pedestrian trajectories with Simple Linear Prediction (SLP). SLP is an extrapolation-based prediction mechanism which uses only GPS data. The method utilizes speed and bearing of the most recent GPS fix to estimate the intermediate positions between two GPS readings.

Figure 5.5 depicts the average and maximum distance errors of predicted points from ground truth trajectory points for the two prediction methods on the two trajectories. Maximum prediction distance

error is included to show the worst-case inaccuracies of the prediction algorithms. For both trajectories, the method that fuses GPS and inertial sensors data has few errors than the one that uses only GPS data. In fact, integrating inertial sensors with GPS improves position prediction accuracy by about 30% since the direction of movement is updated frequently from inertial sensors. The prediction is more accurate for Trajectory 1 due to its simplicity pertaining to its straightness.

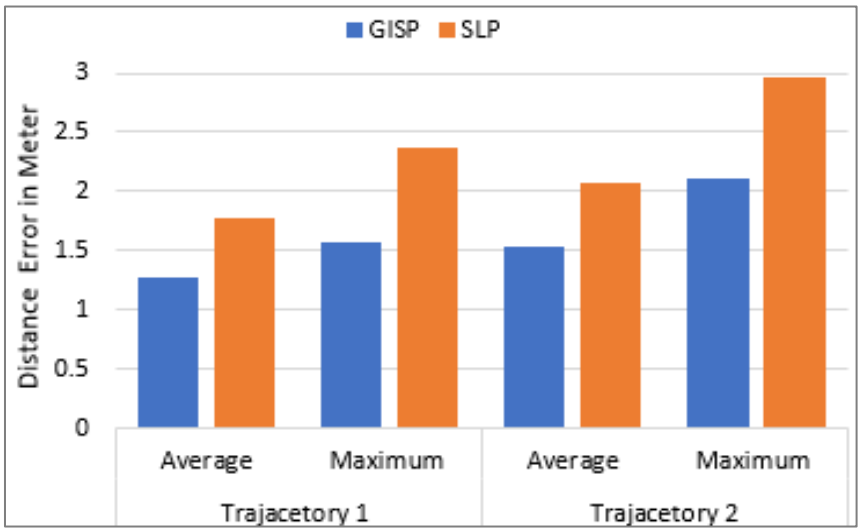


Figure 5. 5: Average and maximum error in distance of predicted points

Correct estimation of the heading of pedestrians is crucial for accurate position prediction. Figure 5.6 portrays average error in the heading of the two methods for the two conceived trajectories. The error for the second trajectory is higher than the first due to more turns in the pedestrian's path. In GISP heading of the pedestrian at each prediction point is feed from inertial sensors. Because of this, the method improves the accuracy of heading estimation by about 61.4% from the one which relies only on GPS readings.

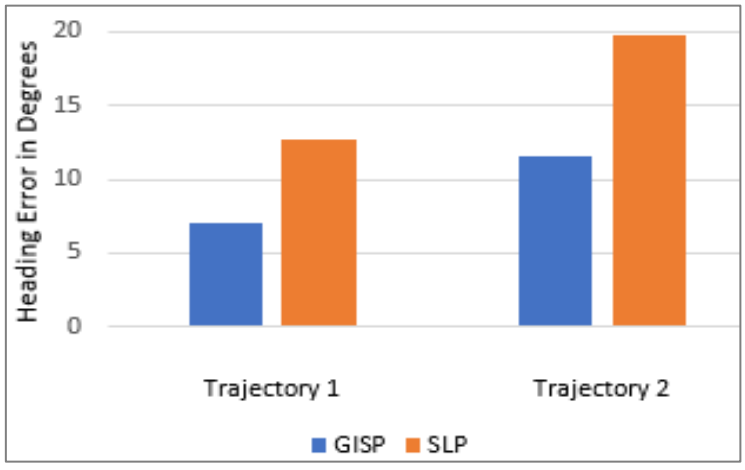


Figure 5.6: Error in heading of the two prediction methods

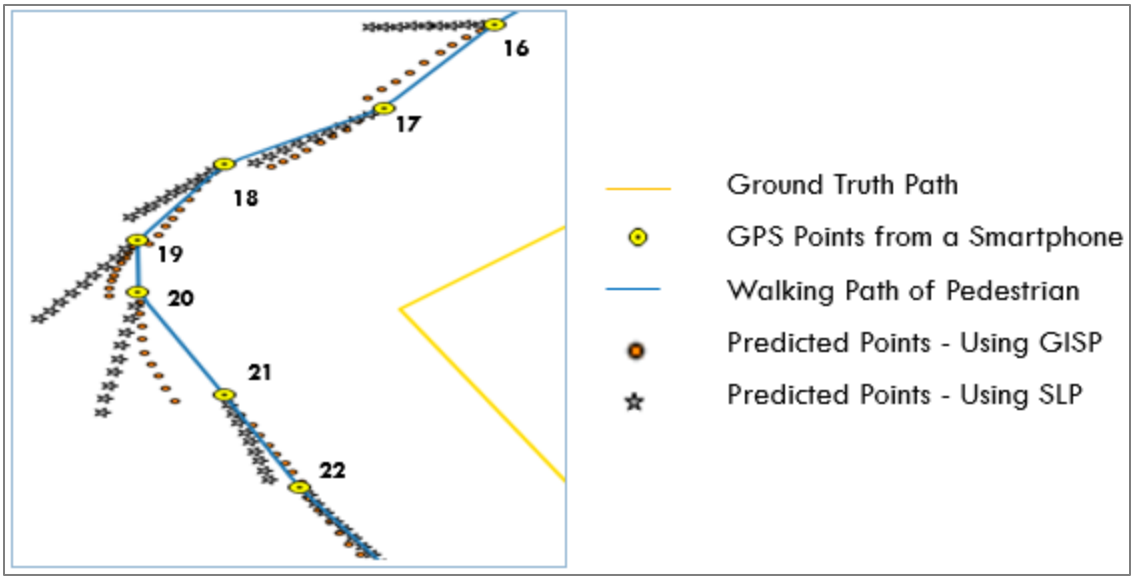


Figure5.7: A section on one of the turnings of Trajectory 2 showing predicted positions

A section of a prediction made on Trajectory 2 at one of the pedestrian's turning corners is illustrated in Figure 5.7. The accuracy of prediction decreases at the turning points due to the inaccuracy of heading estimations from inertial sensors. If GPS point numbered 20 is taken, as it is moved farther from the point, the inaccuracy of prediction increases. If it hadn't been for GPS's occasional fixes that periodically corrects the predictions, the forecasted position could have been deviated largely from actual positions of pedestrian trajectory. This is more visible for the points predicted using only GPS since it uses the bearing angle of the last known GPS point. GISP uses the inertial sensors in the absence of GPS fixes to predict positions. That is why it leans towards walking path as it can be seen on many GPS points. In both cases, when the next GPS fix is attained, it is used as initial and ground truth point for the next position prediction. The prediction tends to be more correct on straight-line walk as it can be seen at GPS fix numbered 21 and onwards.

To visualize the entire prediction trajectory graphically, refer to Figure 5.8. It shows paths constructed from ground truth points, walking path of a pedestrian and the paths constructed from predicted points for Trajectory 2. Paths constructed from predicted points are relatively curvier and non-stable than ground truth and walking path due to prediction inaccuracies. This is especially true for SLP path. From one GPS point to the next GPS point, it keeps deviation. However, as it gets the next GPS point, it returns to the actual walking path until it does the same for next position estimation points.

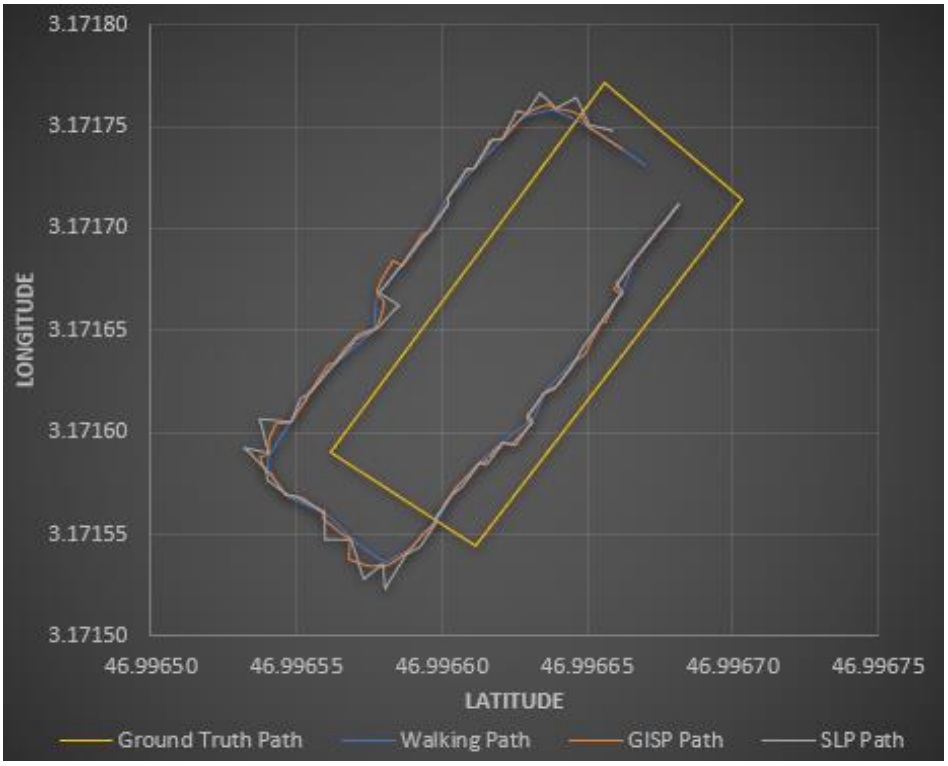


Figure 5.8: Paths constructed from predicted and ground truth points of trajectory 2 (rectangular trajectory)

5.4.2. POSITION PREDICTION MODEL: IMPACT OF THE SAMPLING RATES ON ENERGY CONSUMPTION

The position prediction method explained in previous sections is able to predict navigation path of pedestrian accurately. This method involves sampling GPS and INS sensor data at the highest possible frequency. The sampling frequency of GPS and INS affects energy consumption of smartphones, and of course, the position predictions accuracy [16], [68], [70], [71]. In other words, the higher the sensor data sampling rate the higher the energy consumption, and the more accurate the position estimation. The objective of any traffic safety application that involves energy-constrained devices like smartphones is estimating positions accurately with less energy consumption. In this section, the energy consumption of various GPS and INS sampling rates are assessed. Next, prediction exactitude of the proposed prediction methods, using various sampling methods that are found to enable noticeable energy saving, are evaluated.

The minimum GPS sampling period of smartphones are found to be one second. Higher sampling frequencies, however, could be used for energy saving as long as noticeable energy saving can be obtained and accurate prediction can be made. Energy consumption of GPS samplings at one, two, three, and four seconds are evaluated. Relaxed sampling period of inertial sensor data can also help in saving

energy. Two default Android (FASTEST and GAME) and one user defined inertial sensor sampling rates are assessed. The details of inertial sensor sampling types considered, and approximate number of samples taken for each prediction are displayed in TABLE 5.3.

TABLE 5.3. ANDROID INS SAMPLING TYPES

	FASTEST	GAME	USER DEFINED
Average Sampling Period (ms)	5	20	50
Average Number of Samples	20	5	2

A. Experimental Setup and Procedures

Three Android applications are developed to collect energy consumption information of the smartphone used for testing, TABLE 5.4. The first application is used to get battery consumption of an idle smartphone which doesn't sample GPS or INS sensor data. The other two applications encompass the position prediction algorithm, and they are used to know battery consumption of GPS sampling and INS data sampling.

TABLE 5.4. ANDROID APPLICATIONS FOR HARVESTING BATTERY INFORMATION

Application	GPS sampling Period	INS Sampling Period	Information Logged
Application1	No GPS data Sampling	No INS data sampling	System Time Stamp and Battery Information (Battery Level, Voltage, Average current discharge, and Temperature)
Application2	1s, 2s, 3s and 4s GPS data Sampling	No INS data sampling	System Time Stamp, Battery Information and GPS reading detail (Latitude, Longitude, bearing, accuracy)
Application3	1s GPS data Sampling	Fastest, GAME and User Defined INS Sampling	System Time Stamp, Battery Information and GPS reading detail and Inertial Sensor data (Calculated heading and distance calculated)

The following configurations are made before conducting the experiment:

- The smartphone is reset to factory setting before the experiments. During testing, no application runs except Application1, Application2 or Application3 and the smartphone is used strictly for this experiment.
- All types of connections are turned off and screen brightness is set to the lowest possible value so that the base energy consumption is minimized.
- Root access of the android smartphone is obtained so as to read the current discharge of the smartphone.

- The smartphone is charged to 100% before each experiment. For each experiment, the smartphone holder walked for 50 minutes in outdoor and indoor walking paths. For an additional 10 minutes, the smartphone is placed motionless on a flat desk.

The goal of the experiments is to cognize the energy consumption of various GPS and INS sampling rates to apply the proposed prediction method for those proved to save energy. A smartphone with a battery capacity of 3000mAh is used for the experiment.

B. Energy consumption result and discussions

The result of the energy consumption of smartphones at different GPS sampling period is indicated in Figure 5.9. As it can be obviously seen in the diagram, GPS reading at GPS sampling periods considered has no significant energy consumption difference. As stated in [68] and [70], location updates at lower intervals have very subtle differences in the battery decay over time. In the one-hour test, the battery level of the smartphone has decreased from 100% to 97.17% in 1s GPS sampling period and from100% to 97.84% in 4s GPS sampling period. The drop of battery level due to GPS sampling in the experiment, in general, is modest since the smartphone is used solely for this purpose and the mobile device used has a high battery capacity.

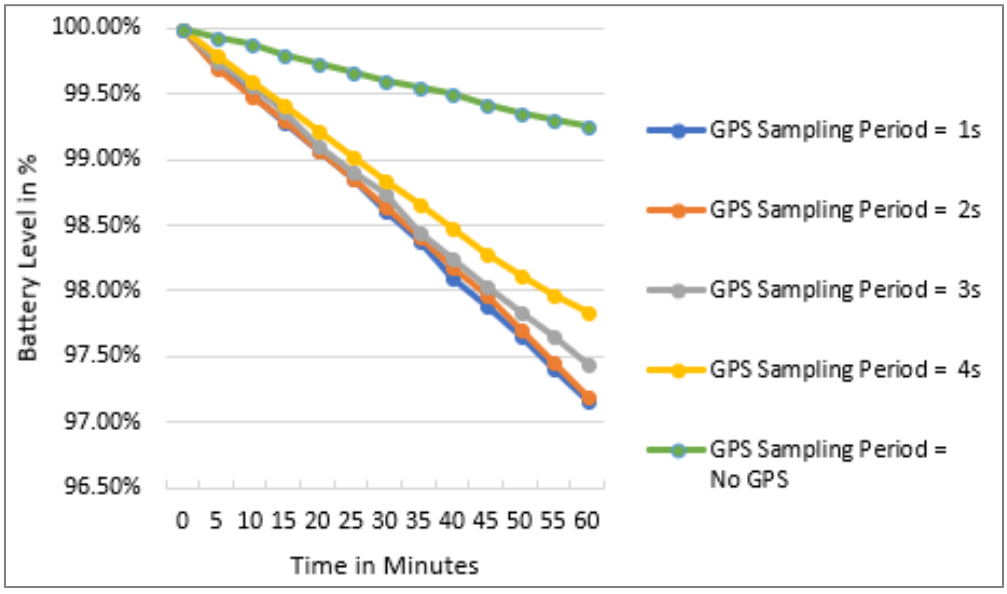


Figure 5.9: Energy consumption of different GPS sampling periods

The sampling rate of INS sensors affects the smartphones energy consumption [16], [71]. Figure 5.10 depicts the energy consumptions with the considered inertial sampling rates (fastest, game, and user-defined). Fastest sampling consumes energy quicker than the other two others. A smartphone battery that uses the FASTEST sampling will run out in just 11 hours. However, it could have been served for 23 hours and 26 hours if GAME and USER DEFINED INS sampling types, respectively, had been used. Note that, together with the inertial sensor, GPS is being read at the fastest rate (i.e., each second).

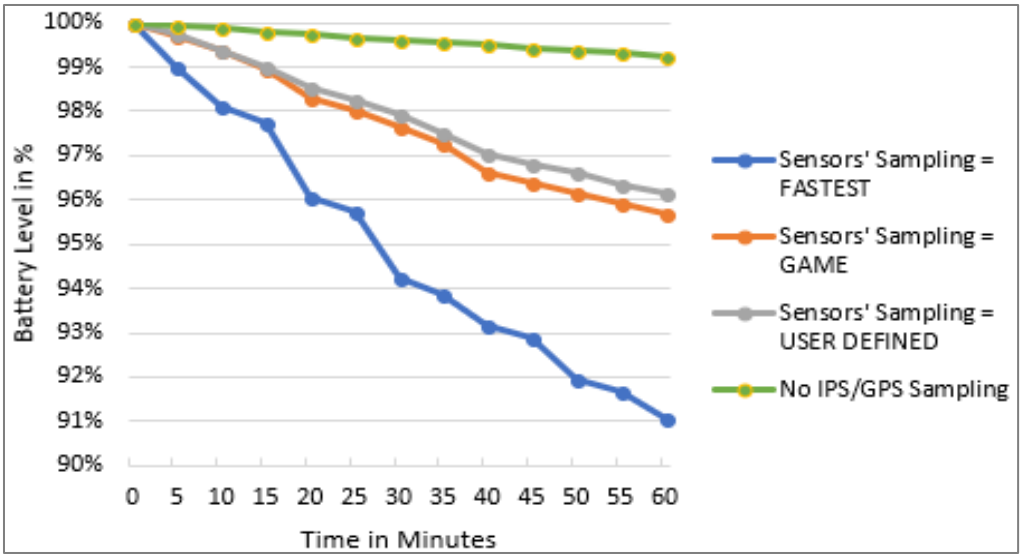


Figure 5.10: Energy consumption of different INS Sampling types

5.4.3. POSITION PREDICTION MODEL: IMPACT OF SAMPLING RATES ON THE PREDICTION ACCURACY

Small-scale energy overhead on different GPS data sampling period doesn't convince us to compromise accuracy by choosing higher sampling periods instead of the fastest GPS data sampling. However, in the case of INS sensor data sampling, an obtrusive energy saving can be achieved by selecting energy-efficient INS data sampling type as far as the sampling type has sufficient accuracy. In subsequent section, the evaluation of position prediction accuracy of INS data sampling types using inertial sensor and GPS based prediction methods are presented.

As illustrated in Figure 5.7, accuracy of position prediction depends on whether the prediction is made on straight or on curvy trajectories. Hence, the evaluation is made for straight and curved sections of Trajectory 2. From the rectangular trajectory, three curves and four straight lines are considered. In addition to GISP and SLP, the other two position predictions methods are compared. Position prediction method that involves GAME inertial sensor sampling, which we named GISP_GAME and the one that involves USER DEFINED inertial sensor sampling, which we named GISP_USER are the other two considered position prediction methods.

The average error in distance and attitude angle of predicted positions from ground truth pedestrian trajectory for both relatively straight trajectory and curved trajectories are displayed in Figure 5.11 and Figure 5.12, respectively. GISP, which depends on the highest INS sensor sampling frequency, is the most accurate prediction method on both straight and curved trajectories since it takes many INS data points to make the prediction. On a straight-line, there is no abrupt change of direction and this is the reason why SLP performs well with this scenario. In a curved trajectory, however, SLP performs worst

because of lack of updated movement direction until the next GPS fix is attained. GISP_USER works well neither on straight nor curved roads. In this prediction type, to make the prediction, the number of inertial sensor data taken on average are two and sometimes the prediction may be made using only one or no data points. Unless a considerable amount of sensor data is taken, due to the noisy nature of inertial sensors prediction is expected to be worst. The location prediction accuracy of GISP_GAME puts it second on the podium. Sampling period of this prediction is lower than GISP but higher than GISP_USER.

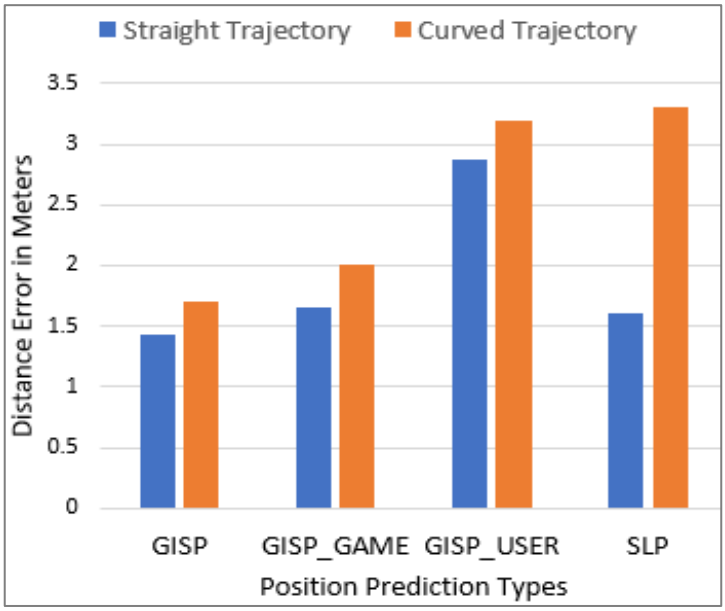


Figure 5.11: Average Error in distance of different position prediction types

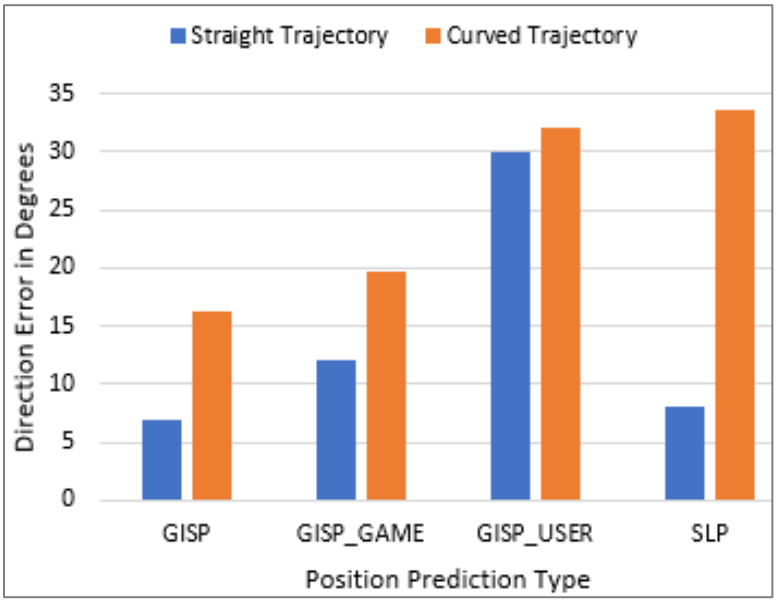


Figure 5.12: Average error in movement direction of pedestrian in different position prediction types

Though GISP has the most accurate position prediction result, it is the most energy-hungry method owing to its fastest INS data sampling rate. Pedestrian navigations are unpredictable and complex which means it is full of curves and twists. Therefore, SLP which is the most energy-efficient prediction method is not accurate enough for pedestrian navigation. GISP_GAME is recommended position prediction method since it doubles the life of smartphone battery with 11.5% compromise of accuracy.

5.5/ CONCLUSION

Smartphones owned by VRUs and drivers are integral components of PV-Alert and other mobile device based ITS applications. However, the handheld devices' GPS sensors do not support high position sampling requirement of those applications. Therefore, an inertial navigation system-assisted positioning system that works together with GPS sensors to predict locations of pedestrians at a very high rate is proposed. The method uses GPS fixes to correct dead reckoning parameters and as ground truth points for the next position estimations. A method that uses only GPS readings to extrapolate positions is compared with the new method using a data from two trajectories. The evaluation result of the solution using the two trajectories conceived shows that it can improve the accuracy of position prediction that solely depends on GPS. This is because the proposed system integrates inertial sensors that have very high short-term accuracy and GPS, which has very good long-term accuracy. Furthermore, to make the position prediction energy conserving, energy efficiency of various sensor sampling rates of GPS and INS data sampling were investigated. Results show that by sparsening GPS samples, the energy that could be saved is minimal while accuracy could be significantly affected. However, by reducing the sampling frequency of INS data sampling, obtrusive energy can be saved with minor accuracy compromise. Therefore, inertial sensors can be integrated with GPS sensor in an energy efficient way to satisfy high position sampling rate demand for traffic safety applications.

High position sampling and VRU to vehicle communication frequencies are the reasons for high energy consumption smartphones used for traffic safety. In this chapter, we have seen how energy can be saved by relaxing inertial sensors sampling. In the next chapter, energy saving by managing beaconing rates between VRUs and central server is addressed.

6

PV-ALERT: ACHIEVING ENERGY-EFFICIENCY BY ADAPTING THE BEACONING RATE

6.1/ INTRODUCTION AND PROBLEM STATEMENT

In chapter 5, we have discussed an energy-efficient position prediction method to meet the high position sampling frequency requirements of traffic safety applications. This chapter also contributes to the energy-efficiency of VRU devices by managing communication between VRUs mobile devices and a central server.

The high accident rate of VRUs [2] has attracted the attention of researchers in academia and industry all over the world. Thus, many passive and active traffic safety measures are proposed. Mobile devices are included as important ingredients of most contemporary active traffic safety solutions. For instance, in chapter 3, a fog-based architecture (PV-Alert) which is proposed to safeguard VRUs uses mobile devices to generate and send CAMs to fog servers as well as to receive DENMs sent from the fog servers. Though such solutions ensure the safety of VRUs, due to high CAM beaconing rate and high GPS sampling frequency requirements of the applications, mobile devices would deplete their already limited energy very quickly. Beaconing, in this context, refers to sending position and other traffic safety data to a central server that runs a traffic safety application.

In wireless communication, energy is consumed at a wireless network interface to send and receive data, and in a host device in processing each packet while it crosses the protocol implementation stack [203]. On the one hand, the energy-efficiency of drivers' mobile devices is not an issue since either the devices can be powered from the vehicle's power supply or the drivers can be connected with the vehicles' onboard computers instead of the handheld devices. Pedestrians' mobile devices, on the other hand, have limited and easily exhaustible power supplies that need to be optimized. The pedestrian and other VRUs can be in different collision risk situations during their mobility periods. Therefore, the rate of communication between mobile devices and servers should be managed based on the collision risk level of the VRUs rather than communicating at high rate all the time. In this schema, the high collision risk level implies high beaconing frequency. In fact, to protect a pedestrian who is in a high collision risk area, the fog server requires, among others, fresh position and kinematics data of the pedestrian and surrounding vehicles. If the pedestrian is in low-risk region, the data can be sent at lower frequencies.

This adaptive beaconing rate management is intended to decrease the energy consumption of mobile devices while keeping road users safe from collision risks.

Since the collision risk is not a binary concept, it can be defined to have multiple values or levels. To address multiple risk levels, the idea of multi-stage collision warning system is perceived [204], [205], [206]. For example, if three collision risk levels (high, medium and low) are defined, drivers and pedestrians can receive first alert messages when the pedestrians are in medium risk region and the final acute warning when they are in high-risk regions. The reason behind this is a single notification may be overlooked due to, for example, inattention or loud voices from surrounding. Furthermore, the type of the notification may be varied based on the risk level; if the risk level is low, only SMS may be sent, and if risk level is high a call/vibration-based notification can be sent. Reaction time differences of drivers and time to brake variation of vehicles based on weather and road conditions are other reasons for the need to have multiple notifications. In addition to notifying an imminent accident, the alerts may also contain information that instructs the mobile devices to increase the beaconing rate.

Considering all factors that increase collision risks is crucial for correct identification of the adequate collision risk level. There is a direct relationship between collision risk levels and energy consumption as high collision risk level induces high beaconing rate to safeguard pedestrians. High beaconing rate is an energy-hungry process [207]. Traffic collision risks are affected by many factors. Some of them are (i) pedestrian's behaviors, (ii) drivers' profiles, (iii) vehicles kinematics, (iv) road conditions, (v) environmental and weather conditions, and (vi) other communication network factors like communication and computation delays. Impaired or distracted pedestrians are more prone to traffic accidents. Old, distracted or speeding drivers or driving under the influence of alcohol accounts for many traffic injury fatalities. An increase in the speed of cars increases both the risk of accidents and the crash severity. The slipperiness of roads and higher slope grades increase the distance required for safely braking, which results in even higher accident risks. Bad weather conditions and time of the day may also affect traffic accident rates. Driver level of experience, drug usage, poor or inappropriate safety precautions, and even inadequate post-crash safety measures are among the most important reasons for high traffic deaths. Moreover, when active safety mobile applications are deployed, road safety is affected by both communication and computation delays.

To save mobile devices energy consumption due to communication with a central server, firstly, we have to identify the risk levels of road users. Next, risk levels are converted to appropriate beaconing rates. Thus, this chapter discusses a Fuzzy Inference System (FIS) proposed to forecast collision risk levels from the factors that affect traffic safety. The system predicts collision risk levels of pedestrians and adjusts beaconing rates accordingly. The fuzzy logic-based adaptive beaconing rate management system protects pedestrians from traffic accidents and at the same time minimizes the energy consumption of mobile devices. Fuzzy logic-based systems have a resemblance to the way our brain works, and they have the capability to give results in the presence of imprecise and vague information.

The fuzzy logic approach is an appropriate method for risk level prediction since the risk is a subjective concept, and fuzzy logic is tolerant to imprecise data [208]. Additionally, most factors that influence risk level are fuzzy and imprecise. Generally, the risk prediction accuracy of fuzzy logic systems depends on the involvement of domain experts in defining rule basis. Hence, to test the risk level estimation accuracy of the fuzzy logic-based solution, another risk level identification method is defined using the same parameters as the FIS. In the second method, the risk level is identified using actual vehicle-to-pedestrian distance and minimum distance for information exchange. The result of risk level prediction of the two methods is found to be the same for most of the traffic accident records used. This assurance us that FIS can, indeed estimate risk levels accurately. Accurate risk level identification implies energy efficiency model of the mobile devices used in traffic safety applications is reliable. The energy consumption of the proposed fuzzy logic-based adaptive beaconing rate management system is evaluated. Results depict that mobile devices that use adaptive beaconing rate consume only half of the energy consumed if a high rate beaconing is used. Additional evaluations portray that energy consumption of adaptive beaconing rate is affected by the factors that affect traffic safety.

The rest of this chapter is organized as follows. Related works are discussed in section 6.2. Section 6.3 presents the proposed fuzzy logic-based adaptive beaconing rate management system. The evaluation made to test the accuracy of the FIS is presented, and the energy-efficiency evaluation of the adaptive beaconing rate are discussed in section 6.4. The conclusion is drawn in section 6.5.

6.2/ RELATED WORKS

Beaconing in telecommunication refers to the continuous transmission of small packets (aka beacons) to signal error conditions or availability of network devices. In this chapter, beaconing denotes continuous transmission of geographical and other related information from mobile devices of road users to servers to protect road users from risk of traffic collision. Beaconing rate management is important for the reduction of network congestion and energy consumption. High rate beaconing threatens the capacity of a network and depletes the transmitter's energy rapidly. Beaconing rate can be managed by message frequency control, transmission power control, or by a combination of the preceding two approaches [209], [210]. Message frequency control involves varying beaconing rate based on situations while transmission power control decides how far information has to be broadcasted. The beaconing rate management is widely dealt in the area of mobile ad-hoc networks like VANET. This is because the number of beacons sent among the nodes is enormous to maintain the network structure and to fulfill the requirements of the applications. In [211], a rate-power control algorithm that adjusts communication power and rate based on the dynamics of vehicles in a VANET and safety-driven tracking process is proposed. Their evaluation indicates that the controlled state information broadcasting to neighboring vehicles can track vehicles accurately and is robust in comparison with solutions that involve static beaconing. Situation adaptive beaconing that relies on the movement of a

vehicle and other surrounding vehicles is presented in [212]. Beaconing rates per vehicle per second are suggested by taking tradeoff between offered load and accuracy into consideration.

For traffic safety applications, beaconing rate can be varied based on collision risk level. Hence, risk level prediction is the most important process to define adaptive beaconing rate management systems. So far, traffic accident prediction models have been proposed in the literature. In [213] an accident prediction model that can accurately predict the expected number of accidents at urban junctions and road links is proposed. However, it doesn't involve traffic risk level prediction, which is very important to thwart accidents. An image processing and computer vision-based traffic accident detection mechanism is presented in [214]. However, image processing-based accident detection is highly affected by the time of the day, weather condition, and the used camera. Hu et al. [215] proposed a probabilistic model for predicting traffic accidents using 3D model-based vehicle tracking. However, all of the above methods focus on accident detections by identifying vehicles without giving attention to other road users. [206] and [216] have used fuzzy logic-based collision risk level inference system for warning system design and for avoiding pedestrian accidents, respectively. In addition to its proven applications in the domain of artificial intelligence, control, and traffic safety systems, fuzzy logic has been applied in many ITS applications. Traffic congestion [217], auto-driving [218], and ride comfort [219] are some of the examples.

Though the following works are not particularly for traffic safety applications, they are proposed for smartphone energy efficiency. In [69], the usage of auxiliary location methods with GPS sensor for Location Based Services (LBS) that require continuous location updates is able to achieve 27% energy saving. An energy-efficient location-based system for a pedestrian touring system used adaptive GPS sampling and saved 45% energy of the smartphone [70]. An adaptive inertial sensors' data sampling method for wheelchair users, which is proposed in [68], is able to save 22% of smartphone energy. A reduction of inertial sensors sampling to 20Hz for a pedestrian navigation system has enabled 25% energy saving [71]. One of the differences between traffic safety and other applications is that traffic safety applications require high rate position sampling and communication. According to ETSI, the beaconing frequency of CAMs for pre-crash sensing warning system should be between 1Hz and 10Hz. This implies that CAM has to be sent from 1s to 100ms based on risk level. Obviously, this will keep the pedestrians, who are the most road accident susceptible road users among VRUs, safe from the accidents. However, when pedestrians' mobile devices are used for such applications, their energy will be depleted in a very short period of time. This is because high beaconing rate implies high energy consumption and the pedestrian's mobile devices, in contrast to mobile devices of drivers, are less likely to be connected to power supply source during the mobility period. That is why adaptive beaconing rate management system that sends beacons at a high rate when a pedestrian is in a high-risk region and at a lower rate otherwise is required. This helps to save a great deal of energy while keeping pedestrians safe from traffic accidents. To the best of our knowledge, only [72] has applied beaconing rate management-

based energy efficiency of mobile devices while using them for VRU safety. The cloud-based pedestrian safety system employs situation adaptive beaconing depending on only two risk levels for energy efficiency. Moreover, [72] uses kinematics of vehicles to determine collision risk level while we have considered many types of factors that affect collision risks and molded them using fuzzy logic model to determine collision risk level.

Other than GPS sampling and communication management-based methods to save energy efficiency of mobile devices, methods that involve grouping pedestrians and computation offloading are also proposed. An energy-efficient V2P communication schemes to exchange safety messages using mobile devices is proposed in [73]. The method involves grouping pedestrians in proximity, electing group leader and making the communication with the vehicle through group leader while P2P communication is made among group members using Wi-Fi direct. Calculating context information on already resource-restricted smartphones of VRU could result in reduced battery lifetime. Hence, an adaptive context information calculation approach which offloads computation to a server at the edge of network is proposed [74]. However, due to the latency the offloading introduces the method can be applied only in situation where sensor data has to be sampled at low frequencies. Otherwise, it is recommended to perform calculations locally and that implies it is not energy efficient. None of the solutions mentioned above has considered collision risk level determinant factors like distraction and driving under the influence of alcohol in risk level determination for energy efficiency. TABLE 6.1 provides a summary of the smartphone energy saving solution proposed in the literature.

TABLE 6.1. SUMMARY OF WORKS ON ENERGY EFFICIENCY OF MOBILE DEVICES

Reference	Application	Energy Saving Method	Collision Risk Considered?	Result
[69]	LBS with continuous Location updates	Using auxiliary Location Method	No	27% Energy saving
[70]	pedestrian touring system	Adaptive GPS Sampling	No	45% energy Saving
[68]	wheelchair user's navigation system	Adaptive inertial sensor data sampling	No	22% energy Saving
[71]	pedestrian navigation system	Adaptive inertial sensor data sampling		25% energy Saving
[72]	Pedestrian Safety	Beaconing Management	Yes (2 risk levels)	13% energy overhead in 2 hours simulation
[73]	Pedestrian Safety	Grouping Pedestrians	No	36.8 % as compared to the WAVE standard
[74]	VRU Safety	Offloading Context information	No	In low sampling rate offload Schema has better energy saving than local schema

6.3/ FUZZY LOGIC-BASED ADAPTIVE BEACONING RATE MANAGEMENT

In this section, we first present the formulation of the problem. Next, the three important parts of fuzzy logic systems in relation to the problem in question are discussed. Finally, the risk level to beaconing rate conversion is explained.

6.3.1. PROBLEM FORMULATION

Since risk is fuzzy in concept and most factors that affect traffic safety are also fuzzy, a fuzzy logic-based collision risk level prediction system is proposed to protect pedestrians from traffic accidents by introducing an energy-efficient beaconing rate management. The multi-stage notification system identifies the risk levels by considering many factors that affect traffic accident risks.

The adaptive beaconing rate management system has three main components: (i) preprocessor component, (ii) fuzzy logic component, (iii) beaconing rate decider. Figure 6.1 shows the three components, while Figure 6.2 indicates the distribution of roles of adaptive beaconing rate management of the components in PV-Alert.

Preprocessor component is responsible for compiling factors that affect traffic safety into inputs of the fuzzy logic model. The fuzzy engine takes factors compiled as input variables and determines the risk level for a pedestrian. The risk levels are converted into beaconing rates that ensure an energy-efficient traffic safety of pedestrians using Beaconing rate decider. The preprocessor component is discussed in this section while the other two components are detailed in subsequent sections.

Road traffic accidents are affected by many factors [220]. In the proposed system, preprocessing stage involves grouping key road safety risk factors into four categories, namely: (i) reaction time, (ii) Time to Collision (TTC), (iii) processing time, and (iv) road type.

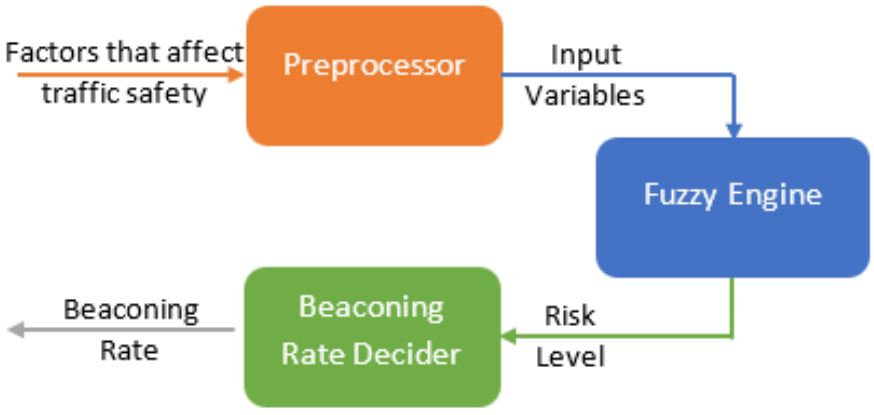


Figure 6.1: Overall process of adaptive beaconing rate management

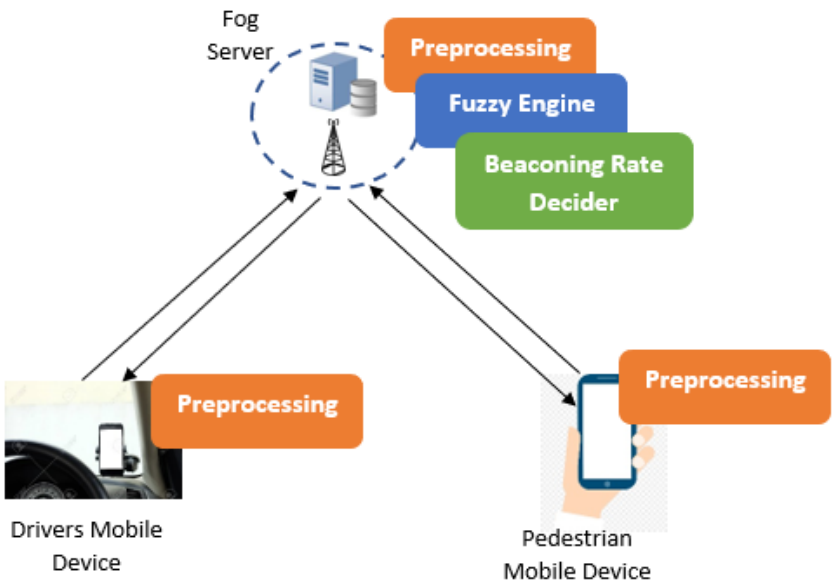


Figure 6.2: The distribution of roles of adaptive beaconing rate management on the components of PV-Aler

Reaction time refers to the perception-reaction time of a driver, and it is affected by age, distraction level, and alcohol intake of the driver plus weather and time of day. The fastest reaction time of a person is 0.83s [55]. Weather condition extremely affects the driver's reaction time [221]. In rainy days, the reaction time of a driver is delayed by 2s. Driving at night, induces 0.4s slower reaction time than driving at daylight [222]. Old drivers are 0.5s slower than young drivers, according to [223]. There are many reasons for a driver to be distracted. Distraction due to cellular phone conversation is considered. A driver in a phone conversation is 0.85s slower than a driver with no phone conversation to react [224]. Drinking and driving is prohibited in many countries. Yet, it is the reason for many traffic accidents. According to [225], a 10% increase in blood alcohol concentration levels results in a 2% increase in reaction time. Influenced reaction time is obtained by summing reaction delays due to the elements mentioned above. The age of a driver can be easily found from his profile. Alcohol intake status can be obtained from the future Driver Alcohol Detection System for Safety [226]. Time of day, weather, and phone conversation distraction can be read from a pedestrian's smartphone or from the central server.

TTC is the time required by a vehicle to collide with a pedestrian if it moves at the current speed, towards the direction of the pedestrian. Assuming constant speed, TTC can be computed from a distance between a vehicle and a pedestrian (D) and velocity (V_{veh}) of the vehicle using simple motion equation 6.1 [227].

$$TTC = \frac{D}{V_{veh}} \tag{6.1}$$

The value of the two variables can be obtained from GPS reading of the mobile devices of the drivers and pedestrians.

Processing time refers to the time a server takes to compute collision prediction algorithm and the round-trip delay of messages from the mobile device of a pedestrian or a driver to the server. The computation time of a server running the traffic safety algorithm depends on its specification and workload. However, it can be taken to be 0.5s [72]. Communication time when LTE is used to connect mobile devices and servers is 0.05 s [72].

The **type of road** has an effect on whether a vehicle could brake in a short distance and prevent an about-to-occur accident. Braking distance (d_{Brake}) of a car depends on friction coefficient (μ) and grade of a road (G) in addition to the velocity of the vehicle and gravitational acceleration 6.2 [206].

$$d_{Brake} = \frac{V_{veh}^2}{2g\,(\mu + G)} \tag{6.2}$$

The value of coefficient of friction ranges from 0.1 (for ice-covered road) to 0.9 (for dry asphalt and concrete roads) [228]. Gravity acceleration g is equal to 9.8m/s^2. Road grade, which represents slope or inclination of roads, is taken to be 0(flat) to 10%(inclined).

Fuzzy logic-based systems help to make decisions in the presence of vague or unclear inputs. It differs from classic logic in that elements can belong to a set partially. Here, the system is utilized to estimate road accident risk level of pedestrians from various vague input factors. The value of most of these factors can only be described with some uncertainties. FISs have three important components; (i) fuzzification, (ii) fuzzy inference system and its rule base, and (iii) defuzzification. The three components are shown in Figure 6.3.

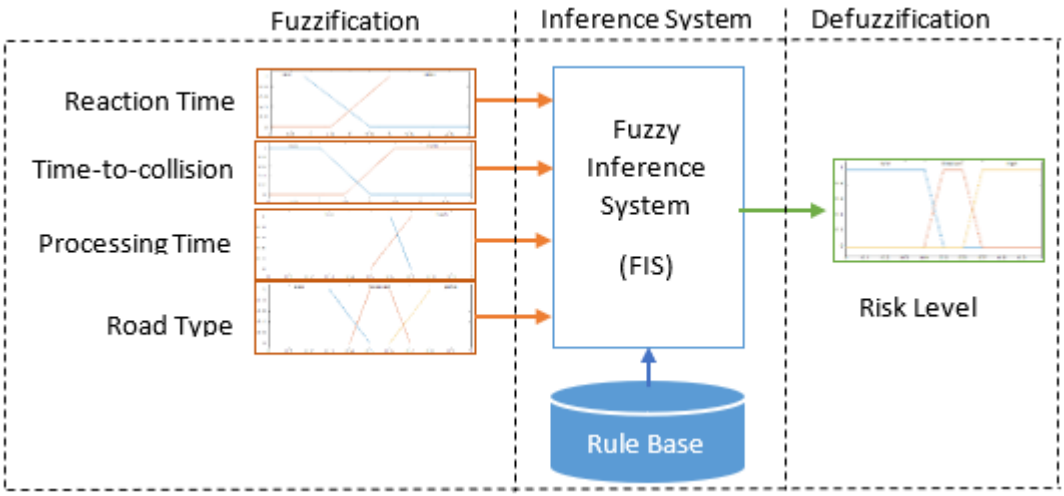


Figure 6.3: Fuzzy inference system for risk level determination

6.3.2. FUZZIFICATION

Fuzzification, which is the first step in the fuzzy inference process, converts crisp values of different inputs into fuzzy sets. It transforms accurate numerical values into linguistic variables based on

predefined membership functions. Membership functions determine the fuzziness of an input. Trapezoidal membership functions are used for all fuzzy engine inputs and outputs as they are among membership functions that work so well in fuzzy systems [229].

In the fuzzy system, the four groups of road risk factors discussed in the preceding section are used as inputs of the FIS. Reaction time, TTC, and processing time have two fuzzy set values (linguistic terms): high and low. The higher the reaction time of a driver, the most probable traffic accident is. The smaller the TTC value, the higher the collision risk is. TTC value less than 1s is more likely to cause accidents [227], and the proposed TTC value to avoid accidents is 3s [230]. The larger the processing time, the riskier it is for a pedestrian. Membership function for reaction time, TTC, and processing time are shown in Figure 6.4 a), b) and c), respectively. The road type is fuzzified to fuzzy set values bad, medium, and good. The larger the sum of the coefficient of friction and road grade, the smaller the distance to brake and hence the safer it is from provoking an accident, see equation 6.3. Hence, fuzzy value *bad* of road type implies a high risk of accident, *medium* refers moderate level of accident risk and *good* implies a low chance of inducing an accident. The member function of the input is shown in Figure 6.4 d).

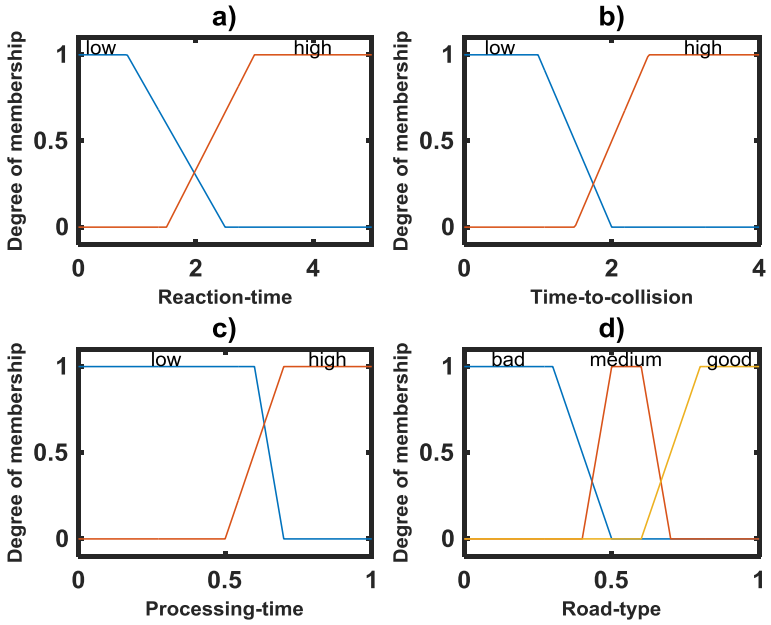


Figure 6.4: Membership function for the four inputs

6.3.3. INFERENCE SYSTEM

The FIS is the most crucial component of the fuzzy logic system for decision making. It contains rule bases and databases to convert fuzzified inputs into fuzzy output sets. Rule bases, which should be defined by experts, contain a set of Fuzzy IF-THEN statement that blends different inputs using AND or

OR fuzzy logic operators. The database refers to membership functions of fuzzy sets used in fuzzy rules. Among the two well-known fuzzy inference methods, Mamdani type of inference system is opted to conjecture fuzzy output sets from fuzzy input sets and 24 rules are defined. Some examples of conventional IF-THEN decrees of the rule base are displayed below:

- *IF Reaction time is low AND TTC is high AND processing time is low and road type is good THEN Risk Level is low.*
- *IF reaction time is low AND TTC is high AND processing time is high AND road type is medium THEN Risk Level is medium.*
- *IF Reaction-time is high AND TTC is low AND processing time is high and road type is bad THEN Risk Level is high.*

The effect of individual inputs on collision risk level, as it is derived from the rule base, is shown in Figure 6.5 (1st and 2nd rows). The last row of the figure depicts the effect of a selected combination of inputs on the risk level.

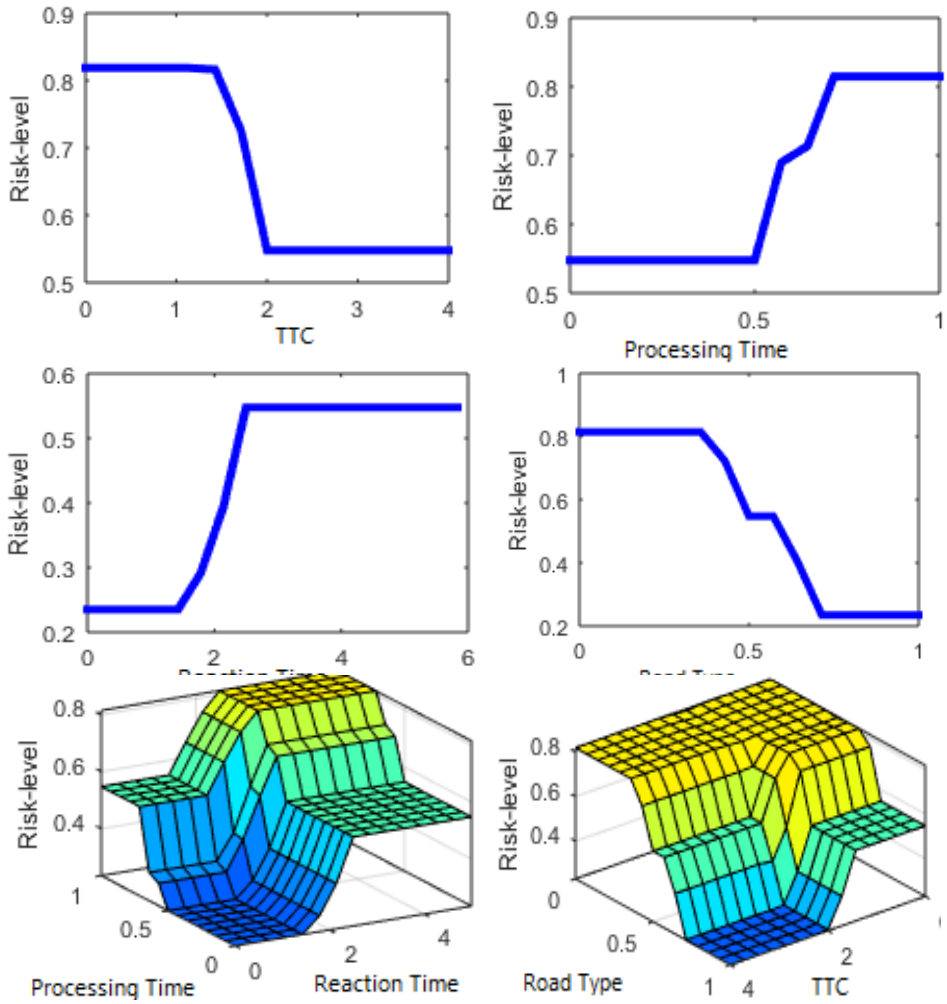


Figure 6.5: Effect of inputs to FIS on risk level

6.3.4. DEFUZZIFICATION

Defuzzification, which is the inverse process of fuzzification, is the process of changing fuzzy values of an output to quantifiable result using defuzzification techniques. Defuzzification determines the type of action that has to be assumed by the system. Crisp values enable us to select more appropriate actions than fuzzy results generated by an inference system. The output of the fuzzy engine, in the proposed solution, is the risk level. The FIS infers risk level as fuzzy sets with the following values *low*, *medium*, and *high*. These values are converted to specific values using the membership function shown in Figure 6.6. In the overall system, the specific values will be used by beaconing rate decider to decide about the frequency of information exchange between a mobile device and a server.

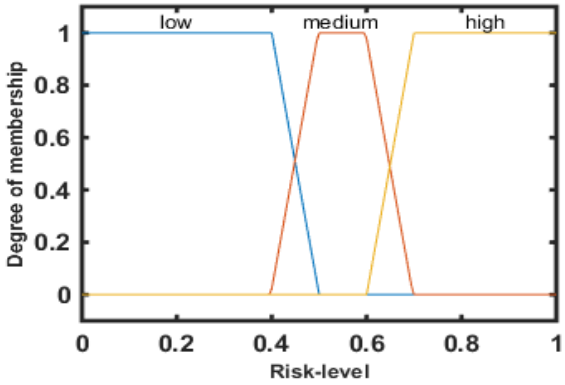


Figure 6.6: Membership function for defuzzification

6.3.5. RISK LEVEL TO BEACONING RATE CONVERSION

Beaconing rate decider, which is shown in Figure 6.1, converts risk levels produced by fuzzy logic to beaconing rates that save mobile device's energy while keeping the pedestrian safe from traffic accidents. As it has been pointed out above, the type of risk level determines the beaconing rate of the traffic safety system. *High*, *medium*, and *low* risk level linguistic terms of the output variable correspond to *high*, *medium*, and *low* beaconing rates. The beaconing rates are decided from crisp risk level values based on the mapping shown in Figure 6.7. The mobile device of a pedestrian in a high-risk region (risk level value 0.7 to 1.0) needs to send position, kinematics, and other related information at a high rate, i.e. 10Hz. If the pedestrian is in medium risk level, beacons will be sent at the rates between 10Hz and 1Hz, non-inclusive. It is named *half* or *medium* rate beaconing rate. If a pedestrian is in low risk region, his mobile will send beacons at la ow rate, i.e. once in a second or even at lower rates.

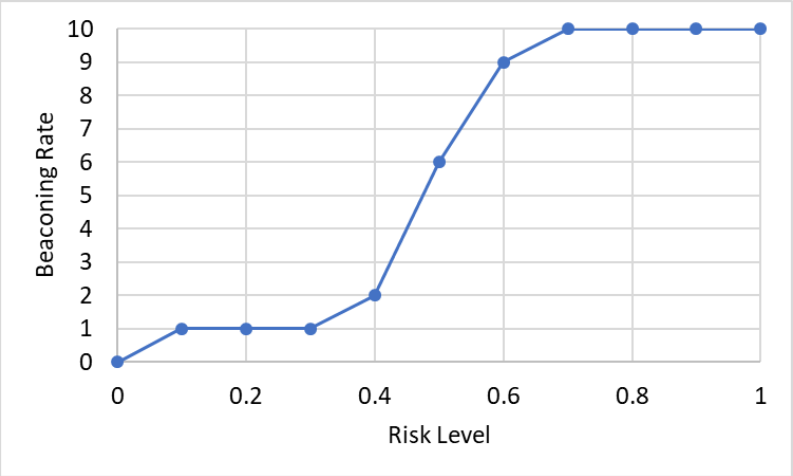


Figure 6.7: Relationship between collision risk level and beaconing rate

6.4/ PERFORMANCE EVALUATIONS AND DISCUSSIONS

In this section two sets of evaluations are made. Section 6.4.1 presents the evaluation of the traffic risk level prediction accuracy of the fuzzy logic-based model in comparison with traffic risk level estimation that depends on minimum distance for information exchange. Subsequently, in sections 6.4.2 to 6.4.4, we discuss the evaluations made on the energy-efficiency of the FIS.

6.4.1. EVALUATION OF THE FUZZY LOGIC MODEL

The fuzzy logic system presented in section 6.3 had been tested with synthetic data to check if it works correctly according to its definition. The system works correctly for all data that cover all possible combinations of the inputs of the fuzzy model. The fuzzy logic system is highly dependent on expert knowledge. To build more faith in the proposed prediction system's ability to predict collision risk level accurately, a collision risk prediction system that depends on minimum information exchange distance (D_{min})[3], is defined and comparison is made on estimated risk levels of the methods. D_{min} is the minimum distance between a vehicle and a pedestrian which is sufficient for the pedestrian and driver to perceive a collision and react soon enough to avoid an imminent accident [60]. The collision risk level of a pedestrian can be identified from D_{min} and its actual distance from the vehicle. The D_{min} based Collision Risk Level (DCRL) prediction system uses the same input parameters as that of the fuzzy logic system. Both have three traffic risk levels where drivers and pedestrians are notified twice to avert a foreseen accident.

D_{min} is obtained by calculating the distance the vehicle travels during reaction time, processing time, braking time, and while a pedestrian is crossing a road, as shown in formula 6.3.

$$D_{min} = d_{reaction} + d_{processing} + d_{brake} + d_{pedcross} \quad (6.3)$$

[3] D_{min} is formulated in different way in chapter 3 for traffic accident prediction. Here it is reformulated by integrating more factors that affect traffic safety.

Where,

$$d_{reaction} = V_{Veh} * t_{reaction} \quad (6.3.1)$$

$$d_{processing} = V_{Veh} * t_{processing} \quad (6.3.2)$$

$$d_{pedcross} = V_{Veh} * \frac{w}{V_{ped}} \quad (6.3.3)$$

Note that: $t_{reaction}$ is the time of reaction; $t_{processing}$ is processing time; w is the width of road; V_{ped} is the speed of pedestrian, and d_{Brake} is calculated based on equation 6.2.

By taking values that maximize the risk of a collision for the parameters mentioned (for best safety), D_{min} of equation 6.3 can be formulated in terms of vehicle velocity in equation 6.4.

$$D_{min} = 7*V_{veh} + 0.26*V_{veh}^2 \quad (6.4)$$

The risk levels of the pedestrian can be identified by comparing the current Vehicle's Actual Distance (VAD) with D_{min}, as shown in TABLE 6.2.

TABLE 6.2. RISK LEVELS, RISK WINDOWS AND ASSOCIATED WARNING OF DCRL PREDICTION SYSTEM

Risk Level	Risk Window	Warning
High Risk	VAD < $\frac{D_{min}}{2}$	Acute Warning
Medium Risk	D_{min} < VAD < $\frac{D_{min}}{2}$	First Warning
Low Risk	VAD > D_{min}	No Warning

The three risk windows of the DCRL prediction system for vehicles moving at various speeds is shown in Figure 6.8. Vehicles moving at higher speeds pose higher traffic accident risk (have longer risk window for high and medium risk levels) to a pedestrian than slow moving vehicles. Therefore, to avoid accidents, fast moving vehicles must receive a notification when the vehicles are far away from the pedestrian. For instance, a vehicle moving at speed of 30m/s (108km/h) will receive first and acute warnings when the vehicle's distance from the pedestrian is at 444m and 222m, respectively. The distance for sending notification decreases as the velocity of the vehicle decreases. For a vehicle that is moving at a speed of 5m/s (18km/h) the warnings are sent when their distance from the pedestrian is 42m and 21m, respectively.

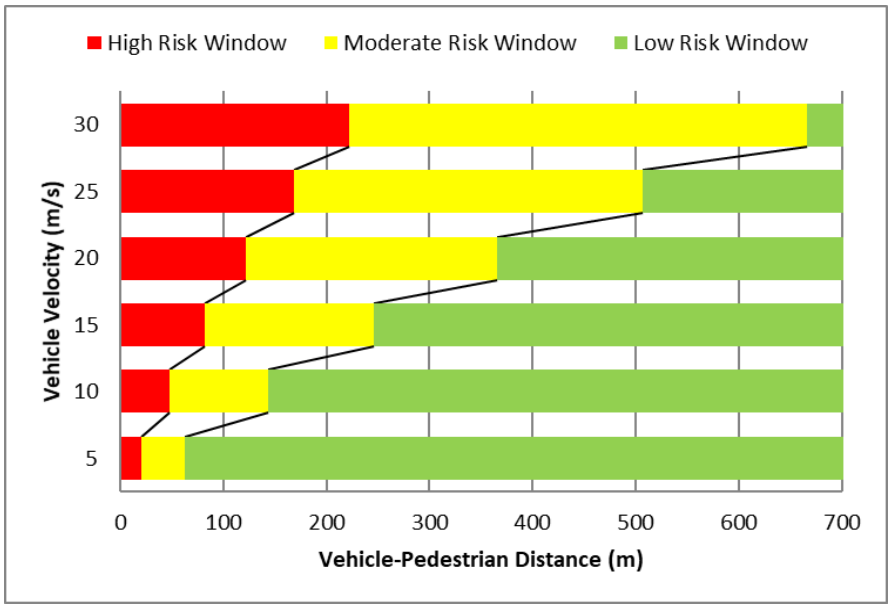


Figure 6.8: Risk windows posed by vehicles moving at different speed

The fuzzy logic and D_{min} based accident prediction systems are compared using a randomly generated traffic accident data for non-intersecting road scenario. Road accidents at non-intersecting roads account most of the pedestrian accidents, and they are the most severe ones that result mostly in fatalities [41], [190], [207], [231]. On the contrary, most studies ignore non-interacting road crash scenarios. Among pedestrian crash scenarios presented in [232], nine of them are non-intersection road scenarios, and they account about 40% of all pedestrian crashes. The testing data have considered those non-intersection scenarios. TABEL 6.3 shows the parameters and corresponding values of the generated data.

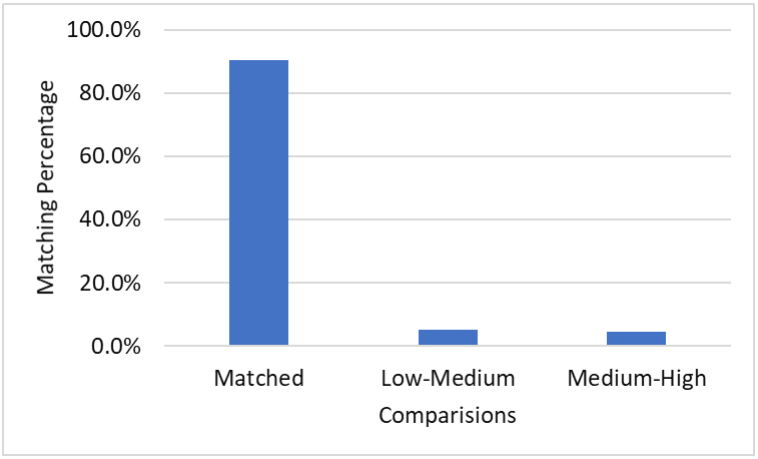


Figure 6. 9: Comparison of FIS based and DCRL prediction systems

The simulation is conducted for two hours, and the risk level vehicles engender to pedestrian is calculated using both fuzzy inferences based and DCRL prediction systems. The comparison of the

results shows that 90.4% of the risk identification of the two methods matches exactly, as shown in Figure 6.9. The remaining ones are identified as low by one system while the other predicts medium (low-medium) or categorized as medium while the other predicts high (medium-high). However, no accident scenario is categorized as *low* while the other estimates high or vice versa. This ensures that the fuzzy logic-based collision risk level system indeed can predict risk levels correctly. This makes the energy saving model correct too. However, the fuzzy logic-based model is more appropriate than the DCRL prediction system since most of the input parameters for risk level prediction are fuzzy in nature and the risk by itself is a fuzzy concept.

The following subsections describe experiments made to know how much energy can be saved using the proposed adaptive beaconing rate management system.

6.4.2. SIMULATION SETUP

The following subsections describe experiments made to know how much energy can be saved by using the proposed adaptive beaconing rate management system. The vehicle arrival rate is assumed to follow Poisson distribution [233], [234]. As the vehicles move towards the pedestrian, the risk they pose to the pedestrian is continuously monitored. Based on their simulation lifetime, input parameters to the fuzzy logic model are categorized into three: (i) area-specific, (ii) vehicle-driver specific, and (iii) simulation time specific. Area-specific or constant parameters are those that remain unchanged all over a road segment. Factors related to environmental condition, friction and width of the road as well as pedestrian speed are included in this category. Vehicles speed and drivers related attributes like age and distraction level are generated as each vehicle-driver are introduced in the simulation. For each simulation interval, the server's computation time and communication time of the wireless channel are estimated. The summary of road accident risk factors and corresponding values are displayed in TABLE 6.3. MATLAB is used to conduct the simulation.

TABLE 6.3. RISK FACTORS AND CORRESPONDING VALUES OF THE DATA GENERATED

No	Risk Factor	Values	Pertaining to
1	Age	Young =0s, Old=0.5s [223]	Driver
2	Alcohol level	Clean = 0s, Alcoholic = 0.034s [224]	
3	Distraction Status	No phone = 0s, simple conversation = 0.5s, complex conversation = 0.85s [224]	
4	Velocity	5 to 30 m/s	Vehicle
5	Initial Distance (to Pedestrian)	1 to 1000 meters	
6	Speed	Walking = 1.28 m/s to 1.83m/s, Running =2.47 to 4.2m/s [41]	Pedestrian
7	Distance (from a	On road = 0, (2). Out-of-road = 1 to 5	

	road)	meters	
8	Friction Coefficient	1(ice) to 8 (dry asphalt and concrete) with values 0.1 to 0.9 [228]	Road
9	Inclination	0 (flat) to 10%(sloppy)	
10	Width	2.5 to 4.6 meters	
11	Weather	Clear =0, foggy = 1, Cloudy=1.4, rainy = 2 [221]	Environmental Conditions
12	Time of day	Daylight = 0s, night-time=0.4s [222]	
13	Computation time	0.31s to 0.91s [72]	Computation Environment
14	Communication time	0.04s to 0.09s [72]	
15	Scenario	1 to 9 [232]	Scenario

Simulation traces are analyzed to calculate the risk level of the pedestrian at each simulation time. Then the risk levels are converted into beaconing rates, and beaconing rates are finally converted to energy consumption.

LTE is the wireless communication channel that connects servers with mobile devices of pedestrians and drivers. According to [235], LTE is 23 times less power efficient in comparison to Wi-Fi due to tail energy. It is also less power efficient than 3G. Their experiments show that energy per bit of LTE is 10μJ/bit. However, due to its large coverage area, high bandwidth, and fast response time, LTE is recommended for active traffic safety applications [72], [236].

Simulation Parameters

Simulation is conducted for two hours while running a fuzzy logic-based risk level prediction system every 0.1s. Vehicle arrival rates considered are 5, 10, 30, and 60 Vehicles Per Minute (VPM). A two-lane road is considered, and vehicles within a 1km radius from a pedestrian are monitored. The length of the packet is 1KB [237], and the smartphone battery capacity for analysis is 3000mAh. The important simulation parameters are summarized in TABLE 6.4.

TABLE 6.4. SIMULATION PARAMETERS AND VALUES

Parameter	Value
Simulation Period	2hrs
Simulation Interval	0.1s
Vehicle arrival rate	5, 10, 30, 60 VPM
Number of lanes	2
Maximum Vehicle Monitoring Radius	1000 meters
Smartphone Battery capacity	3000mAh
Packet/beacon size	1KB

6.4.3. SIMULATION RESULTS AND DISCUSSIONS

A fuzzy logic-based adaptive beaconing rate is compared with static full rate, half rate, and low rate beaconing types in terms of energy consumption over the simulation period, Figure 6.10. The simulation result is grouped into chunks of five minutes, and the energy consumption is summated. In adaptive beaconing rate, the frequency of beaconing is guided by the risk level of the pedestrian while high, half and low rates beaconing are constant over the complete simulation period. Since the pedestrian cannot be in the same risk level over the whole simulation time energy consumption of adaptive beaconing rate varies from time to time. Adaptive beaconing rate is more energy-efficient than high and half rate beaconing rates. This can be clearly seen from accumulated energy over time graph, Figure 6.11.

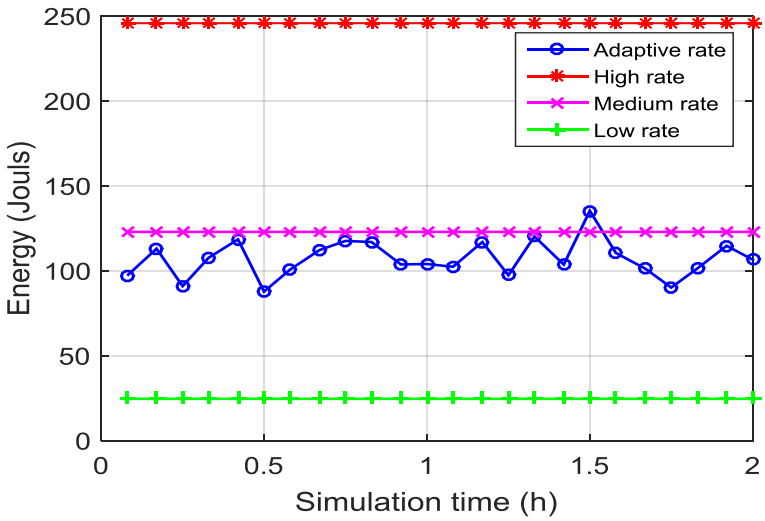


Figure 6.10: Energy consumed over simulation period

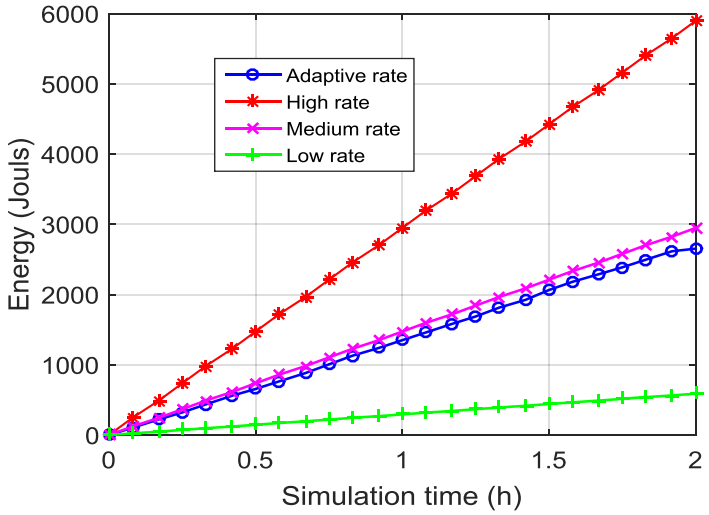


Figure 6.11: Accumulated energy over simulation period

A traffic safety system that involves high rate beaconing makes sure that the pedestrian is safe from accidents. However, beaconing at a constant high rate even in situations the pedestrian is in low or in no

collision risk area makes it the most energy-hungry process. A system that involves beaconing at a low rate, indeed, saves a lot of energy but it puts the road user in danger of traffic collision as an accident prediction algorithm lacks fresh data to estimate an imminent accident. Adaptive beaconing rate both saves energy and keeps the pedestrian safe from car accidents.

Figure 6.12 shows how the battery level of the mobile device used for simulation decreases over the simulation period. Low rate beaconing is the least energy-hungry while high rate beaconing is the most energy-hungry beaconing rate. The life time of a smartphone that uses adaptive beaconing rate is twice greater than the one that uses high rate beaconing.

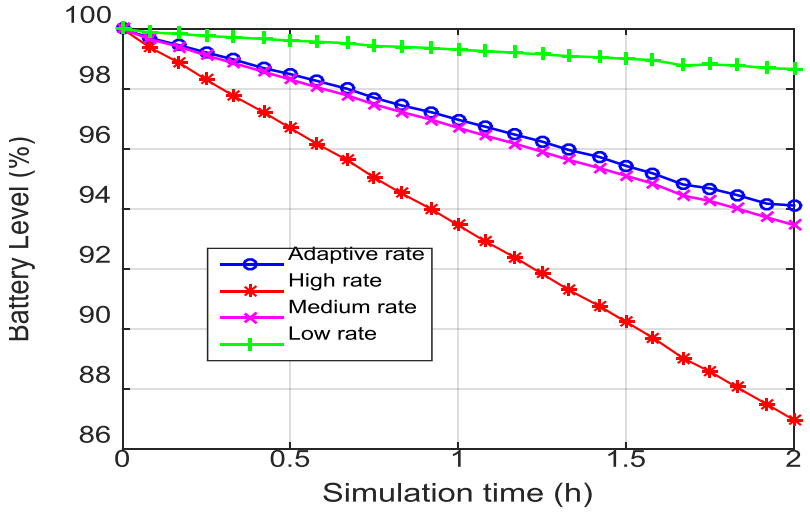


Figure 6.12: Battery level over pedestrian mobility period

The effect of the number of cars approaching a pedestrian on energy consumption of his mobile device, which is running traffic safety application that employs adaptive beaconing rates is assessed. TABLE 6.5 shows the vehicle arrival rate in a minute and estimated the speed of the vehicles. The energy evaluation of different arrival rates is displayed in Figure 6.13.

TABLE 6.5. VEHICLE ARRIVAL RATES AND ESTIMATED CORRESPONDING SPEEDS

Type	Car arrival rate (VPM)	Speed (m/s)
Crowded	60	2 -13.89
Urban	30	5 -20
Sub-Urban	10	5 – 30
Rural	5	10 – 40

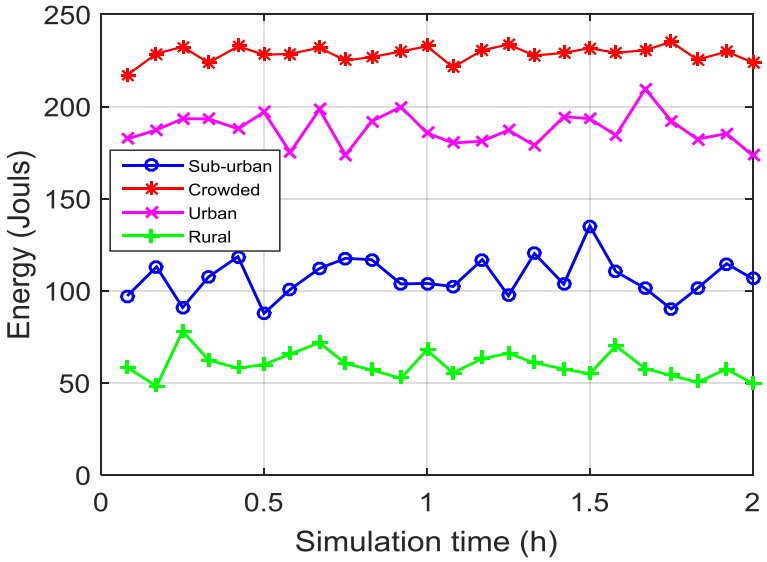


Figure 6.13: Energy consumed over simulation period for different vehicle arrival rates

A pedestrian in a road segment with an increased number of vehicles will be in the high-risk region most of his mobility period. This leads to more energy consumption as a high-risk level implies high beaconing rate. Because of the large number of vehicles, smartphones of pedestrians in urban area are more energy-hungry than rural if adaptive beaconing management is used. If the vehicle arrival rate is 60 VPM, almost the same energy as high rate beaconing is consumed. This means that most of his mobility period, the pedestrian is in high traffic risk region. Hence, to assure pedestrian safety, high rate beaconing is employed.

The last set of evaluations made is checking the effect of factors that aggravate traffic accidents on smartphones energy consumption that use adaptive beaconing rate management for traffic safety. Factors are categorized into two as *bad* and *good* environmental conditions. In *bad* environmental conditions, roads are slippery and down inclined. The driver's reaction time is influenced by distraction, alcohol, and age, the weather is rainy, and time of day is night. *Good* cases take values that reduce accidents for the stated factors. The results of energy consumption are displayed in Figure 6.14.

Factors that increase traffic accidents also increase energy consumption of mobile devices that run traffic safety applications relying on the adaptive beaconing rate. This is because, to be safe from accidents, beaconing rate needs to increase, and this ultimately increases energy consumption. However, with factors that increase traffic accidents, applications relying on adaptive beaconing rate spend much less energy than the ones relying on a high beaconing rate. The energy consumed due to worst environments conditions is approximately equal to safety application that involves constant half-rate beaconing. The proposed adaptive beaconing rate management enables to save a large amount of energy even in the presence of factors that escalate traffic accidents.

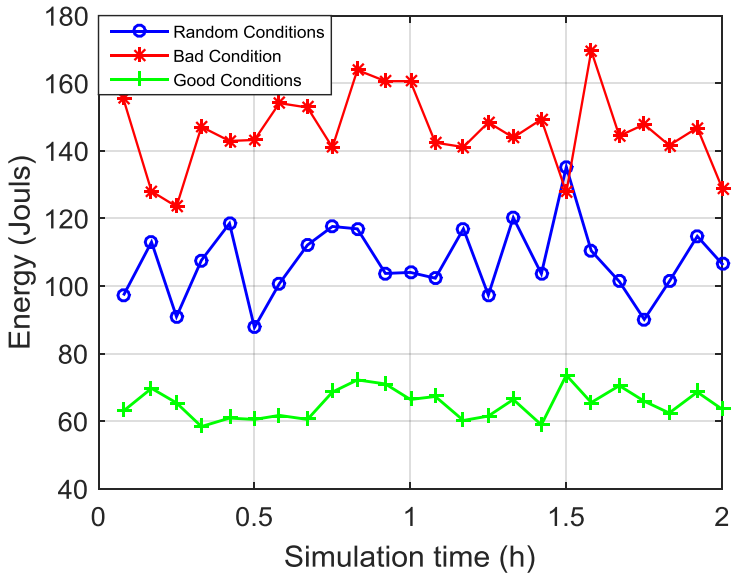


Figure 6.14: Energy consumed over simulation period for different environmental conditions

6.5/ CONCLUSION

PV-Alert is an active traffic safety solution that employs mobile devices of VRUs and drivers for collecting their position and other related data. However, the excessive energy consumption of mobile devices is a bottleneck to keep using the devices as part of the application. High beaconing rate requirement of traffic safety applications is the main reason for high energy consumption. The problem can be addressed by adjusting communication of the mobile devices according to the pedestrian's traffic risk level. For risk level identification, a fuzzy logic-based method is proposed. This is because the risk is a fuzzy concept, and most of the factors that affect risk level are imprecise and essentially subjective. According to the risk level, the beaconing rates values are adjusted. That is if the identified risk level is high, a higher beaconing rate is performed, and if the risk level is low, a lower beaconing rate is opted. The solution is feasible to husband energy since a pedestrian won't be in high collision risk level his entire mobility period.

The accuracy and ability to save mobile device energy of the system is evaluated. Comparison of the fuzzy logic-based model with a prediction system that relies on minimum distance for information exchange shows that more than 90% of risk levels predicted by the two methods are matched. This proves that the fuzzy logic-based collision risk level prediction system can predict the risk level of pedestrian accurately. The evaluation of energy efficiency of the system shows that the adaptive beaconing rate management can double the battery life of smartphone in comparison with the one that uses full-rate beaconing rate. Moreover, the energy-efficiency of the system is evaluated in urban and rural environments. The environments are distinguished with vehicle arrival rates. Mobile devices running the system are more energy-hungry when they are used in urban areas. Finally, the effect of

factors that influence traffic accidents on energy consumption is tested. Results indicate that factors that increase traffic accidents increase the energy consumption of smartphones. Based on all abovementioned results, it can be concluded that adaptive beaconing rate managements enables to save a huge amount of energy of mobile devices used in active traffic safety applications while ensuring traffic safety of road users.

The next chapter presents a subjective logic-based two-way trust management system proposed to ensure data security and user privacy in PV-Alert.

7

PV-ALERT: TRUST MANAGEMENT

7.1/ INTRODUCTION AND PROBLEM STATEMENT

Fog computing, which is an extension of cloud computing, is used to process a huge amount of information produced by numerous IoT devices. Hence, it is proposed for many applications [97], [98], [99], [100]. In PV-Alert fog computing is a central infrastructure that is responsible for taking CAM messages from VRUs and drivers and predicts accidents. In case of an imminent accident, fog servers forward DENM to both drivers and VRUs. However, due to its features and flexibility of deployment, fog computing is highly susceptible to information security and user privacy violations [18], [19], [110], [111]. Fog computing confronts new privacy and security challenges in addition to those assumed from cloud computing [19]. High mobility support, dynamic environment, geographical distribution, location awareness, proximity to end users, and lack of redundancy are among characteristics of fog computing which have a negative impact on its security and privacy despite their proven merits. Existing privacy and security remedies for cloud computing cannot be applied directly to fog computing as the architectures of the two computing paradigms are quite dissimilar [110]. Imposing security and privacy in cloud computing is relatively simpler because of the centralized component in comparison with distributed fog computing architectures. Apt measures need to be taken on security and privacy issues of fog computing to maintain its pace of acceptance and development in academia and industry.

Another challenge for a fog computing environment, which is much related to security and privacy, is trust management. Trust is defined as the level of assurance that an object will behave satisfactorily [238]. The behavior pertains to the Quality of Service (QoS) or the security policies that the object has to possess. Thus, a trustworthy object conforms to QoS requirements without violating any security policy. The level of assurance depends on the deployment environment, the type of network application, and the required level of security. For distributed environments like fog computing and for safety and security critical network application like traffic safety or health applications, a high degree of trust is needed. On the contrary, a low level of trust is demanded for centralized architectures for which other security mechanisms can be easily imposed and for applications whose reliability is not a priority [239]. In fog environment, devices may encounter other “strange” or new devices in the network, and the interaction with them should be carried out in caution since there is uncertainty on their behavior. To predict the future trustiness of an entity and avoid any uncertainty or risk about an entity, trust

management systems gather information about the entity from direct observations and recommendations of other entities. That is why Jin-Hee Cho et al., formulated trust management as one way of risk mitigation techniques which involves trust establishment and trust update tasks, among others [240].

There are two entities in trust management: trustor and trustee. The trustor is an entity that puts faith in the other entity, i.e. trustee. Trust can be delineated as trustor's belief in trustee's capabilities, honesty, reliability, etc. [241]. Trust is directional in that trustfulness of trustee does not depict whether the trustor itself is trusty or not. Moreover, trust is subjective meaning that what is trustworthy for one entity may not be trustworthy for the other.

Trust management enables objects in a network to determine the level of trustworthiness of another object. In other words, it provides a mechanism to decide whether to put faith in an entity to which a connection is going to be established. It allows detection of damaged or misbehaving nodes and enables autonomous communication among entities in a network [115], [239]. Trust is crucial for creating interaction in an uncertain environment [242]. It ensures information security and user privacy, and it is also related to reliability, integrity, dependability, and ability to perform a service [115].

Trust computation enables to calculate trust value of a target entity dynamically. An effective trust computation method has five design dimensions: trust composition, trust propagation, trust aggregation, trust update, and trust formation [243]. Trust composition determines the information required for trust computation. This information can be QoS and/or social relationship information. QoS trust refers to the belief of trustor that the trustee can provide a service with the desired quality [244]. Since, social relationships among human beings are also reflected by devices they own [245], [246], it can be used for trust computation. Trust propagation determines how trust values are stored and calculated. It can be either centralized or distributed. Trust update decides how often will trust of entities be updated. Trusts can be updated in an event driven and/or time driven fashion. Trust formation describes how to combine the trust properties determined by trust composition. Trust can be formed from either a single trust property or multiple trust properties. Trust aggregation decides how to integrate trust evidence from different recommenders and from own experience. Weighted sum, Bayesian inference, fuzzy logic, subjective logic, and regression analysis are some examples of trust aggregation techniques.

Even though trust management is a crucial and hot topic, it is a challenging problem to enforce in fog environment due to its flexibility of deployment. Fog nodes can be from different providers, they may be owned, operated, and maintained by different individuals or providers independently, and new nodes can join or leave the network anytime [19]. Geo-distribution and proximity of fog nodes to end users imply that the nodes are easily accessible, making them susceptible to corruption and rogue node built up by adversaries. Lack of redundancy, dynamicity, high mobility support, and low processing power of nodes [18] are among other properties of fog computing that adds complication to trust management in fog computing. Due to these reasons, fog servers are potential threats to not only fog clients but also to other fog servers. The same is true from fog clients' perspective.

In the traffic safety architecture presented in chapter 3 (PV-Alert), connected VRUs send their location and other associated data to fog servers periodically. This means that VRUs expose their location continuously. This poses privacy concern. Fog-based traffic safety applications in general are most susceptible to privacy violation. Due to the following reasons, maintaining privacy in such type of applications is challenging.

- Since the traffic safety application is a hard-real-time application, it is hard to apply location accuracy preservation methods as most of them involve computations that introduce a delay in response time.
- In PV-Alert, privacy and security can be violated at multiple places: mobile devices, in the communication channel, fog node, and cloud server. It is challenging to find privacy preservation method that works across all the components.
- Positions of VRU and drivers should be sent continuously to the fog server at very a high rate for the whole mobility period of the VRU. Protecting the privacy of continuous user position updates in real-time as used for online tracking remains a challenging problem [247].
- Even though trajectories of VRUs are unpredictable, they are on known walkways. This makes the application susceptible to map matching attacks.
- The application runs in a distributed environment where relatively simple and matured centralized privacy mechanism is not possible.

Because of the reasons pointed above, we believe that user privacy and data security issues should be solved indirectly using trust management. Trust management ensures privacy and security. Therefore, the problem of privacy can be addressed by enabling VRUs to connect to only trusted fog servers. Fog servers in their turn allow connection request of only trustworthy VRU devices. In fog networks trust should work in two-ways so that fog clients can verify fog servers that they can provide the right, reliable, and secure services. On the reverse, fog servers must be able to check the legitimacy and roguery of fog clients based on their trust values.

Hence, this chapter presents a subjective logic-based system which aggregates trusts using a specific version of belief theory called subjective logic [248]. In the novel two-way, scalable, and efficient trust management solution trustor and trustee evaluate each other by exchanging their trust computation role to create trusted data communication. The distributed and event-driven trust management system considers both QoS and social trust metrics to determine the trust of a fog node. The trust values are calculated using the information obtained from self-observation and recommendations of neighboring nodes. The accuracy, convergence, and resilience of the solution are demonstrated by conducting extensive evaluations using a simulation tool developed for this purpose. Evaluations made include the effect of the weight of direct and indirect trust values and the effect of the number of malicious or bad nodes in the network. Additionally, different derivatives of the trust management system are produced, and a comparative analysis is made on the effectiveness of selecting the right service providers among a

set of good and dishonest servers. Experimental evaluation demonstrates that the two-directional trust management surpasses one-way trust management system in opting more trusted service providers.

The remainder of this chapter is organized as follows. Section 7.2 discusses related works in trust management in fog computing and other related computing environments. The system model of Two-way Trust Management (TTM) and the trust metrics comprised in the system are discussed in section 7.3. This section also explains the proposed subjective logic-based trust management system. Performance evaluations made are detailed in section 7.4. Finally, section 7.5 concludes the chapter.

7.2/ RELATED WORKS

Because of limited works on trust management in fog computing and similarities of the computing paradigm to IoT systems and cloud computing, selected related researches in these domains are reviewed. Many trust management mechanisms are introduced for IoT systems [115], [243], [249], [250], [251], [252], [253],[254], [255], and cloud computing [116], [256], [257], [258], [259], [260], [261], [262]. These mechanisms allow to select trusted nodes for reliable and secure communications and take single or multiple QoS and social trust metrics [249], [250]; the QoS trust metrics being more studied than social trust metrics [243].

In [253], a fuzzy reputation-based trust management system that considers only QoS trust metrics is presented. The final trust is computed from trust information obtained from direct observation and from recommended indirect trusts. The main drawback of this work is ignorance of social relationships among devices on the Internet. A series of works by Fenye Bao et al [249], [250], [251], [252] emphasized on social relationships among IoT devices to define trust management systems for IoT applications. Trusts are calculated from information obtained from both direct observation and opinions of other nodes based on trust metrics like honesty, cooperativeness, Community of Interest (COI), friendship, etc. and their solutions are evaluated mainly for trust assessment accuracy and convergence. [252] focuses on addressing the problem of misbehaving nodes whose characters may change over time. A scalable, adaptive, and survivable trust management system is presented in [251]. Scalability of the trust management system is achieved by keeping trust information of the subset of nodes encountered using a defined storage strategy. The main contribution of [249] is the introduction of a novel adaptive filtering technique to determine the best way to combine direct and indirect trusts so that convergence time and trust estimation bias are minimized. More recent works on trust management on Social Internet of Things (SIoT) include [254], [255]. A recommendation and reputation-based trust computation model for distributed SIoT networks, which is able to converge in few iterations is discussed in [254]. However, the method depends solely on social trust metrics and final trust scores do not include knowledge from direct observation in the trust computation. A context-aware trust management system for SIoT is proposed in [255] to prevent attacks of malicious nodes which acts dishonestly based on a

context. Three trust contexts are identified using context-aware QoS and social similarity-based trust metrics are used to identify honest and dishonest devices effectively.

Trust in cloud computing enables service consumers to select a cloud service provider with desired reliability, quality, and performance. If the service consumer has no prior experience with a cloud service provider, it is challenging to put faith in the service offered [116]. Trust is vital for fast adaption and growth of cloud computing [256], [257]. However, non-transparent nature of cloud services has made trust management in a cloud environment challenging [257]. Yet, there are many published works on recommendation, prediction, reputation, and policy-based trust management in cloud computing [258]. Most of these works rely on verification of Service Level Agreement (SLA) [259] and QoS attribute information [260]. Some works consider identity and interaction history in trust computation. A behavior graph and service grouping based trust evaluation method that encompasses relationship parameters such as identity, interaction evolution, and service quality attributes such as availability and reliability are proposed in [261]. Other trust metrics that depict social relationships like honesty and sincerity can also be used in trust computation for a cloud computing environment. Ing-Ray Chen et al., proposed a scalable trust protocol which depends on social trust metrics for mobile cloud IoT systems [262]. The protocol named IoT-HiTrust allows IoT devices to report their experiences and query the service trustworthiness of other IoT device through cloudlets.

Trust management in fog environment is different from trust management in a cloud environment in varies ways from their architecture to ways of deployment. The distributed nature of fog architecture complicates trust computation because of lack of a global centralized entity that enables to impose traditional security mechanisms like authentication and access control to allow secure and trusted communication [110], [263], [264]. Secondly, mobility support, location awareness, a huge number of nodes, the low processing power of nodes are among the features of fog computing that pushes to strive for dynamic, scalable, and computationally efficient trust management system. Thirdly, the flexibility of deployment of fog computing makes fog environments more vulnerable to trust-based attacks [19]. Trust in cloud environments is more-or-less unidirectional. In contrary, the two-way requirement of trust is another issue that makes trust issue a formidable challenge in fog computing [110]. Fog nodes that provide services must be able to evaluate the trust level of nodes that request services and service requestors must also be able to check whether they depend on trusty service providers.

Hence, trust is one of the issues that have to be addressed to boost the acceptance of fog computing in industries [112]. However, little work is done on trust management in fog computing. Most of the works that deal with trust in fog computing merely affirm imperativeness of trust management in the environment. Only a handful of works that suggest particular methods for trust computation in fog computing till the end of 2018 are found. Rahman et al., in [263] identified a fuzzy logic configuration that affects trust values of a fog node. Distance, latency, and reliability are trust metrics considered in the configuration. The work provides some insights to the definitions of trust and advantage of fuzzy

logic for trust evaluation for fog computing. The same authors as in [263] extended their work to propose a broker-based trust evaluation framework for fog service allocation [117]. However, the proposed work conceives only QoS trust metrics, and it is unidirectional. In addendum, usage of broker implies malfunctioning of the broker results in a complete cessation of the trust evaluation framework. A summary of some related trust management works in IoT, cloud computing, and fog computing research domains from the five trust dimensions of trust computation perspective are presented in TABLE 7.1.

TABLE 7.1. SUMMARY OF WORKS ON RELATED TRUST MANAGEMENT SYSTEM FROM FIVE DIMENSIONS OF TRUST COMPUTATION

Research Domain	IOT	Cloud Computing	Fog Computing
Trust Composition	Social Trust [249], [250], [251], [254], QoS Trust [253] and both [252], [255]	QoS Trust [260], [261], QoS from SLA [259]	QoS including mobility and distance [117]
Trust Propagation	Distributed [249], [250], [251], [252], [253], [254], [255]	Centralized [259], [260], [261]	Distributed [117]
Trust Update	Time-driven [249], [252], [253] & Event-driven [250], [251]	Event-driven [259], [260], [261]	Event-driven [117]
Trust Formation	Multi-trust [249], [250], [251], [252], [255] & Single-trust [253], [254]	Multi-trust [259], [260], [261]	Multi-trust [117]
Trust Aggregation	Bayesian Systems [249], [251], Weighted sum [250], [252], [254], [255], Fuzzy-logic [253]	Weighted Sum [259], [260], [261]	Fuzzy-logic [117]

Our work is different from the aforementioned ones. Firstly, the work involves two-way trust computation where fog server checks trustworthiness of fog clients and fog clients checks back if the server is fit to provide a service. Secondly, we have considered QoS trust information besides considering social relationship information among nodes. The trust management system relies on both self-observations and recommendations from neighboring nodes, which are combined adaptively. Our bidirectional trust management solution does not depend on any third-party component. Multiple recommendation trusts are assembled using a trust aggregation technique called subjective logic. It is a kind of a belief theory and suggested to be most appropriate for fog computing [239], [243].

7.3/ SUBJECTIVE LOGIC-BASED TRUST MANAGEMENT SYSTEM

In this section we cover three important topics in relation to the trust management system proposed. First, the system model conceived, and trust metrics used in TTM are explained. Next, subjective logic and trust computation are discussed. Finally, the two-way trust management algorithm is presented.

7.3.1. SYSTEM MODEL

The two-way trust management system is based on a simplified fog computing environment whose system model is shown in Figure 7.1.

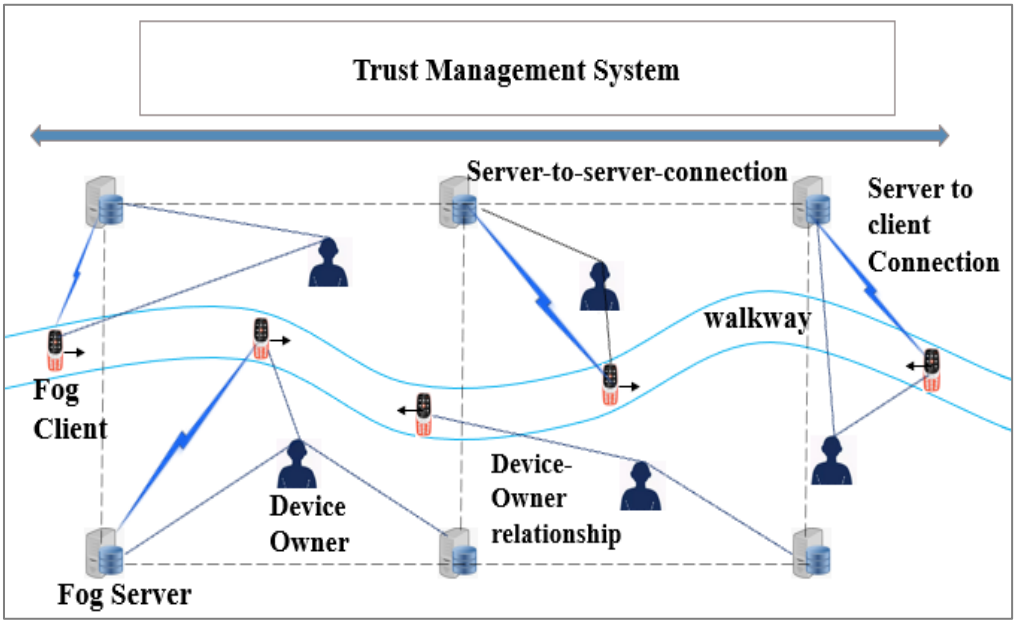


Figure 7.1: System model of the two-way trust management system

The architecture of fog computing may contain more than one layer [90]. However, without losing generality, we have conceived a single-layered fog computing environment. Fog servers can be mobile, and multiple devices may be combined to form a fog node [89]. We assumed that single static devices as fog nodes. We also assume that fog servers are evenly arranged on both sides of a road as shown in the diagram above. The reason for this arrangement is to test the robustness of TTM algorithm in selecting trusted servers among many neighboring servers. Fog server can communicate with neighboring 1-hop fog nodes, i.e. fog servers and fog clients. Fog client in fog computing can be user carried devices like mobile devices, laptops, or non-user accompanied devices like smart lighting, smart washing machine, Closed Circuit TV (CCTV) or video surveillance, etc. [265]. This research is about the first group of devices which are carried by pedestrians. Fog clients are mobile on a predefined trajectory. Fog clients can communicate with other neighboring fog servers. Each fog node has an owner, and a person may own more than one node or device. The high-level description of how the proposed system works and trust-related information considered to compute trust levels of fog nodes are presented below.

How it works?

A mobile device of VRU (i.e. fog client) intending to get a traffic safety application service, requests a fog server for a connection. The fog server then wants to ensure that its connection is with a trusted (non-rogue) fog client. Therefore, to capture a malicious or bad fog client, the server calculates the trust value of the client by dynamically combining indirect trust obtained from neighboring servers and from

its direct observation. Detected fraudulent clients will then be refused for the service, and its trust value will be stored to monitor the client further. The value will also be sent to servers that request for trust level of the client as recommendations. A fog client which is allowed to connect to the server, in its turn wants to make sure that the fog server is trustable, and can give the right service. A malicious fog server may provide wrong or incorrect service posing the VRU for accidents. The fog client consults neighboring fog servers besides its direct observation to determine the trust status of the server. Just like fog servers, fog clients also propagate their experience about the server to other nearby servers. Trust management systems do not require disseminating trust information over the entire network [266]. Therefore, nodes only keep and exchange trust information about neighboring nodes within the radio ranges for computational efficiency.

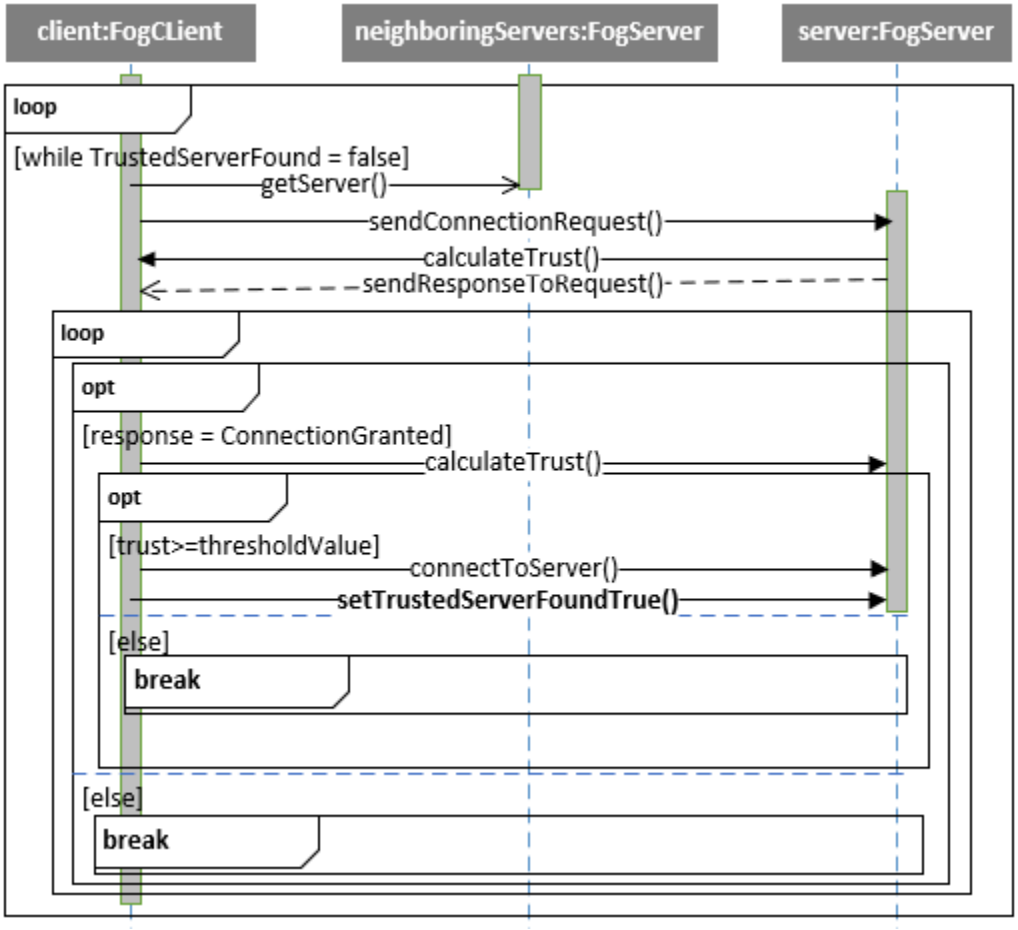


Figure 7.2: Dialog between fog clients and fog servers

The sequence of communication between fog client and fog server to create a trusted connection is depicted in Figure 7.2. The conversation is summarized as follows. A fog client sends a connection request to a fog server. The server evaluates the trust value of the client and allows the connection if the client is trustworthy; otherwise, it refuses the connection. If the client is granted a connection, it evaluates the trust value of the server and establishes connection if the server is trustworthy. If the server refuses the connection, or the server is found to be untrustworthy, the client sends a connection request

to another server. This conversation continues until a trusted service provider is found among neighboring fog servers.

Trust Metrics

A trust metric or trust property is the information needed to calculate the trust level of a node. In the TTM system, more than one trust properties are used to evaluate the trust of fog servers and clients. Choice of trust property depends on the issue the trustor is interested in [116], [240], [244]. QoS trust evaluates the capability of a fog server to complete a requested mission successfully. Since fog client's interest is to select a server that can provide the services properly, more QoS are used, and selection of clients by servers largely relies on social relationships. Metrics used by fog servers to evaluate trustiness of fog clients are friendship, honesty, and ownership, while fog clients use latency, PDR and ownership to evaluate the trust value of a server. The definitions of the metrics and how they are calculated are explained underneath:

- *Latency*: the time required by a fog server to provide a service to a fog client. High latency and irregularities in response time predict possible intrusions in the system [267]. The value is returned from the latency response-time model produced using log-normal distribution [268] with the mean and standard deviation taken from latency evaluation of PV-Alert [56].
- *PDR*: is the ratio of packets successfully received to the total sent. It is the ratio between the number of packets received by the application layer of destination nodes to the number of packets sent by the application layer of the source node. In the solution proposed, PDR is modeled using a well-known packet loss model called the Gilbert-Elliott model [259]. The parameters of the model are obtained from packet loss observation of links of a good and bad node [270]. Hence, the probability of transferring from good state to the bad state, and the probability of transferring from the bad state to the good state are generated based on the PDR result PV-Alert [56].
- *Ownership*: each fog node has an owner. This metric is included with the assumption that devices owned by the same person are trustable each other [245]. Therefore, if the same person owns a fog server and a client, the value of ownership metrics is one; otherwise, it is zero.
- *Friendship*: refers degree of closeness of a node in comparison with other nodes. Instead of defining it initially in friendship matrix [249], [271], calculation of friendship in the solution presented in this chapter relies on interaction history. It follows the maturity model proposed in [266], in that, the more positive interaction experiences between two nodes implies more trust and confidence between them. Friendship is calculated as the ratio of the number of successful connection requests of a client to the maximum connection of all requests. A connection request is said to be successful if the request is accepted by the server. A server accepts clients connection request if the client's trust is above the required threshold value.
- *Honesty:* evaluates the belief that a node is dependable based on another node's direct observation over a given period of time [250], [252], [271]. It is calculated by keeping a count of suspicious

dishonest experiences of a trustee node as observed by trustor node during a time period. The detection involves a set of anomaly detection rules such as a high discrepancy experienced in the recommendation, as well as interval, retransmission, repetition, and delay rules. Hence, honesty is figured out as the ratio of valid trust propagations and realized connection requests. Realized connection requests are those resulted in a trusted connection between trustor and trustee. Exaggerated fog clients' recommendations are conceived as invalid propagations, and connection requests from nodes of low trust values are rejected.

7.3.2. SUBJECTIVE LOGIC AND TRUST COMPUTATION

Trust computation enables to calculate trust value of a target entity dynamically. If the trust value is acceptable, then trusted data communication follows; otherwise, entities abstain from untrusted connection to other entities. To establish trust values, an effective trust computation method has five design dimensions [243]. As stated earlier, the TTM system uses QoS and social trust metrics and it is distributed, event-driven, and multi-trust system. This section discusses subjective logic and its application for trust aggregation, how final trust values of fog nodes are calculated from direct and indirect trusts, the details of TTM algorithm and the justification for the resilience of the proposed system to thwart trust-based attacks.

The TTM system staged in this chapter uses subjective logic to aggregate recommendations from neighboring fog servers. Though subjective logic has the ability to defend trust-based attacks because of its discounting step, it is less explored [243]. This section briefly introduces subjective logic and shows how it is used in the trust management system.

Subjective logic

Standard logic is designed for an idealized world where propositions can be either evidently true or false [272]. However, in the real world, nobody can be absolutely certain whether a proposition is true or false, and the assessment of the proposition is individual, i.e. not general and objective [273]. Therefore, many calculi and logic-based methods which consider uncertainty and ignorance have been proposed. These methods allow concluding a proposition with insufficient evidence. Trust is one of such propositions since it is a statement or assertion that expresses a judgment or opinion about an object. Subjective logic, which is a special form of belief theory, builds on the belief that trust is subjective, and it is differently experienced by everyone [274]. It is not practical for recommenders to consider all pertinent trust metrics to evaluate the trust value of a node. This implies that trust is computed with insufficient evidence and each node in a fog computing environment computes its own trust value subjectively for each node it encounters.

In subjective logic, uncertain probabilities are represented with belief model as opinion. Opinion or degree of trust of a node x, ω_x, is defined with 4-tuples [248] as:

$$\omega_x = (b_x, d_x, u_x, a_x) \quad (7.1)$$

where b_x is the belief that the node is trustable, disbelief d_x denotes the doubt that the node is trustable, u_x is uncertainty to conclude that a node is trustable or not, and atomicity a_x is the prior probability of x without any evidence. If the value of atomicity is 0.5, an opinion has an equal probability of giving true or false output. Note that the sum of belief, disbelief, and uncertainty must be equal to 1. The degree of trust represented as a 4-tuple opinion can be converted into a single-valued trust value using the equation:

$$p(x) = b_x + a_x * u_x \quad (7.2)$$

To illustrate this using an example, suppose the probability of rain falling in Paris on 25 October 2019 is 0.4, the chance of no rain is 0.3, and the uncertainty of raining is 0.3. Assuming equal chance of giving a true or false output, this can be represented as opinion in the form ω_x = (0.4, 0.3, 0.3, 0.5) and uncertain probability is 0.4 + 0.5*0.3 = 0.55.

Now the challenge is how to get the values of the tuples of subjective trust from the interaction among fog nodes. To calculate the degree of trust of nodes in fog networking, the values of belief (b_x), disbelief (b_x), and uncertainty (u_x) of a node x can be obtained from its positive and negative experience [272]. If positive and negative experiences are denoted by *p* and *n* respectively, then the three variables can be calculated using the following set of equations:

$$b_x = \frac{p}{n + p + 1} \quad (7.3.1)$$

$$d_x = \frac{n}{n + p + 1} \quad (7.3.2)$$

$$u_x = \frac{1}{n + p + 1} \quad (7.3.3)$$

Fog node count good and bad experiences of another node it came across and forward this value as a subjective trust when they are asked to recommend. Recommended trusts have to be weighted and combined to get the final trust value. There are two ways of combining trust recommendations in subjective logic; *discounting* and *consensus*. They are described hereafter.

- *Discounting*: A node computing trust value of another node scales the recommendations it received using discounting (denoted by the operator $\otimes$) with the trust values the node has about the recommenders. Hence, trust values from trusted recommenders will have more weight than less trusted ones. This is essential to defend trust-based attacks. Testimonial requester has trust values of the recommenders from previous communications. Suppose a trustor node, *i*, has a subjective trust value of a recommender node *k* as $T_{i,k} = (b_{i,k},\ d_{i,k},\ u_{i,k},\ a_{i,k})$ and the recommender has trust value of trustee node *j* as subjective trust $T_{k,j} = (b_{k,j},\ d_{k,j},\ u_{k,j},\ a_{k,j})$. See the visual representation of the statement in Figure 7.3 a). Then the indirect trust of node *j* as evaluated by *i* based on *k*'s

recommendation is calculated as:

$$T_{i,j} = (b_{i,k}b_{k,j}, b_{i,k}d_{k,j}, d_{i,k} + u_{i,k} + b_{i,k}u_{k,j}, a_{k,j}) \quad (7.4)$$

- *Consensus:* Recommendations from several recommenders are combined using consensus (denoted by operator $\oplus$). Suppose node *i* and *k* have recommendations about node *j* as $T_{i,j} = (b_{i,j},\ d_{i,j},\ u_{i,j},\ a_{i,j})$ and $T_{k,j} = (b_{k,j},\ d_{k,j},\ u_{k,j},\ a_{k,j})$, respectively, see Figure 7.3 b). The combined recommendation for *j* is given by 7.5.1:

$$\mathrm{T}_{ik,j} = (\frac{\mathrm{b}_{i,j}\mathrm{u}_{k,j} + \mathrm{b}_{k,j}\mathrm{u}_{i,j}}{k}, \frac{\mathrm{d}_{i,j}\mathrm{u}_{k,j} + \mathrm{d}_{k,j}\mathrm{u}_{i,j}}{k}, \frac{\mathrm{u}_{i,j} * \mathrm{u}_{k,i}}{k}, \mathrm{a}_{ik,j}) \quad (7.5.1)$$

where,

$$k = \mathrm{u}_{i,j} + \mathrm{u}_{k,j} - \mathrm{u}_{i,j}\mathrm{u}_{k,j} \quad (7.5.2)$$

$$\mathrm{a}_{ik,j} = \frac{\mathrm{a}_{i,j}\mathrm{u}_{k,j} + \mathrm{a}_{k,j}\mathrm{u}_{i,j} - (\mathrm{a}_{i,j} + \mathrm{a}_{k,j})\,\mathrm{u}_{i,j}\mathrm{u}_{k,j}}{\mathrm{u}_{i,j} + \mathrm{u}_{k,j} - 2\mathrm{u}_{i,j}\mathrm{u}_{k,j}} \quad (7.5.3)$$

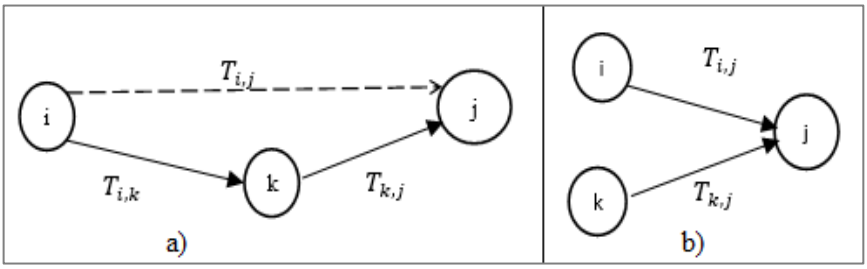


Figure 7.3: a) Discounting and b) Consensus operators

Overall indirect trust is calculated by applying *discounting* and *consensus* together on the recommendations obtained from all neighboring 1-hop nodes as subjective trust. So, as to get more reliable recommendations and to be more resistant to trust-based attacks, recommendations can be taken only from trusted recommenders by applying threshold-based filtering [244]. However, in the case of the proposed solution, as the number of neighboring nodes might be limited, all recommendations are taken, and trust-based attacks are taken care of by the trust aggregation method. Suppose a node, *i*, has trust value of recommenders $r_1, r_2, \dots, r_k$ at time *t* as $T_{i,r1}(\mathrm{t}),\ T_{i,r2}(\mathrm{t}), \dots, T_{i,rk}(\mathrm{t})$ respectively, and the recommenders have trust towards node *j* at time *t* as $T_{r1,j}(\mathrm{t}),\ T_{r2,j}(\mathrm{t}), \dots, T_{rk,k}(\mathrm{t})$, see Figure 7.4., then by applying *discounting* and *consensus* operations, the final cumulative indirect trust of node *j* as evaluated by *i*, is calculated using equation 7.6.

$$T_{i,j}^{Indirect}(t) = (T_{i,r1}(t) \otimes T_{r1,j}(t)) \oplus (T_{i,r2}(t) \otimes T_{r2,j}(t)) \oplus \dots \oplus (T_{i,rk}(t) \otimes T_{rk,j}(t)) \quad (7.6)$$

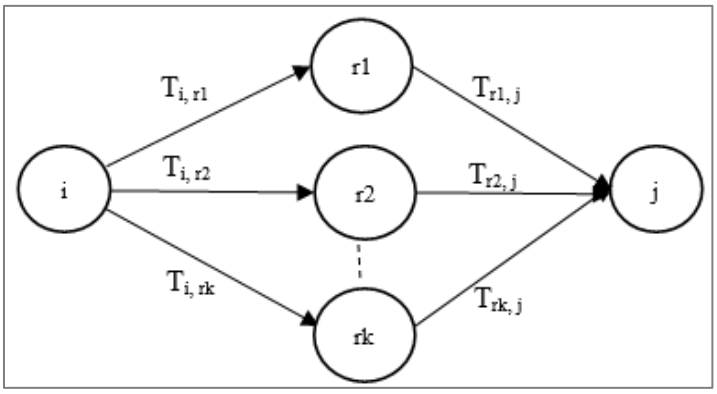


Figure 7. 4: Computation of overall indirect trust

The trust management system relies on the trust value of a node calculated from direct observation in addition to recommendations. Trust metrics defined above are used to calculate direct trust. Direct trust value of a node *j* as it is evaluated by node *i* at time *t* is calculated using the following formula:

$$T_{i,j}^{Direct}(t) = \alpha * T_{i,j}^{X}(\mathrm{t}) + \beta * T_{i,j}^{y}(\mathrm{t}) + \mu * T_{i,j}^{z}(\mathrm{t}) \quad (7.7)$$

Where *x*, *y*, and *z* are trust metrics and α, β, and μ are weighting factors of individual trust metrics. For fog servers, *x*, *y*, and *z* are latency, PDR, and ownership, respectively while for fog clients they are friendship, honesty, and ownership, respectively. The weighting factors of the QoS and social trust metrics are adjusted adaptively based on belongingness of trustor and trustee to an owner and reputation of the trustee. Reputation, in this case, refers to overall trust value of a node in previous encounters. If the trustor and trustee are owned by the same person or reputation of a trustee is above a threshold trust value that splits complete trust and distrust, average values of the existing trust metrics are taken. Otherwise, half the weight provided for the other trust metrics is assigned to ownership metrics. This formulation is clarified in the following pseudocode.

if (trustor & trustee are owned by same person OR reputation of trustee > threshold trust value)

$\alpha = \beta = \mu = 0.33$

else

$\alpha = \beta = 0.4$

$\mu = 0.2$

This simple weighting procedure encourages nodes with good reputations and penalizes bad ones. Furthermore, the procedure is suitable for resource-constrained fog clients.

Calculating direct and indirect trust values paves a way to compute the overall final trust level of a node. It is calculated using the following formula:

$$T_{i,j}(t) = \gamma * T_{i,j}^{Direct}(\mathrm{t}) + (1 - \gamma) * T_{i,j}^{Indirect}(\mathrm{t}) \quad (7.8)$$

γ is the factor that specifies the contribution of direct and indirect trusts on the overall trust value. The contribution of indirect trust value ($\gamma_{Indirect} = 1 - \gamma$) to overall trust is adaptively decided based on the trust value of trustee in preceding trust computation ($T_{i,j}(t - \Delta t)$), number of recommenders (n(rec)), and maximum possible recommenders the configuration allows (max(rec)), see formula 7.9.

$$\gamma_{Indirect} = \frac{n(rec) * T_{i,j}(t - \Delta t)}{\max(rec) + n(rec) * T_{i,i}(t - \Delta t)} \tag{7.9}$$

The indirect trust weighting factor is normalized to the past experience and the current number of recommenders relative to the maximum possible number of recommenders a fog node can have in the setup. The formula ensures that the contributions of indirect trust do not exceed more than half of the overall trust and an increase of the contribution proportionally with a number of recommenders. Providing more weight to direct trust and using more recommendations leads to accurate and fast converging trust values [252].

7.3.3. TWO-WAY TRUST COMPUTATION ALGORITHM

The detailed steps of the two-way trust computation algorithm are described in Algorithm 7.1. The final trust value is in the range of [0, 1], where 0 implies complete distrust and 1 is complete trust. The ignorance or threshold point at which trust and distrust are dissected depends on the type of application. For most applications, it is 0.5, but for safety-critical and health applications the value is usually higher. TABLE 7.2 displays important notations used in the algorithm.

TABLE 7.2. LIST OF IMPORTANT NOTATIONS FOR THE ALGORITHM

Notation	Description
Clients = {C_1, C_2, …, C_n}	List of Fog Clients
Servers = {S_1, S_2, …, S_m}	List of Fog Servers
$T_{i,j}$	Trust of node j as evaluated by node i
$\boldsymbol{T_{i,j}^{X}}$	Trust of node j as evaluated by node i w.r.t trust metrics or trust type X
I[2][Ci]	Interactions between a server and client C_i
R[2][Ci]	Interactions realized by client C_i
P[2][Ci]	Propagations made by client C_i
$STrust_i$	Subjective trust of a node defined as belief, disbelief, uncertainty and atomicity
α1, β1, μ1, γ1	Adaptively calculated weighting factors for trust computation of clients
α2, β2, μ2, γ2	Adaptively calculated weighting factors for trust computation of Servers

Fog clients initiate trust computation by sending a connection request to a nearby fog server. The fog server checks the trustworthiness of the client (i) by computing direct trust from friendship, honest and ownership trust metrics, steps 4-13, and (ii) by consulting and aggregating recommendations from neighboring servers using subjective logic, steps 14-20. At step 21, direct and indirect trusts are combined based on their respective weights to determine the final trust value of the client.

Algorithm 7.1: Two-way trust computation Algorithm

Inputs: $\{C_1, C_2, \ldots, C_n\}$, $\{S_1, S_2, \ldots, S_m\}$, $\alpha_1, \beta_1, \mu_1, \gamma_1, \alpha_2, \beta_2, \mu_2, \gamma_2$(adaptively calculated)

Output: Trusted connection established

Steps:

for $i = 1$ to n ▷ *Iterate over clients*

ns = neighboring servers of client C_i

for j = 1 to ns. size

▷ Calculate direct trust of Ci

$T^{Friendship}_{i,j} = C_i.I[1][j] / Max(C_i.I[1][k] \mid_{k = 1, 2, \ldots, n})$

$T^{Honesty}_{i,j} = (C_i.P[1][j] + C_i.R[1][j]) / (C_i.P[0][j] + C_i.P[1][j] + C_i.R[0][j] + C_i.R[1][j]))$

if C_i and S_j are owned by same person and Trust of $C_i > threshold_1$

$T^{Ownership}_{i,j} = 0.33$

else

$T^{Ownership}_{i,j} = 0.2$

end if

$T^{Direct}_{i,j} = \alpha_1 * T^{Friendship}_{i,j} + \beta_1 * T^{Honesty}_{i,j} + \mu_1 * T^{Ownership}_{i,j}$

▷ Calculate indirect trust of C_i

$STrust_i$ = Initial Subjective Trust Value of C_i

for $a = 1$ to ns.size

$discounting = T_{j,a} \otimes T_{a,i}$

$STrust_i = STrust_i \oplus discounting$

end for

$T^{Indirect}_{i,j} = STrust_i.Belief + STrust_i.Uncertainty * STrust_i.Atomicity$

$T_{i,j} = \gamma_1 T^{Direct}_{i,j} + (1 - \gamma_1) T^{Indirect}_{i,j}$

if $T_{i,j} \geq threshold_1$

▷ If the client is trusted, calculate trust of S_j

$T^{Latency}_{j,i}$ = logNormalResponse(mean, SD)

$T^{PDR}_{j,i}$ = gilbertElliott_Model (p, r)

if C_i and S_j are owned by same person Trust of $Si > threshold_2$

$T^{Ownership}_{j,i} = 0.33$

else

$T^{Ownership}_{j,i} = 0.2$

end if

$T^{Direct}_{j,i} = \alpha_2 T^{Latency}_{j,i} + \beta_2 T^{PDR}_{j,i} + \mu_1 * T^{Ownership}_{j,i}$

▷ Calculate indirect trust of S_j

$STrust_j$ = Initial Subjective Trust Value of S_j

for $a = 1$ to ns.size

$discounting = T_{i,a} \otimes T_{a,j}$

$STrust_j = STrust_j \oplus discounting$

end for

$T^{Indirect}_{j,i} = STrust_j.Belief + STrust_j.Uncertainity * STrust_j.Atomicity$

$T_{j,i} = \gamma_2 T^{Direct}_{j,i} + (1 - \gamma_2) T^{Indirect}_{j,i}$

if $T_{j,i} \geq thrushold_2$

▷ make trusted connection

end if

end if

end for

end for

If the final trust is greater than or equal to the minimum threshold trust value the server expects, it allows the connection. In this case, it is fog client's turn to assure if the fog server is a trusted service provider. Hence, it executes steps 23 - 39 to find out the trust value of the server. Two QoS trust information, latency and PDR, and a social relationship trust information, ownership, are used to calculate the direct trust value of the server. Recommendations are collected from neighboring servers and aggregated to form the indirect trust. Next, the last trust value of the server is decided from weighted sum of direct and indirect trusts. If the server has acceptable trust value, a trusted connection is established between the fog server and fog client. If either fog server or fog client is untrustworthy, then the client sends a connection request to another server, and the steps described above are repeated. The name two-way trust management is given because of trust computation involved from the fog server to the fog client and from the fog client to the fog server.

Resistance of the model to Trust-based Attacks

Service requesters must have the desired level of trust value since service providers entertain only trusted requesters. Service providers want to be profitable by serving as many service requesters as possible. Hence, nodes related in trust computation and sharing may be involved in trust-based attacks. A malicious node may transmit wrong information about another entity or itself, collude with others to control service, or may also act incorrectly to mischief those in trust relation. A list of trust-based attack models [243] with definitions and how effective is the TTM algorithm to thwart those attacks is presented in this section.

- *Self-Promotion Attack (SPA)*: if a malicious object is requested about its trust value, it provides good recommendation, and once it is selected, it may provide poor service or abuse the network. The trust management system presented is fully resilient to SPA because in the algorithm a node can't recommend itself.
- *Ballot-Stuffing Attack (BSA):* a type of collusion attack where malicious recommender gives exaggerated trust value about a bad object to trust information requester with an intention of increasing reputation of the object. In the proposed trust management system, a bad fog server may send incorrect recommendations about a fog node, and a bad fog client may also propagate false trust information to neighboring servers. The problem is addressed by the selected trust aggregation method. In the method, recommendations are weighted based on the trust level of recommenders. Consequently, a recommendation of a bad node will have a very small contribution to the overall indirect trust. The second solution applied to fight back BSA is ignoring exaggerated values of recommendations.
- *Bad-Mouthing Attack (BMA):* even though an object is trustable, colluding recommenders provide false trust values to vituperate false information about the object. When malicious nodes are selected because of false information, they get access to resources posing security threats to the entire system. This kind of attacks is viable to happen, but solutions applied for BSA address this attack too.

- *Opportunistic-Service Attack (OSA)*: trust management systems decrease the reputation of malicious nodes from time to time. When the node notices that its reputation is dropping, it performs good service, and when its reputation is high, it starts giving bad service. OSA is dealt with monitoring the behavior of a node and removing it from the network if its behavior is fluctuating over a certain period of time.
- *On-Off Attack (OOA):* with this attack, a malicious object performs good and bad services randomly to level itself as a normal or good object. To foil this attack, the same solution proposed for OSA is used.

7.4/ PERFORMANCE EVALUATION AND DISCUSSIONS

The trust management system discussed is evaluated in a simulated environment. Evaluation setup and the results of the evaluations are presented in this section. There are some simulation tools for fog computing; iFogSim [275] for measuring the impact of resource management techniques, Discrete Event System Specification (DEVS) based tool [276] for evaluating impact of deploying fogging, EmuFog [277] is extensible emulation framework for fog computing environments without mobility feature, and FogTorch[278] for QoS-aware deployment of multi-component IoT applications to fog infrastructures. However, there is no full-fledged simulation tool for the new computing paradigm. Therefore, a Java-based simulation tool for the scenario explained in the system model section has been developed. The tool contains classes like fog node, topology manager, mobility manager, and trust computer as the most important components and other many miscellaneous components.

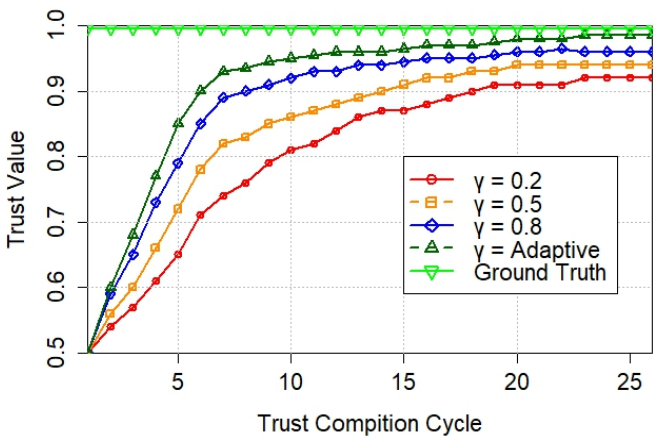
The list of parameters used, and their default values are indicated in TABLE 7.3. We considered a fog environment with 200 fog clients and 40 fog servers randomly distributed over 20 owners. The maximum number of 1-hop neighboring nodes that could send recommendation is six. At the beginning of the simulation, fog clients which are placed on a walkway are connected to fog server. While fog servers are assumed to be static, the clients are mobile. The clients travel in the direction they are originally set with a pedestrian speed randomly assigned based on the values obtained from [41]. The clients walk from left to right, and right to left continuously on a defined trajectory throughout the simulation period. The proposed system is an event-driven trust computation where, when a moving client arrives at a trust computation zone, it starts exchanging information with fog servers to connect to one of the trusted fog servers. Trust computation zones are regions in the simulation environment where a fog client is leaving the network coverage area of the currently connected service provider. A trust computation cycle (simulation cycle) is equal to travel from one end of the walkway to the other. If there are multiple trust zones between the two ends of the road, the average value of trusts computed in all zones is taken. We first presented evolutions of trust accuracy, trust convergence, and how resistant is the system to malicious nodes. Next, a comparative analysis of different derivatives of the proposed algorithm is given.

TABLE 7.3. DEFAULT SIMULATION PARAMETERS

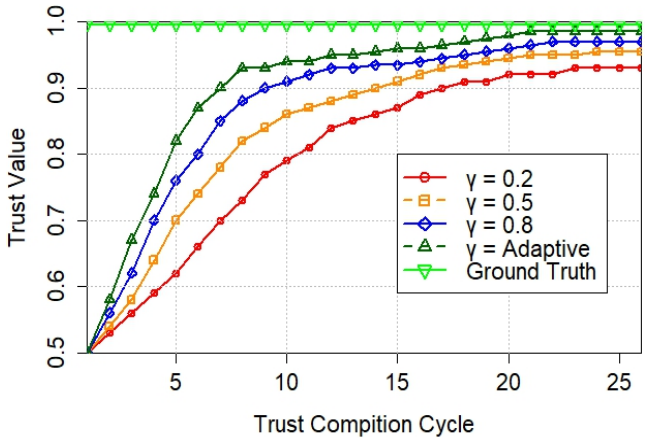
Parameters	Values
Number of Fog Servers	40
Number of Fog Clients	200
Number Owners	20
% of dishonest nodes (PD)	20%
Simulation period (Cycle)	25

7.4.1. EVALUATION OF TRUST ACCURACY, CONVERGENCE AND RESILIENCE

The evaluation results of accuracy, convergence, and resilience of the proposed algorithm are presented in the next paragraphs. Unless specified, the default parameters shown in TABLE 7.3 are used. Figure 7.5 shows trust accuracy and convergence of randomly picked normal or good fog client a) and good fog server b) with adaptive and static weighting factors **(γ)** among direct and indirect trusts. The trust management that relies on adaptive weighting factor is the most accurate and the fast converging one. This is because indirect trust gets higher weights only when it is obtained from larger number of recommenders. For static weighting, as the values of **γ** increase, the trust converges faster, and it has better accuracy. This confirms that the trust value obtained by self-observation better describes the final trust value of an entity. This is because recommendations are affected by the presence of malicious nodes [279]. In our system, by default, 20% nodes are dishonest. Trust value of 0.9 is achieved at the 17th cycle when more weight is given to indirect trust for fog clients while only at 9th cycle, the same value is achieved if more weight is provided for direct trust. As shown in the diagram, though it takes a longer time to converge, relying on indirect trust doesn't prevent the algorithm from convergence. Therefore, we can say that indirect trust has a very important role, especially in cases direct observation is imprecise or not possible. There is no significant difference between trust values of fog clients and fog servers except in case of fog servers, where the graph is a bit smoother due to a constant set of neighboring servers that feed recommendations.



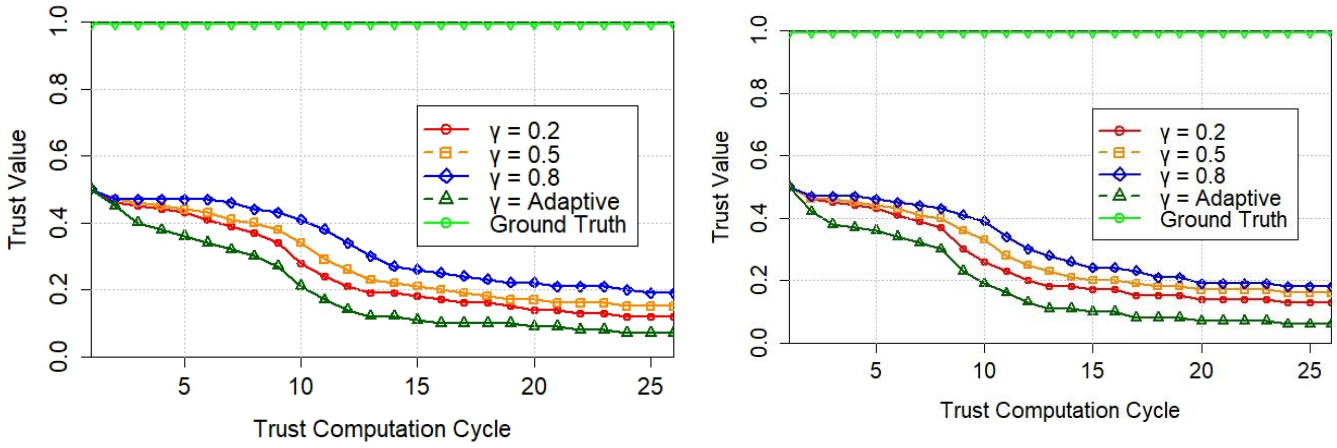
a) Fog Client



b) Fog Server

Figure 7.5: Trust values of a) Good fog client and b) Good fog server over trust computation cycle

The evaluation of the trust value of a randomly selected bad fog client and bad fog server are shown in Figure 7.6. If a node is bad either intentionally or unintentionally, it acts undesirably. The algorithm captures this behavior, and this is manifested by decreasing trust value of such nodes. The main objective of this evaluation is assuming that a node is bad, how trust management system handles such situations without going through the nitty-gritty of malicious node detection. The default trust value of a node in this evaluation is 0.5. Based on the type of a node, the trust level increases or decreases in the course of trust computation cycle. The algorithm is able to turn bad nodes worst. This is especially true when the weighting factor of direct and indirect trust values is dynamically determined since the factor depends on preceding trust values. The reduction of the trust values helps other nodes abstain from creating a connection to such nodes and to remove such nodes from the network whenever necessary.



a) Fog Client b) Fog Server

Figure 7.6: Trust values of a) Bad fog client and b) Bad fog server over trust computation cycle

Figure 7.7 shows the resilience of the algorithm when the percentage of dishonest fog clients increases with adaptive γ. The percentage of dishonest nodes is set to 20%, 40%, and 60%. It can be observed that as the percentage of dishonest nodes increases, it takes more time for a good fog client's trust to converge. Moreover, the trust value at which convergence appears decreases as more population of malicious nodes is introduced. For instance, the trust value of a good fog client can't attain 0.85 till 22^{nd} simulation cycle if the percentage of dishonest nodes is 60%. However, the algorithm is resilient to hostility since it provides reasonably high trust value even in the presence of a large population of dishonest nodes. The value meets the requirements of many applications, although the population of bad nodes is large.

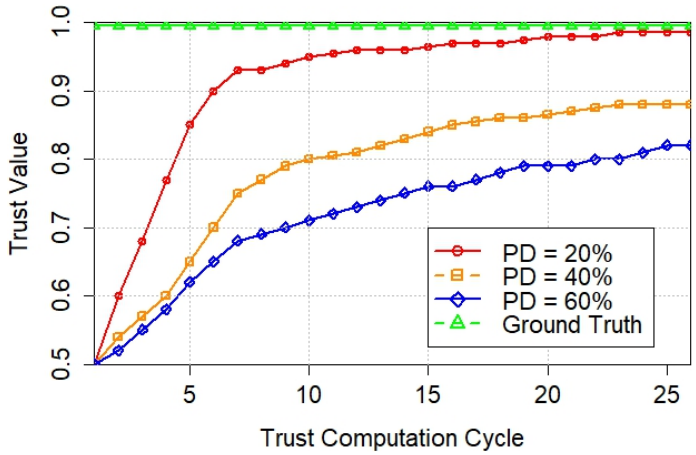


Figure 7.7: Effect of percentage of bad nodes on trust values of a good fog client

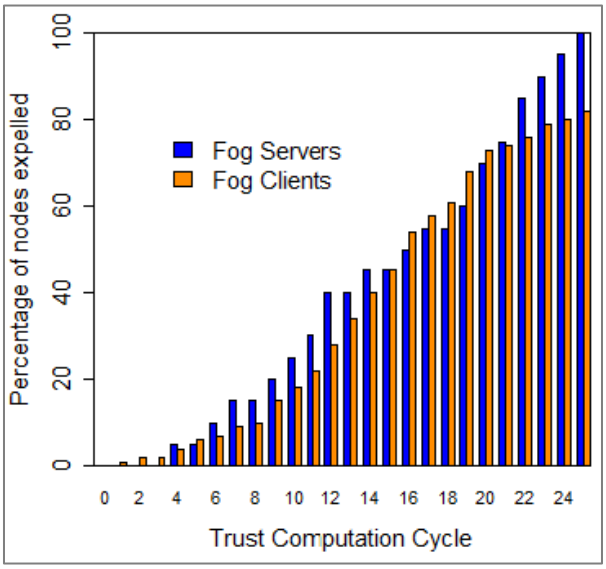
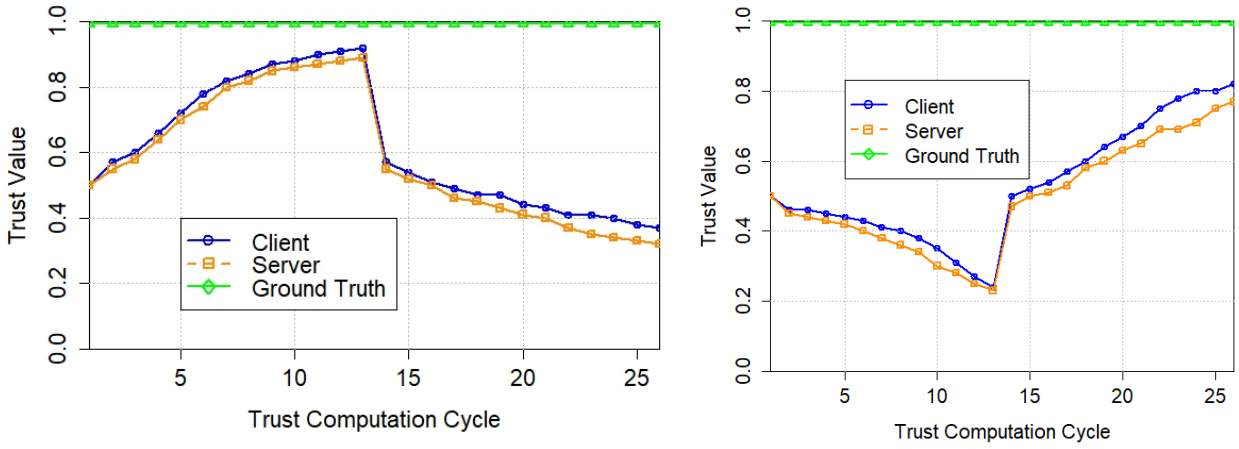


Figure 7.8: Percentage of expelled dishonest nodes over trust computation cycle

Algorithm 7.1 is modified in such a way that dishonest nodes are expelled from the network. A fog client is expelled if it is unable to be accepted by any neighboring service provider. That is, it passes a trust computation zone without successfully connecting to another service provider due to its low trust value. A fog server is expelled if it is not selected for service provision by any service requester over a trust computation cycle. The percentage of expelled dishonest nodes in the simulation environment, where the percentage of dishonest nodes is 50% is graphed in Figure 7.8. This data is collected by counting nodes expelled up to a simulation cycle. At 25th trust computation cycle, all bad fog servers and 82% of bad fog clients are expelled from the network.

The behavior of fog nodes may change over time [266], [280]. A good node may change its behavior to a bad node because of malfunctioning, or to pose attacks, and a dishonest node may also change to good behaving node. Figure 7.9 shows the trust value of a randomly selected good node whose behavior

has turned to bad Figure 7.9 a) and a bad node whose behavior has changed to good Figure 7.9 b) at 12th simulation cycle. The algorithm is able to capture the behavior change of nodes.



a) Good to bad

b) Bad to Good

Figure 7.9: Change of behavior of nodes a) from Good to Bad and b) from Bad to Good

7.4.2. COMPARATIVE ANALYSIS

The TTM system's algorithm can be amended in different ways. Hence, the algorithm is modified in such a way that a fog client evaluates the trust values of all neighboring servers and send a connection request to the server with the highest possible trust value. The modification is named Modified Two-way Trust Management (MTTM) system. In the original two-way algorithm, any fog server encountered early, and that fulfills trust value requirement of the client is selected as long as the client itself is found to be trustworthy. Random service provider selection, which randomly opts service providers without regard to trust is another method on the plate for comparison. The three methods are evaluated in terms of the average percentage of bad servers selected for service provision over 25 simulation cycles. A bad server, in this case, is the one with trust value less than 0.5. The objective of the evaluation is to check how effective is the proposed method in terms of selection of the best service provider with the assumption that the quality of services provided depends on the trust level of the service provider. For this evaluation, the percentage of dishonest nodes is set to 40%, and the number of fog servers has the default value. The average percentage of bad service providers selected over the trust computation cycles is plotted in Figure 7.10.

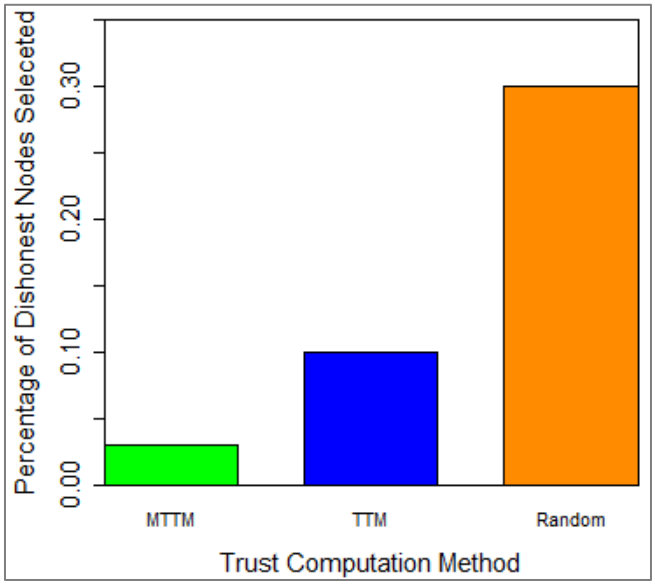


Figure 7.10: Average percentage of dishonest fog servers selected for service provision

MTTM has chosen only one dishonest fog server on average in all trust computation cycles. It is the most effective method because of its ability to choose the most trusted node to create a connection. However, since the method involves high overhead due to the computation of trust of all neighboring servers, it is not suitable for real-time systems. TTM may select a server which does not possess the highest trust value, but it is optimal in the selection of service providers with desired trust value, and it has lesser computational overhead than MTTM.

The last set of experiments conducted are the evaluation of the trust level of servers opted for service provision using MTTM, TTM and a newly added conventional One-way Trust Management (OTM) system where clients can evaluate the trust of servers to which they are going to connect without their trust being evaluated by the servers. This method works in the same way as TTM, except in this case, clients' trust is not evaluated. The purpose of this evaluation is to check if two-way trust computation has indeed advantage over one-way trust computation. Hence, trust convergence and accuracy of the three algorithms on randomly selected good fog server are evaluated over trust computation cycles. Percentage of dishonest nodes is set to have the default value (i.e. 20%) and direct and indirect trust contributions to the overall trust are decided dynamically. The result is shown in Figure 7. 11.

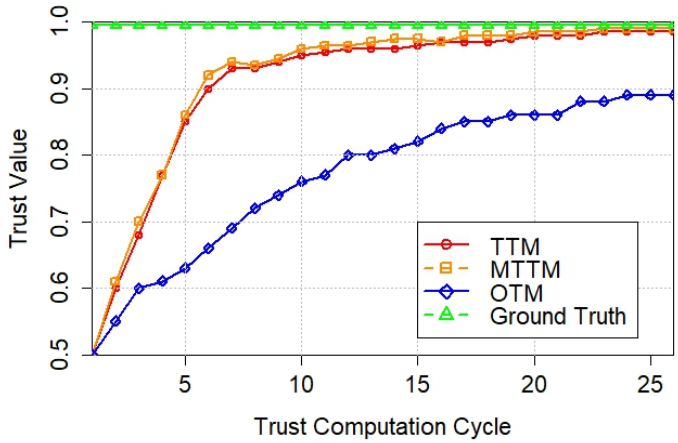


Figure 7.11: Trust values of different derivatives of the algorithm for randomly selected good fog server

Modified two-way trust management system, MTTM, outperforms the other methods both in accuracy and trust convergence though its difference with TTM is minor. This is bearing to its ability to choose the most trusted fog server. One-way trust management system is the least performing algorithm. The reason behind this is that, firstly, the trust value of the server they first encountered and selected may not have the highest trust value in comparison with neighboring servers. Secondly, the indirect trust computation of the servers misses recommendations from nearby servers. In the main algorithm, clients propagate trust values of the servers they have computed to establish trusted data communication to servers, and the servers use this value to weight recommendations of the servers. Therefore, we can conclude that the two-way trust management system chooses most trusted service providers than the one-way trust management system.

7.5/ CONCLUSION

Fog computing is the next frontier of cloud computing since it can compute, and store a massive amount of data generated by IoT devices near their sources. Indeed, transmitting all these data to the cloud will take up a huge amount of bandwidth. Fog computing is a promising architecture that allows data processing near to where they are generated instead of sending them to the cloud. Because of this, it saves a great deal of bandwidth, and it is suitable for latency-sensitive applications like traffic safety applications. Fog computing can be combined with omnipresence mobile devices to reduce high fatality rates due to traffic safety architectures. Current mobile devices have a high computation, storage, communication, and sensing capacity making them candidates to many solutions. An architecture that uses mobile devices of VRUs to track the users and fog nodes to run collision prediction algorithms and notify both VRUs' and drivers is proposed in chapter 3. The evaluation of the solution reveals that it is able to render alerts in real-time. However, before deploying the solution in a real environment, challenges attributed to fog computing needs to be addressed. Its features and flexibility of deployment make fog computing vulnerable to privacy attacks. For instance, co-location of a user and fog node

means that users can be localized up to one fog node coverage area (e.g. city block area) by an eavesdropper.

In this chapter, a P2P two-way trust management system that enables service requesters to evaluate trust level of service providers before awarding the service and that allows service providers to check the trustworthiness of the service demanders is presented. By exposing their information to only trusted nodes, information security, and user privacy are ensured. The bidirectionality of the solution is the first of its kind for fog computing, and it allows fog nodes abstain from connecting to untrustworthy nodes and ensures secure data communication with only trusted nodes. The system dynamically incorporates both QoS and social trust information to compute trust levels of fog nodes from an adaptive combination of direct observation and recommendations. Subjective logic is used to aggregate trust values obtained from neighboring recommenders. Extensive evaluations of the trust management system show that it converges quickly, have high accuracy, and is resilient to trust-based attacks. The solution is modified in two different ways and analytical comparison is made in terms of percentage of dishonest nodes selected for service provision and trust convergence. The first modification is that service requester selects a service provider with the highest trust value instead of selecting a trusted service provider encountered first. The second amendment whereas is the conversion of TTM to the conventional one-way trust management system. It is found that the proposed system gives an optimal solution since the modifications have either high overhead, or do not converge in time, or have less accuracy.

The next chapter provides conclusions of the thesis and discusses the possible extension of researches to the problems addressed by this thesis.

8

CONCLUSIONS AND PERSPECTIVES

8.1/ CONCLUSIONS

Road traffic injuries are reasons for large numbers of avoidable deaths. It is the eighth leading cause of death globally for all age groups and it is the leading cause of death for people aged five to twenty-nine. Vulnerable road users make up more than 50% of all road traffic deaths and injuries. The rate of road accidents is increasing globally. Deaths, injuries, physical disabilities, and psychological distress caused by road traffic injuries are creating an incredible undesirable economic, and social consequence on victims, their families, and the society in general, particularly in low- and middle-income countries. Human errors are the main reasons for road traffic accidents. Some of the typical conduct of humans which contribute to traffic accidents are speeding, drunken and intoxicated driving, distracted driving and walking, not abiding by traffic laws, not using gears like seat belts and helmets. To solve the severe public health problem caused by road traffic injuries, many passive and active road safety measures are being taken.

The thesis began with a deep survey on road safety systems. We also discussed requirements of VRU devices (VRU carried devices for traffic safety), and communication technologies to connect VRUs with vehicles. Fog computing as intermediate infrastructure for V2VRU communication is also explained. The descriptions include architecture, features, applications, and challenges of the computing paradigm.

Next, an active safety system that integrates mobile devices owned by VRU and the rising fog computing paradigm is presented. Rather than being causes of traffic accidents due to the new kind of distractions they brought, mobile devices can function as VRU devices to save lives of many VRUs. On the one hand, the devices have high computation, storage, sensing, and networking capabilities. Moreover, they are possessed by almost all road users. Fog computing, on the other hand, comes with plenty of attractive features that make the technology the best candidate for traffic safety, and other real-time applications. Some features of fogging that suits traffic systems include low latency, location awareness, geo-distribution, heterogeneity, scalability, reliability, and predominance of wireless connections. The main duties of smartphones in the solution are sensing position and other data needed for traffic accident prediction from VRUs and vehicles, and sending the CAM to a nearby fog server. Once the fog server receives the data, it executes the VRU collision prediction algorithm. If an imminent

accident is estimated, the server sends DENM to both VRUs and drivers. Mobile devices of VRUs and drivers may be connected to fog server using either Wi-Fi, or cellular communication technologies. The feasibility of the architecture is proven by testing its response time and packet delivery ratio in the simulated environment, and by comparing it with other smartphone-based traffic accident avoidance solutions based on criteria pertaining to the application.

Before deploying the architecture in a real environment, there are certain challenges that must be addressed. The challenges are related to important components of the architecture: smartphones GPS position accuracy doesn't suffice for traffic safety applications, position sampling frequency of the mobile device is slack, and the usage of the devices in traffic safety applications drains their batteries quickly. Revealing users position continuously and densely exposes the identity of VRU's and drivers. Despite ample advantages of fog computing, there are challenges, including information security and user privacy. Thus, we have provided solutions for the challenges mentioned above.

After conducting an experiment to check the position accuracy of contemporary mobile devices, a two-stage position accuracy improvement algorithm based on map matching is able to correct inaccurate position readings of mobile devices. In the first stage, deviated position readings are smoothed using the Kalman filter. In the second stage, OTW based map matching is performed to align the positions to the right road segments. Various variations of the OTW algorithms are compared in terms of matching accuracy and time complexity. To satisfy the high sampling demand of traffic safety application (10Hz), we have proposed a method that fuses position data obtained from GPS and inertial sensors. The experiment we have conducted shows that maximum sampling frequency of smartphones is 1Hz while inertial sensors can provide the data at a much higher rate. GPS fixes are used as ground truth positions and to correct dead reckoning parameters. Other positions between two GPS fixes are dead reckoned using inertial position data. Combining GPS positioning, which has long term accuracy and inertial positioning, which has short term accuracy resulted in accurate positioning.

High rate position sampling and communicating with fog servers make small mobile devices more energy-hungry devices. Thus, to increase the energy-efficiency of mobile devices, we have done two different tasks. To reduce energy consumption due to position sampling, optimal inertial sensor data sampling that saves energy without degrading the position accuracy is conceived. Energy consumption due to high communication is dealt with a fuzzy-logic based adaptive beaconing management system-based risk level VRU. The system makes traffic risk level prediction by considering factors that affect traffic risks. The factors are related to pedestrian profile, the drivers, the kinematics of the vehicles, and the road and environmental factors. Finally, the road accident levels are converted to beaconing rates that conserve energy while keeping the VRU safe from traffic accidents. A smartphone that uses adaptive beaconing rate can save twice more energy than the one with a static beaconing at a highest rate.

The last contribution of this thesis is on establishing trusted communication between fog servers and VRU devices. Fog computing is susceptible to security and privacy attacks due to its proximity to end users, location awareness, geo-distribution, etc. To overcome this problem, a two-way subjective logic-based trust management system that enables VRU devices to check if fog servers can provide the right service and that allows fog server to check the trustworthiness of the VRU devices is proposed. It incorporates both QoS and social metrics to compute an aggregated trust of direct and indirect trusts. The trust management is accurate, converges in few trust computations cycles, is resilient to trust attacks, and captures behavior changes of nodes.

8.2/ PERSPECTIVES

This section is dedicated to highlighting some open questions and perspectives for future work in relation to the problems addressed by the thesis.

- *Offloading Trajectory Data among Fog Nodes:* during their mobility, VRUs and vehicles may leave the coverage area of a fog server they are currently connected, and join a new fog server. For better accuracy of traffic accident prediction by looking at mobility history of the road users, their trajectories have to be passed to the new fog node. The other reason for offloading road users' trajectories to nearby fog nodes is to distribute loads among fog nodes. Based on the situations, part of the trajectory may be sent instead of the entire mobility history.

- *Network Congestion:* in roads which are densely populated by VRUs and vehicles, congestion is a threat in the traffic safety architecture proposed. Sending position and other information at such high rate to fog servers by road users through wireless communication channel may cause congestion of the network, which eventually leads to transmission errors, and high VRUs devices energy consumption. Clustering road users, contextual transmission, and letting fog servers predict some information rather than sending all the time are candidate solutions to reduce congestion.

- *Collective Energy Saving:* based on [281], up to 70% of people in a crowd are actually moving in groups, such as friends, couples, or families walking together. If a group of people are moving together, only the smartphone of the person with the highest risk of collision or/and the better power charge level is supposed to beacon at high frequency. Others can beacon at a lower frequency to check their battery level and for better accuracy. The frequent beaconing role is periodically switched among cluster members, for fair energy efficiency. Grouping pedestrians implies overall energy gain can be achieved and the gain increase as the number of people in a group increase. However, caution has to be taken not to compromise safety.

- *Combining Direct and Indirect Communication:* communication between vehicle and VRU

can be made using either in direct mode or in indirect mode through an infrastructure. So, as to exploit the advantages of the two communication modes for maximum safety, they can be combined. In normal situations, the two parties can communicate indirectly through an infrastructure. However, when an about-to-occur collision is detected, they may be set to communicate with each other. This highly reduces communication latency and increases safety. However, the effort put to get the benefits is not sufficient.

- *3D position Tracking (3D Localization):* is the measurement of a 3D position and orientation of an object in a defined space relative to a known location. It has got a lot of attention from the wide research community. 3D localization of vehicles and VRUs increases position accuracy and hence traffic safety. However, as far as we know, no efforts have been made to employ 3D localization for tracking VRUs in traffic safety.

PUBLICATIONS

Conference papers

- **Esubalew Alemneh,** Sidi-Mohammed Senouci, and Philippe Brunet, "An Energy Efficient Smartphone Sensors' Data Fusion for High Rate Position Sampling Demands", 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019.
- **Esubalew Alemneh**, Sidi-Mohammed Senouci, and Philippe Brunet, "An Online Time Warping based Map Matching for Vulnerable Road Users' Safety", 14th International Wireless Communications and Mobile Computing Conference, 2018.
- **Esubalew Alemneh**, Sidi-Mohammed Senouci, and Philippe Brunet, "Application of Fog Computing for Vulnerable Road Users' Safety", FuturMob'18: Preparing for the transition to autonomous and sustainable mobility, May 28-29, 2018.
- **Esubalew Alemneh,** Sidi-Mohammed Senouci, and Philippe Brunet, "PV-Alert: A fog-based architecture for safeguarding vulnerable road users," 2017 Global Information Infrastructure and Networking Symposium (GIIS), 2017.

Newsletters

- **Esubalew Alemneh,** and Sidi-Mohammed Senouci, "Ensuring Safety of Vulnerable Road Users using their smartphones and fogging: Challenges and Solutions", IEEE ComSoc AHSN TC Newsletter (2019).

Papers Under Review

- **Esubalew Alemneh**, Sidi-Mohammed Senouci, Philippe Brunet, and T. Tegegne, "A Two-way Trust Management System for Fog Computing", (Future Generation Computer Systems Journal)
- **Esubalew Alemneh**, Sidi-Mohammed Senouci, Mohamed-Ayoub Messous, "An Energy-Efficient Fuzzy Logic-based Adaptive Beaconing Rate Management for Pedestrian Safety" (Personal and Ubiquitous Computing Journal).

Other Publications

- Ahmed Alioua, Sidi-Mohammed Senouci, Samira Moussaoui, **Esubalew Alemneh**, Med Ahmed-Amine Derradji, Fella Benaziza, A Distributed Multi-hop Clustering Algorithm for Infrastructure-less Ad-Hoc Networks, 1st EAI International Conference on ICT for Development for Africa, September 25-27, 2017, Bahir Dar, Ethiopia.

Talks

- **Esubalew Alemneh**, Sidi-Mohammed Senouci, and Philippe Brunet, "An Online Time Warping based Map Matching for Vulnerable Road Users' Safety", 14th International Wireless Communications and Mobile Computing Conference, June 25-29, Limassol, Cyprus, 2018.

- **Esubalew Alemneh**, Sidi-Mohammed Senouci, and P. Brunet, "Application of Fog Computing for Vulnerable Road Users' Safety", FuturMob'18: Preparing for the transition to autonomous and sustainable mobility, May 28-29, Nevers, France, 2018.
- **Esubalew Alemneh**, Sidi-Mohammed Senouci, and P. Brunet, "PV-Alert: A fog-based architecture for safeguarding vulnerable road users", 8th Thematic Day on Vehicular Networks, 22 March 2018, Paris, France.
- Ahme Alioua, Sidi-Mohammed Senouci, Samira Moussaoui, **Esubalew Alemneh**, Med Ahmed-Amine Derradji, Fella Benaziza, A Distributed Multi-hop Clustering Algorithm for Infrastructure-less Ad-Hoc Networks, 1st EAI International Conference on ICT for Development for Africa, September 25-27, 2017, Bahir Dar, Ethiopia.

BIBLIOGRAPHY

[1] Who.int, "Global status report on road safety 2015", 2016. [Online]. Available: http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/. [Accessed: 15- Jan- 2017]

[2] Who.int, "2018 road safety statistics", 2018. [Online]. Available: https://www.who.int/violence_injury_prevention/road_safety_status/2018/English-Summary-GSRRS2018.pdf. [Accessed: 02 – Jan- 2018]

[3] Europa.eu, "2016 road safety statistics: What is behind the figures", 2017. [Online]. Available: http://europa.eu/rapid/press-release_MEMO-17-675_en.htm. [Accessed: 20 – Apr- 2017]

[4] Robyn D. Robertson, "Pedestrians: What We Know?", TI RF, Ottawa, Ontario Canada, 10 November, 2015.

[5] automotive-fleet.com, "The Alarming Rise of Distracted Pedestrians", 2017. [Online]. Available: http://www.automotive-fleet.com/channel/safety-accident-management/article/story/2017/03/the-alarming-rise-of-distracted-pedestrians.aspx. [Accessed: 29-Mar-2017].

[6] dailymail.uk, "Latest menace on our roads? It's the smartphone zombies",2016. [Online]. Available: http://www.dailymail.co.uk/news/article-3522026/Latest-menace-roads-s-smartphone-zombies-Three-quarters-drivers-say-seen-pedestrian-veer-pavement-staring-device.html. [Accessed: 09 – Jan- 2017]

[7] Safety.com, "Distracted Walking a Major Pedestrian Safety Concern," Safety.com, 23-Feb-2016. [Online]. Available: https://www.safety.com/blog/distracted-walking-a-major-pedestrian-safety-concern/. [Accessed: 26-Apr-2017].

[8] J. L. Nasar and D. Troyer, "Pedestrian injuries due to mobile phone use in public places," Accident Analysis & Prevention, vol. 57, pp. 91–95, 2013.

[9] K. Terzano, "Bicycling safety and distracted behavior in The Hague, the Netherlands," Accident Analysis & Prevention, vol. 57, pp. 87–90, 2013.

[10] M. Másilková, "Health and social consequences of road traffic accidents," Kontakt, vol. 19, no. 1, 2017.

[11] statista.com, "Number of smartphone users worldwide from 2014 to 2020(in billions)," 2017. [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ [Accessed: 23-Nov-2017]

[12] seekingalpha.com, “Smartphone Prices Will Collapse Soon”, 2017. [Online]. Available: https://seekingalpha.com/article/4026699-smartphone-prices-will-collapse-soon. [Accessed: 23-Nov-2017]

[13] A. Campbell and T. Choudhury, “From Smart to Cognitive Phones,” IEEE Pervasive Computing, vol. 11, no. 3, pp. 7–11, 2012.

[14] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the internet of things,” in Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, ser. MCC’12. ACM, 2012, pp. 13–16.

[15] M. Liebner, F. Klanner, and C. Stiller, “Active safety for vulnerable road users based on smartphone position data,” IEEE Intelligent Vehicles Symposium (IV), 2013.

[16] Z. Ma, Y. Qiao, B. Lee, and E. Fallon, “Experimental evaluation of mobile phone sensors,” 24th IET Irish Signals and Systems Conference, 2013.

[17] E. Alemneh, S.-M. Senouci, and P. Brunet, “An Energy Efficient Smartphone Sensors’ Data Fusion for High Rate Position Sampling Demands”, 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019

[18] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing Fog Computing for Internet of Things Applications: Challenges and Solutions,” IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 601–628, 2018.

[19] S. Yi, Z. Qin, and Q. Li, “Security and Privacy Issues of Fog Computing: A Survey,” Wireless Algorithms, Systems, and Applications Lecture Notes in Computer Science, pp. 685–695, 2015.

[20] europa.eu, “2018 road safety statistics: what is behind the figures?”, [Online]. Available: http://europa.eu/rapid/press-release_MEMO-19-1990_en.htm. [Accessed: 15 – Mar-2019].

[21] R. Rissanen, H.-Y. Berg, and M. Hasselberg, “593 Quality of life following a road traffic injury: a systematic literature review,” Injury Prevention, vol. 22, no. Suppl 2, 2016.

[22] World Bank, “The High Toll of Traffic Injuries: Unacceptable and Preventable”, Washington, DC, 2017. [Online]. https://openknowledge.worldbank.org/handle/10986/29129. [Accessed 07-Mar-2017].

[23] etsc.eu, “France backtracks on 80km/h speed limit despite positive results, “, Available: https://etsc.eu/france-backtracks-on-80km-h-speed-limit-despite-positive-results/ [Accessed: 15-Dec-2017]

[24] NHTSA, “Highlights of 2009 motor Vehicle Crashes”, [Online]. Available: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/811363. [Accessed December 20, 2017].

[25] R. A. Retting, S. A. Ferguson, and A. T. Mccartt, “A Review of Evidence-Based Traffic Engineering Measures Designed to Reduce Pedestrian–Motor Vehicle Crashes,” American Journal of Public Health, vol. 93, no. 9, pp. 1456–1463, 2003.

[26] WHO, “Save LIVES - A road safety technical package”, ISBN 978-92-4-151170-4, 2017.

[27] D. A. Sleet, G. Baldwin, A. Dellinger, and B. Dinh-Zarr, “The Decade of Action for Global Road Safety,” Journal of Safety Research, vol. 42, no. 2, pp. 147–148, 2011.

[28] Santacreu, A. Safer City Streets: Global Benchmarking for Urban Road Safety; OECD Publ.: Paris, France, 2018.

[29] Ptak, M. "Method to Assess and Enhance Vulnerable Road User Safety during Impact Loading." Applied Sciences 9.5 (2019): 1000.

[30] A. Jarašūnienė and G. Jakubauskas, “Improvement of Road Safety Using Passive and Active Intelligent Vehicle Safety Systems,” Transport, vol. 22, no. 4, pp. 284–289, 2007.

[31] World Health Organization, “Pedestrian Safety”, WHO, Geneva, Swizerland, 2013.

[32] V. Kausalyah, S. Shasthri, K. Abdullah, M. Idres, Q. Shah, and S. Wong, “Optimisation of vehicle front-end geometry for adult and pediatric pedestrian protection,” International Journal of Crashworthiness, vol. 19, no. 2, pp. 153–160, 2014.

[33] G. Li, M. Lyons, B. Wang, J. Yang, D. Otte, and C. Simms, “The influence of passenger car front shape on pedestrian injury risk observed from German in-depth accident data,” Accident Analysis & Prevention, vol. 101, pp. 11–21, 2017.

[34] N. Yusof, S. Sapuan, M. Sultan, M. Jawaid, and M. Maleque, “Design and materials development of automotive crash box: a review,” Ciência & Tecnologia dos Materiais, vol. 29, no. 3, pp. 129–144, 2017.

[35] S. Stanisławek and T. Niezgoda, “The ability of flexible car bonnets to mitigate the consequences of frontal impact with pedestrians,” 2018.

[36] G. O. Babio and A. Daponte-Codina, “Factors Associated with Seatbelt, Helmet, and Child Safety Seat Use in a Spanish High-Risk Injury Area,” The Journal of Trauma: Injury, Infection, and Critical Care, vol. 60, no. 3, pp. 620–626, 2006.

[37] automotive.silicones.elkem.com, “External airbags for pedestrian protection”, [Online]. Available: http://automotive.silicones.elkem.com/trends-of-tomorrow/external-pedestrian-airbags, [Accessed: 12-Apr-2017].

[38] Devi, V.S. & Kumar, B.V.S. & Sulaipher, M. (2016). Education and enforcement in traffic management. 9. 2073-2081.

[39] Mock C, Joshipura M, Arreola-Risa C et al. An estimate of the number of lives that could be saved through improvements in trauma care globally. World Journal of Surgery, 2012, 36:959-963

[40] C. G. Keller, T. Dang, H. Fritz, A. Joos, C. Rabe, and D. M. Gavrila, “Active Pedestrian Safety by Automatic Braking and Evasive Steering,” IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 4, pp. 1292–1304, 2011.

[41] H. Hamdane, T. Serre, C. Masson, and R. Anderson, “Issues and challenges for pedestrian active safety systems based on real world accidents,” Accident Analysis & Prevention, vol. 82, pp. 53–60, 2015.

[42] Carsten O, Tate F. Intelligent speed adaptation: The best collision avoidance system? SAE Technical Paper; 2001 Jun 4.

[43] A. Solodkiy and V. Yenokayev, “Cooperative ITS – A Strategic Way to Ensure Road Safety,” Transportation Research Procedia, vol. 20, pp. 630–634, 2017.

[44] A. Silla, P. Rämä, L. Leden, M. V. Noort, J. D. Kruijff, D. Bell, A. Morris, G. Hancox, and J. Scholliers, “Quantifying the effectiveness of ITS in improving safety of VRUs,” IET Intelligent Transport Systems, vol. 11, no. 3, pp. 164–172, 2017.

[45] Scholliers, M. V. Sambeek, and K. Moerman, “Integration of vulnerable road users in cooperative ITS systems,” European Transport Research Review, vol. 9, no. 2, 2017.

[46] bodyguardsafety.com, “BodyGuard’s i-Tag Proximity Warning System “, [Online]. Available: http://www.bodyguardsafety.com.au/proximity-warning-system/. [Accessed: 22-Feb-2018].

[47] iis.fraunhofer.de, “Ko-TAG Directional Antenna“, [Online]. Available: https://www.iis.fraunhofer.de/en/ff/kom/ant/ko-tag-peilantenne.html. [Accessed: 22-Feb-2018].

[48] Anund A, Chalkia E, Nilsson L, Diederichs F, Ferrarini C, Montanari R, Strand L, Aigner-Bruess E, Jankoska D, Wacowska-Slezak J (2012) SafeWay2School D10.5 Final report.

[49] A. Rostami, B. Cheng, H. Lu, M. Gruteser, and J. B. Kenney, “Reducing Unnecessary Pedestrian-to-Vehicle Transmissions Using a Contextual Policy,” Proceedings of the 2nd ACM International

Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services - CarSys 17, 2017.

[50] Motorcycles become part of the connected vehicle world: BMW Motorrad, Honda and Yamaha cooperate to further increase safety of powered two-wheelers, Honda News Release, 7.10.2015.

[51] Maruyama K, Chiba T, Kizaki T, Horozovic A (2014) Vehicle-to-X functions for improved motorcycle safety. Auto Tech Rev 3:50–55

[52] P. Sewalkar and J. Seitz, "Vehicle-to-Pedestrian Communication for Vulnerable Road Users: Survey, Design Considerations, and Challenges," Sensors, vol. 19, no. 2, p. 358, 2019.

[53] M. Bagheri, M. Siekkinen, and J. K. Nurminen, "Cellular-based vehicle to pedestrian (V2P) adaptive communication for collision avoidance," 2014 International Conference on Connected Vehicles and Expo (ICCVE), 2014.

[54] U. Hernandez-Jayo, I. De-la-Iglesia, J. Perez, "V-Alert: Description and Validation of a Vulnerable Road User Alert System in the Framework of a Smart City", . Sensors 15, Vol. 8, pp. 18480–18505, 2015.

[55] K. David and A. Flach, "CAR-2-X and Pedestrian Safety," IEEE Vehicular Technology Magazine, vol. 5, no. 1, pp. 70–76, 2010.

[56] E. Alemneh, S.-M. Senouci, and P. Brunet, "PV-Alert: A fog-based architecture for safeguarding vulnerable road users," 2017 Global Information Infrastructure and Networking Symposium (GIIS), 2017.

[57] E. Uhlemann, "Introducing Connected Vehicles [Connected Vehicles]," IEEE Vehicular Technology Magazine, vol. 10, no. 1, pp. 23–31, 2015.

[58] ETSI TS 101 539-1 (2013) Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) application requirements specification, v1.1.1

[59] ETSI TR 102 638 (2009) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, V1.1.1.

[60] J.J. Anaya, P. Merdrignac, O. Shagdar , F. Nashashibi, and J.E. Naranjo, "Vehicle to pedestrian communications for protection of vulnerable road users", In Intelligent Vehicles Symposium Proceedings, 2014 IEEE (pp. 1037-1042), June, 2014.

[61] P. A. Zandbergen and S. J. Barbeau, "Positional Accuracy of Assisted GPS Data from High-Sensitivity GPS-enabled Mobile Phones," Journal of Navigation, vol. 64, no. 03, pp. 381–399, Jul. 2011.

[62] Wu X., Miucic R., Yang S., Al-Stouhi S., Misener J., Bai S., Chan W. Cars Talk to Phones: A DSRC Based Vehicle-Pedestrian Safety System; Proceedings of the 80th Vehicular Technology Conference (VTC Fall); Vancouver, BC, Canada. 14–17 September 2014.

[63] R. Ercek, P. De Doncker, and F. Grenez. NLOS-multipath effects on pseudo-rangeestimation in urban canyons for gnss applications. InAntennas and Propagation,2006. EuCAP 2006. First European Conference on, pages 1–6. IEEE, 2006

[64] K.M. Pesyna , R.W. Heath and T.E. Humphreys. "Centimeter positioning with a smartphone-quality GNSS antenna." In Proceedings of the ION GNSS+ Meeting, 2014

[65] Engel S, Kratzch C, David K, Warkow D, Holzknecht M, "Car2Pedestrian positioning: methods for improving GPS positioning in radio-based VRU protection systems", advanced microsystems for automotive applications 2013, smart syst, 2013

[66] D. Yoon, C. Kee, J. Seo, and B. Park, "Position Accuracy Improvement by Implementing the DGNSS-CP Algorithm in Smartphones," Sensors, vol. 16, no. 6, p. 910, 2016.

[67] Z. Ma, Y. Qiao, B. Lee, and E. Fallon, "Experimental evaluation of mobile phone sensors," 24th IET Irish Signals and Systems Conference, 2013.

[68] T. Liu, C. Chen, M. King, G. Qian, and J. Fu, "Balancing Power Consumption and Data Analysis Accuracy Through Adjusting Sampling Rates: Seeking for the Optimal Configuration of Inertial Sensors for Power Wheelchair Users," Lecture Notes in Computer Science Digital Human Modeling. Applications in Health, Safety, Ergonomics and Risk Management: Ergonomics and Health, 2015.

[69] T. O. Oshin, S. Poslad, and A. Ma, "Improving the Energy-Efficiency of GPS Based Location Sensing Smartphone Applications," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[70] C.-M. Huang, C.-H. Lee, and W.-S. Chen, "A power efficient pedestrian touring scheme based on sensor-assisted positioning and prioritized caching for smart mobile devices," 2013 21st International Conference on Software, Telecommunications and Computer Networks, 2013.

[71] P.-L. Shih, P.-J. Chiu, Y.-C. Cheng, J.-Y. Lin, and C.-W. Yi, "Energy-Aware Pedestrian Trajectory System," 41st International Conference on Parallel Processing Workshops, 2012.

[72] M. Bagheri, M. Siekkinen, and J. K. Nurminen, "Cloud-Based Pedestrian Road-Safety with Situation-Adaptive Energy-Efficient Communication," IEEE Intelligent Transportation Systems Magazine, vol. 8, no. 3, pp. 45–62, 2016.

[73] S. Lee, J. Park, D. Kim, and Y.-G. Hong, "An energy efficient vehicle to pedestrian communication method for safety applications," 2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN), 2014.

[74] Nguyen, Q.H., Morold, M., David, K. and Dressler, F., 2019. Adaptive Safety Context Information for Vulnerable Road Users with MEC Support. In WONS (pp. 28-35).

[75] ETSI.Org, "Intelligent Transport Systems (ITS); ITS-G5 Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band ", [Online]. Available: https://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.03.00_20/en_302663v010300a.pdf [Accessed: 16-Nov-2018].

[76] A. Tahmasbi-Sarvestani, H. N. Mahjoub, Y. P. Fallah, E. Moradi-Pari, and O. Abuchaar, "Implementation and Evaluation of a Cooperative Vehicle-to-Pedestrian Safety Application," IEEE Intelligent Transportation Systems Magazine, vol. 9, no. 4, pp. 62–75, 2017.

[77] Sugimoto C., Nakamura Y., Hashimoto T, "Prototype of pedestrian-to-vehicle communication system for the prevention of pedestrian accidents using both 3G and WLAN communication;" Proceedings of the 3rd International Symposium on Wireless Pervasive Computing; Santorini, Greece. 7–9 May 2008.

[78] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, and L. Zhao, "Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G," IEEE Communications Standards Magazine, vol. 1, no. 2, pp. 70–76, 2017.

[79] J. Lee, Y. Kim, Y. Kwak, J. Zhang, A. Papasakellariou, T. Novlan, C. Sun, and Y. Li, "LTE-advanced in 3GPP Rel -13/14: an evolution toward 5G," IEEE Communications Magazine, vol. 54, no. 3, pp. 36–42, 2016.

[80] Huang K.S., Chiu P.J., Tsai H.M., Kuo C.C., Lee H.Y., Wang Y.C.F, "RedEye: Preventing Collisions Caused by Red-Light-Running Scooters With Smartphones", IEEE Trans. Intell. Transp. Syst. 2016;17:1243–1257. doi: 10.1109/TITS.2015.2502142.

[81] Dhondge K., Song S., Choi B.Y., Park H, "WiFiHonk: Smartphone-based Beacon Stuffed WiFi Car2X-Communication System for Vulnerable Road User Safety", Proceedings of the IEEE 79th Vehicular Technology Conference; Seoul, Korea. 18–21 May 2014.

[82] Liu Z., Pu L., Meng Z., Yang X., Zhu K., Zhang L, "POFS: A Novel Pedestrian-oriented Forewarning System for Vulnerable Pedestrian Safety", Proceedings of the International Conference on Connected Vehicles and Expo (ICCVE); Shenzhen, China. 19–23 October 2015.

[83] Liu Z., Liu Z., Meng Z., Yang X., Pu L., Zhang L, "Implementation and performance measurement of a V2X communication system for vehicle and pedestrian safety", Int. J. Distrib. Sens. Netw. 2016;12 doi: 10.1177/1550147716671267.

[84] Anaya J.J., Talavera E., Giménez D., Gómez N., Jiménez F., Naranjo J.E, "Vulnerable Road Users Detection using V2X Communications", Proceedings of the 18th International Conference on Intelligent Transportation Systems; Las Palmas, Spain. 15–18 September 2015.

[85] Nagai M., Nakaoka K., Doi Y, "Pedestrian-to-vehicle Communication Access Method and Field Test Results", Proceedings of the International, 2012.

[86] Lewandowski A., Boecker S., Koester V., Wietfeld C, "Design and Performance Analysis of an IEEE 802.15.4 V2P Pedestrian Protection System", Proceedings of the 5th International Symposium on Wireless Vehicular Communications; Dresden, Germany. 2–3 June 2013.

[87] D. Alsen, M. Patel, and J. Shangkuan, "The future of connectivity: Enabling the Internet of Things". [online] McKinsey & Company. [Online]. Available at: https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-future-of-connectivity-enabling-the-internet-of-things [Accessed 28-Jun-2018].

[88] "Building an Open Architecture for Fog Computing," Articles and Publications | OpenFog Consortium. [Online]. Available: https://www.openfogconsortium.org/. [Accessed: 09-Aug-2018]

[89] E. Marín-Tordera, X. Masip-Bruin, J. García-Almiñana, A. Jukan, G.-J. Ren, and J. Zhu, "Do we all really know what a fog node is? Current trends towards an open definition," Computer Communications, vol. 109, pp. 117–130, 2017.

[90] [90]. R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions," Internet of Things Internet of Everything, pp. 103–130, 2017.

[91] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," SIGCOMM Comput. Commun. Rev., vol. 44, no. 5, pp. 27–32, 2014.

[92] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 1, pp. 416–464, 2018.

[93] M. Mukherjee, L. Shu, and D. Wang, "Survey of Fog Computing: Fundamental, Network Applications, and Research Challenges," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1826–1857, 2018.

[94] S. Bitam, A. Mellouk, and S. Zeadally, "VANET-cloud: a generic cloud computing model for vehicular ad hoc networks," IEEE Wireless Communications, vol. 22, no. 1, pp. 96–102, 2015.

[95] H. Atlam, R. Walters, and G. Wills, "Fog Computing and the Internet of Things: A Review," Big Data and Cognitive Computing, vol. 2, no. 2, p. 10, 2018.

[96] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog Computing: Platform and Applications," 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb), 2015.

[97] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, and P. Liljeberg, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," Future Generation Computer Systems, vol. 78, pp. 641–658, 2018.

[98] C.-F. Lai, D.-Y. Song, R.-H. Hwang, and Y.-X. Lai, "A QoS-aware streaming service over fog computing infrastructures," 2016 Digital Media Industry & Academic Forum (DMIAF), 2016.

[99] T. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela, and M. Vilar-Montesinos, "A Fog Computing and Cloudlet Based Augmented Reality System for the Industry 4.0 Shipyard," Sensors, vol. 18, no. 6, p. 1798, 2018.

[100] B. Tang, Z. Chen, G. Hefferman, S. Pei, T. Wei, H. He, and Q. Yang, "Incorporating Intelligence in Fog Computing for Big Data Analysis in Smart Cities," IEEE Transactions on Industrial Informatics, vol. 13, no. 5, pp. 2140–2150, 2017.

[101] O. T. T. Kim, N. D. Tri, N. H. Tran, C. S. Hong et al., "A shared parking model in vehicular network using fog and cloud environment," in Proceedings of the 2015 IEEE 17th Asia-Pacific Network Operations and Management Symposium. IEEE, 2015, pp. 321–326

[102] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," IEEE Transactions on Vehicular Technology, vol. 65, no. 6, pp. 3860–3873, 2016

[103] X. Chen and L. Wang, "Exploring fog computing based adaptive vehicular data scheduling policies through a compositional formal method – PEPA," IEEE Communications Letters, 2017.

[104] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of Vehicles: A Fog-Enabled Real-Time Traffic Management System," IEEE Transactions on Industrial Informatics, vol. 14, no. 10, pp. 4568–4578, 2018.

[105] Liao, S., Li, J., Wu, J., Yang, W. and Guan, Z., 2019. Fog-Enabled Vehicle as a Service for Computing Geographical Migration in Smart Cities. IEEE Access, 7, pp.8726-8736.

[106] Luan, T.H., Gao, L., Li, Z., Xiang, Y., Wei, G. and Sun, L., 2015. Fog computing: Focusing on mobile users at the edge. arXiv preprint arXiv:1502.01815.

[107] Y. Huo, C. Yong, and Y. Lu, "Re-ADP: Real-Time Data Aggregation with Adaptive ω-Event Differential Privacy for Fog Computing," Wireless Communications and Mobile Computing, vol. 2018, pp. 1–13, 2018.

[108] Dastjerdi, A.V., Gupta, H., Calheiros, R.N., Ghosh, S.K. and Buyya, R., "Fog computing: Principles, architectures, and applications", In Internet of things (pp. 61-75), 2016

[109] Nath, S.B., Gupta, H., Chakraborty, S. and Ghosh, S.K., "A survey of fog computing and communication: current researches and future directions", arXiv preprint arXiv:1804.04365, 2018.

[110] Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges, "IEEE Access, vol. 5, pp. 19 293–19 304, Sept. 2017.

[111] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data Security and Privacy in Fog Computing," IEEE Network, vol. 32, no. 5, pp. 106–111, 2018.

[112] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[113] C. Dsouza, G.-J. Ahn, and M. Taguinod, "Policy-driven security management for fog computing: Preliminary framework and a case study," in Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IRI). IEEE, 2014, pp. 16–23.

[114] P. Zhang, J. K. Liu, F. R. Yu, M. Sookhak, M. H. Au, and X. Luo, "A Survey on Access Control in Fog Computing," IEEE Communications Magazine, vol. 56, no. 2, pp. 144–149, 2018.

[115] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120–134, 2014.

[116] M.B.Monir, M.H.Abdelaziz, A.A. AbdelhamidA, M. EI-Horbaty. "Trust management in cloud computing: a survey," Proceedings of the IEEE 7th international conference on intelligent computing and information systems, ICICIS2015, pp.231–42, 2016.

[117] F. H. Rahman, T.-W. Au, S. S. Newaz, W. S. Suhaili, and G. M. Lee, "Find my trustworthy fogs: A fuzzy-based trust evaluation framework," Future Generation Computer Systems, 2018.

[118] M. Tsugawa, A. Matsunaga, and J. A. Fortes, "Cloud computing security: What changes with software-defined networking?" in Secure Cloud Computing. Springer, 2014, pp. 77–93.

[119] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure intelligent traffic light control using fog computing," Future Generation Computer Systems, 2017

[120] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," IEEE Internet of Things Journal, 2017.

[121] L. Ma, A. Y. Teymorian, and X. Cheng, "A hybrid rogue access point protection framework for commodity wi-fi networks," in Proceedings of the 2008 27th IEEE International Conference on Computer Communications (INFOCOM). IEEE, 2008, pp. 1220–1228.

[122] Sudqi Khater, B.; Abdul Wahab, A.W.B.; Idris, M.Y.I.B.; Abdulla Hussain, M.; Ahmed Ibrahim, A. A "Lightweight Perceptron-Based Intrusion Detection System for Fog Computing.", Appl. Sci. 2019.

[123] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy-preserving vehicular crowdsensing based road surface condition monitoring system using fog computing," IEEE Internet of Things Journal, 2017.

[124] S. He, B. Cheng, H. Wang, X. Xiao, Y. Cao, and J. Chen, "Data security storage model for fog computing in large-scale IoT application," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2018.

[125] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for Fog Computing," Future Generation Computer Systems, vol. 78, pp. 799–806, 2018.

[126] [126]. J. Ni, X. Lin, K. Zhang, and X. Shen, "Privacy-Preserving Real-Time Navigation System Using Vehicular Crowdsourcing," 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), 2016.

[127] J. Ni, A. Zhang, X. Lin, and X. S. Shen, "Security, Privacy, and Fairness in Fog-Based Vehicular Crowdsensing," IEEE Communications Magazine, vol. 55, no. 6, pp. 146–152, 2017.

[128] P. Zhang, M. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," Future Generation Computer Systems, vol. 88, pp. 16–27, 2018.

[129] T. Gandhi and M. Trivedi, "Pedestrian Protection Systems: Issues, Survey, and Challenges," IEEE Trans. Intelligent Transportation Systems, vol. 8, no. 3, pp. 413-430, Sept. 2007.

[130] C. Sugimoto, Y. Nakamura, and T. Hashimoto, "Development of Pedestrian-to-Vehicle Communication System Prototype for Pedestrian Safety Using both Wide-Area and Direct Communication," 22nd International Conference on Advanced Information Networking and Applications (aina 2008), 2008.

[131] Munir, K. Prasanna, and SU. Khan, "IFCIoT: Integrated Fog Cloud IoT Architectural Paradigm for Future Internet of Things." arXiv preprint arXiv:1701.08474, 2017.

[132] M.Lu, K.Wevers, and R.V.D. Heijden, "Technical Feasibility of Advanced Driver Assistance Systems (ADAS) for Road Traffic Safety," Transportation Planning and Technology, vol. 28, no. 3, pp. 167–187, 2005.

[133] K.J. Boxey, "Pedestrian air bag." U.S. Patent No. 8,016,066. 13 Sep. 2011.

[134] techworm.net, "Dutch authorities testing out traffic lights for smartphone addicts", 2017. [Online]. Available: https://www.techworm.net/2017/02/dutch-authorities-testing-traffic-lights-smartphone-addicts.html. [Accessed: 20 – Feb- 2017]

[135] K. Abbas, A. F. Hefny, and F. M. Abu-Zidan, "Seatbelts and road traffic collision injuries," World Journal of Emergency Surgery, vol. 6, no. 1, p. 18, 2011.

[136] J. C. A. Pérez, F. Seco, V. Milanés, A. Jiménez, J. C. Díaz, and T. D. Pedro, "An RFID-Based Intelligent Vehicle Speed Controller Using Active Traffic Signals," Sensors, vol. 10, no. 6, pp. 5872–5887, Sep. 2010.

[137] N. Virtanen, A. Schirokoff, J. and Luoma, "Impacts of an automatic emergency call system on accident consequences", In Proceedings of the 18th ICTCT, Workshop Transport telemetric and safety, pp. 1-6, 2005.

[138] S. Dashtinezhad, T. Nadeem, B. Dorohonceanu, C. Borcea, P. Kang, and L. Iftode, "TrafficView: a driver assistant device for traffic monitoring based on car-to-car communication," 2004 IEEE 59th Vehicular Technology Conference. VTC 2004-Spring , 2004

[139] Breed, D.S. and Shokoohi, F., "Padding to reduce injuries in automobile accidents", Automotive Technologies International Inc.. U.S. Patent 5,098,124, 1992.

[140] M. Mackay, S. Parkin, and A. Scott., "Intelligent restraint systems–what characteristics should they have", Advances in Occupant Restraint Technologies, pp.113-126, 1994

[141] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea, and L. Iftode, "Adaptive Traffic Lights Using Car-to-Car Communication," 2007 IEEE 65th Vehicular Technology Conference - VTC2007-Spring, 2007.

[142] F. Philip, W. Fangman, J. Liao, M. Lilienthal, and K. Choi, "Helmets Prevent Motorcycle Injuries with Significant Economic Benefits," Traffic Injury Prevention, vol. 14, no. 5, pp. 496–500, Apr. 2013.

[143] M. Ptak and K. Konarzewski, “Numerical Technologies for Vulnerable Road User Safety Enhancement,” New Contributions in Information Systems and Technologies Advances in Intelligent Systems and Computing, pp. 355–364, 2015.

[144] T. Takahashi, H. Kim, and S. Kamijo, “Urban road user classification framework using local feature descriptors and HMM,” 2012 15th International IEEE Conference on Intelligent Transportation Systems, 2012.

[145] Bauer, “On the (In-)Accuracy of GPS Measures of Smartphones,” Proceedings of International Conference on Advances in Mobile Computing & Multimedia - MoMM '13, 2013.

[146] backyardbrains.com, “Experiment: How Fast Your Brain Reacts to Stimuli”. [Online]. Available: https://backyardbrains.com/experiments/reactiontime. [Accessed:30 – Feb- 2017].

[147] S. Kato, M. Hiltunen, K. Joshi, and R. Schlichting, “Enabling vehicular safety applications over LTE networks,” 2013 International Conference on Connected Vehicles and Expo (ICCVE), 2013.

[148] “ns-3,” ns3 RSS. [Online]. Available: https://www.nsnam.org/. [Accessed: 28-Feb-2017].

[149] “Professionelle Suchmaschinenoptimierung,” UDG SUMO. [Online]. Available: http://www.sumo.de/. [Accessed: 28-Mar-2017].

[150] Keum, Clara Binnara. "Analysis of road traffic crashes and injury severity of pedestrian victims in the Gambia." MS (Master of Science) thesis, University of Iowa, 2016. http://ir.uiowa.edu/etd/2097

[151] J Knowles, L Smith, R Cuerden and E Delmonte, “Analysis of police collision files for pedestrian fatalities in London”, TRL, London, England, 2006.

[152] D.R. Kouabenan, and J.M. Guyot, “Study of the causes of pedestrian accidents by severity”, Journal of Psychology in Africa, 14(2), pp.119-126, 2004.

[153] J. Rokytova, and M. Sklenar, .” Analysis of road accidents on pedestrian crossings caused by speeding,” In speed management strategies and implementation-planning, evaluation, behavioural, legal and institutional issues-proceedings and abstracts of 15th ictct workshop held brno, czech republic, October 2002.

[154] timesofindia.indiatimes.com, “City recorded 82 accidents at pedestrian crossings last year”, 2015. [Online]. Available: http://timesofindia.indiatimes.com/city/coimbatore/City-recorded-82-accidents-at-pedestrian-crossings-last-year/articleshow/48229641.cms. [Accessed: 12 – Jan- 2017]

[155] Z. H. Mir and F. Filali, “LTE and IEEE 802.11p for vehicular networking: a performance evaluation,” EURASIP Journal on Wireless Communications and Networking, vol. 2014, no. 1, p. 89, 2014.

[156] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, “LTE for vehicular networking: a survey,” IEEE Communications Magazine, vol. 51, no. 5, pp. 148–157, 2013.

[157] G. Guido, A. Vitale, V. Astarita, F. Saccomanno, V. P. Giofré, and V. Gallelli, “Estimation of Safety Performance Measures from Smartphone Sensors,” Procedia - Social and Behavioral Sciences, vol. 54, 2012.

[158] J. Wahlstrom, I. Skog, and P. Handel, “Smartphone-Based Vehicle Telematics: A Ten-Year Anniversary,” IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 10, pp. 2802–2825, 2017.

[159] D.A. Ritchie, "Factors That Affect the Global Positioning System and Global Navigation Satellite System in an Urban and Forested Environment." (2007). Electronic Teses and Dissertations. Paper 2089. http://dc.etsu.edu/etd/2089

[160] M. Hashemi and H. A. Karimi, “A critical review of real-time map-matching algorithms: Current issues and future directions,” Computers, Environment and Urban Systems, vol. 48, pp. 153–165, 2014.

[161] S. Brakatsoulas, D. Pfoser, R. Salas, and C. Wenk. "On map-matching vehicle tracking data." In Proceedings of the 31st international conference on Very large data bases, pp. 853-864, 2005.

[162] P. Senin, "Dynamic time warping algorithm review." Information and Computer Science Department University of Hawaii at Manoa Honolulu, USA 855 (2008): 1-23

[163] S. Dixon, "Live tracking of musical performances using on-line time warping”, Proc. of the 8th Int. Conference on Digital Audio Effects (DAFx’05), Madrid, Spain, September 20-22, 2005

[164] M.A. Quddus, “High Integrity Map Matching Algorithms for Advanced Transport Telematics Applications”, Imperial College London, United Kingdom, thesis, 2006.

[165] M. A. Quddus, W. Y. Ochieng, and R. B. Noland, “Current map-matching algorithms for transport applications: State-of-the art and future research directions,” Transportation Research Part C: Emerging Technologies, vol. 15, no. 5, pp. 312–328, 2007.

[166] R. Jirawimut, P. Ptasinski, V. Garaj, F. Cecelja, and W. Balachandran, “A method for dead reckoning parameter correction in pedestrian navigation system,” IEEE Transactions on Instrumentation and Measurement, vol. 52, no. 1, pp. 209–215, 2003.

[167] J.D. Martina, J. Kroscheb, S. Boll, “Dynamic GPS-position correction for mobile pedestrian navigation and orientation “, Proceedings of the 3rd Workshop On Positioning, Navigation And Communication (WPNC’06), pp. 199-2008, 2006

[168] M. Ren, “Advanced Map Matching Technologies and Techniques for Pedestrian/Wheelchair Navigation”, University of Pittsburgh, 2012

[169] M. Ren and H. A. Karimi, “A Chain-Code-Based Map Matching Algorithm for Wheelchair Navigation,” Transactions in GIS, 2009.

[170] M. Ren and H. A. Karimi, “A Hidden Markov Model-Based Map-Matching Algorithm for Wheelchair Navigation,” Journal of Navigation, vol. 62, no. 03, p. 383, 2009.

[171] M. Ren and H. A. Karimi, “A fuzzy logic map matching for wheelchair navigation,” GPS Solutions, vol. 16, no. 3, pp. 273–282, Dec. 2011.

[172] D. Bétaille, F. Peyret, and M. Voyer, “Applying Standard Digital Map Data in Map-aided, Lane-level GNSS Location,” Journal of Navigation, vol. 68, no. 05, pp. 827–847, 2015.

[173] L. T. Hsu, Y. Gu, and S. Kamijo, “3D building model-based pedestrian positioning method using GPS/GLONASS/QZSS and its reliability calculation,” GPS Solutions, vol. 20, no. 3, 2015.

[174] Y. Bang, J. Kim, and K. Yu, “An Improved Map-Matching Technique Based on the Fréchet Distance Approach for Pedestrian Navigation Services,” Sensors, vol. 16, no. 12, p. 1768, 2016.

[175] Y. Wakuda, S. Asano, N. Koshizuka, and K. Sakamura, “An adaptive map-matching based on Dynamic Time Warping for pedestrian positioning using network map,” Proceedings of the 2012 IEEE/ION Position, Location and Navigation Symposium, 2012.

[176] I. Oregi, A. Pérez, J. D. Ser, and J. A. Lozano, “On-Line Dynamic Time Warping for Streaming Time Series,” Machine Learning and Knowledge Discovery in Databases Lecture Notes in Computer Science, 2017.

[177] E. J. Keogh, and M. J. Pazzani, “Derivative Dynamic Time Warping”

[178] M. Meinard, “Information Retrieval for Music and Motion”, 2007

[179] J. Zhao and L. Itti, “shapeDTW: Shape Dynamic Time Warping,” Pattern Recognition, vol. 74, pp. 171–184, 2016.

[180] H. Sakoe and S. Chiba, “Dynamic Programming Algorithm Optimization for Spoken Word Recognition,” Readings in Speech Recognition, pp. 159–165, 1990.

[181] T. Górecki and M. Łuczak, “First and Second Derivatives in Time Series Classification Using DTW,” Communications in Statistics - Simulation and Computation, vol. 43, no. 9, 2014.

[182] J. Podesta, “Brief Tutorial on the Kalman Filter,” Jan. 1994.

[183] S. Zhang and S. Yang, “A novel fusion method for DR/GPS integrated navigation system,” 6th IEEE International Conference on Industrial Informatics, 2008.

[184] J. Gomez-Gil, R. Ruiz-Gonzalez, S. Alonso-Garcia, and F. Gomez-Gil, "A Kalman Filter Implementation for Precision Improvement in Low-Cost GPS Positioning of Tractors," Sensors, vol. 13, no. 12, 2013.

[185] OpenstreetMap.com, "OpenStreetMap," 2017. [Online]. Available: http://www.OpenstreetMap.com. [Accessed: 12-Dec-2017]

[186] M. Hashemi and H. A. Karimi, "A Machine Learning Approach to Improve the Accuracy of GPS-Based Map-Matching Algorithms (Invited Paper)," 2016 IEEE 17th International Conference on Information Reuse and Integration (IRI), 2016.

[187] K. L. A. El-Ashmawy, "Testing the positional accuracy of OpenStreetMap data for mapping applications," Geodesy and Cartography, vol. 42, no. 1, pp. 25–30, Feb. 2016.

[188] F. Xia, C.-H. Hsu, X. Liu, H. Liu, F. Ding, and W. Zhang, ''The power of smartphones,'' Multimedia Syst., vol. 21, no. 1, pp. 87–101, Feb. 2015.

[189] A. Jaiswal, Y. Chiang, C. A. Knoblock, and L. Lan, "Location Prediction with Sparse GPS Data", In Proceedings of the 8th Geographic Information Science, 2014.

[190] Y. Han, Q. Li, W. He, F. Wan, B. Wang and K. Mizuno, "Analysis of Vulnerable Road User Kinematics Before/During/After Vehicle Collisions Based on Video Records", IRCOBI Conference, Antwerp, Belgium, 13-15 September, 2017

[191] A. Correa, M. Barcelo, A. Morell and J. L. Vicario, "A Review of Pedestrian Indoor Positioning Systems for Mass Market Applications," Sensors, vol. 17, no. 8, p. 1927, 2017.

[192] M. Kourogi and T. Kurata, "A method of pedestrian dead reckoning for smartphones using frequency domain analysis on patterns of acceleration and angular velocity," IEEE/ION Position, Location and Navigation Symposium, 2014.

[193] K. Nawarathne, F. Zhao, F. C. Pereira, and J. Luo, "Dead reckoning on smartphones to reduce GPS usage," 13th International Conference on Control Automation Robotics & Vision, 2014.

[194] Wei-Wen Kao, "Integration of GPS and dead-reckoning navigation systems," Vehicle Navigation and Information Systems Conference, 1991.

[195] W. Kang and Y. Han, "SmartPDR: Smartphone-Based Pedestrian Dead Reckoning for Indoor Localization," IEEE Sensors Journal, vol. 15, no. 5, pp. 2906–2916, 2015.

[196] R. Zhou, "Pedestrian dead reckoning on smartphones with varying walking speed," 2016 IEEE International Conference on Communications, 2016.

[197] J. Biagioni, A. B. M. Musa, and J. Eriksson, “Thrifty tracking,” Proceedings of the 21st ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems - SIGSPATIAL13, 2013.

[198] Z. Tian, Y. Zhang, M. Zhou, and Y. Liu, “Pedestrian dead reckoning for MARG navigation using a smartphone,” EURASIP Journal on Advances in Signal Processing, 2014.

[199] L. Ilkovičová, P. Kajánek, and A. Kopáčik. "Pedestrian Indoor Positioning and Tracking using Smartphone Sensors, Step Detection and Map Matching Algorithm." International Symposium on Engineering Geodesy. 2016.

[200] J.-K. Liao, K.-W. Chiang, and Z.-M. Zhou, “The Performance Analysis of Smartphone-Based Pedestrian Dead Reckoning and Wireless Locating Technology for Indoor Navigation Application,” Inventions, vol. 1, no. 4, p. 25, May 2016.

[201] android.com, “Sensor Types”, 2017. [Online]. Available: https://source.android.com/devices/sensors/sensor-types#gravity. [Accessed: 22-Mar-2018]

[202] E. Alemneh, S.-M. Senouci, and P. Brunet, An Online Time Warping based Map Matching for Vulnerable Road Users’ Safety”, 14th International Wireless Communications and Mobile Computing Conference, 2018.

[203] S. Kitanov and T. Janevski, “Energy efficiency of Fog Computing and Networking services in 5G networks,” IEEE EUROCON 2017 -17th International Conference on Smart Technologies, 2017.

[204] S. Winkler, J. Kazazi, and M. Vollrath, “Distractive or Supportive -- How Warnings in the Head-up Display Affect Drivers Gaze and Driving Behavior,” 2015 IEEE 18th International Conference on Intelligent Transportation Systems, 2015.

[205] S. Winkler, J. Kazazi, and M. Vollrath, “Practice makes better – Learning effects of driving with a multi-stage collision warning,” Accident Analysis & Prevention, vol. 117, pp. 398–409, 2018.

[206] R. B. Zadeh, M. Ghatee, and H. R. Eftekhari, “Three-Phases Smartphone-Based Warning System to Protect Vulnerable Road Users Under Fuzzy Conditions,” IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 7, pp. 2086–2098, 2018.

[207] E. Wang, Y. Yang, and J. Wu, “Energy Efficient Beaconing Control Strategy Based on Time-Continuous Markov Model in DTNs,” IEEE Transactions on Vehicular Technology, vol. 66, no. 8, pp. 7411–7421, 2017.

[208] K. Boc, J. Vaculik, and D. Vidrikova, “Fuzzy approach to risk analysis and its advantages against the qualitative approach.”, In Proceedings of the 12th International Conference “Reliability and Statistics in Transportation and Communication” (RelStat’12) 2012 Oct (pp. 17-20).

[209] K.Z. Ghafoor, J. Lloret, K.A. Bakar, A. S. Sadiq, and S.A. Mussa, “Beaconing approaches in vehicular ad hoc networks: A survey”, Wireless personal communications, 885-912, 2013.

[210] S. A. A. Shah, E. Ahmed, F. Xia, A. Karim, M. Shiraz, & R. M. Noor, “Adaptive beaconing approaches for vehicular ad hoc networks: A survey.”, IEEE Systems Journal, 12(2), 1263-1277, 2018.

[211] C.-L. Huang, Y. Fallah, R. Sengupta, and H. Krishnan, “Adaptive intervehicle communication control for cooperative safety systems,” IEEE Network, vol. 24, no. 1, pp. 6–13, 2010.

[212] R. Schmidt, T. Leinmuller, E. Schoch, F. Kargl, and G. Schafer, “Exploration of adaptive beaconing for efficient intervehicle safety communication,” IEEE Network, vol. 24, no. 1, pp. 14–19, 2010.

[213] P. Greibe, “Accident prediction models for urban roads,” Accident Analysis & Prevention, vol. 35, no. 2, pp. 273–285, 2003.

[214] Ki, Y.K., 2007. Accident detection system using image processing and MDR. International Journal of Computer Science and Network Security IJCSNS, 7(3), pp.35-39.

[215] W. Hu, X. Xiao, D. Xie, T. Tan, & S. Maybank, “Traffic Accident Prediction Using 3-D Model-Based Vehicle Tracking,” IEEE Transactions on Vehicular Technology, vol. 53, no. 3, 2004.

[216] J. Castro, M. Delgado, J. Medina, and M. Ruiz-Lozano, “Corrigendum to ‘An expert fuzzy system for predicting object collisions. Its application for avoiding pedestrian accidents’, Expert Systems with Applications 2011.

[217] A. S. Tomar, M. Singh, G. Sharma, and K. Arya, “Traffic Management using Logistic Regression with Fuzzy Logic,” Procedia Computer Science, vol. 132, pp. 451–460, 2018.

[218] C. Zhang, J. Hu, J. Qiu, W. Yang, H. Sun, and Q. Chen, “A Novel Fuzzy Observer-Based Steering Control Approach for Path Tracking in Autonomous Vehicles,” IEEE Transactions on Fuzzy Systems, pp. 1–1, 2018.

[219] Y. Z. Arslan, A. Sezgin, and N. Yagiz, “Improving the ride comfort of vehicle passenger using fuzzy sliding mode controller,” Journal of Vibration and Control, vol. 21, no. 9, pp. 1667–1679, 2013.

[220] J. J. Rolison, S. Regev, S. Moutari, and A. Feeney, “What are the factors that contribute to road accidents? An assessment of law enforcement views, ordinary drivers’ opinions, and road accident records,” Accident Analysis & Prevention, vol. 115, pp. 11–24, 2018.

[221] N.Chakrabarty & K.Gupta, “Analysis of Driver Behaviour and Crash Characteristics during Adverse Weather Conditions,” Procedia - Social and Behavioral Sciences, vol. 104, pp. 1048–1057, 2013.

[222] S. Plainis and I. J. Murray, “Reaction times as an index of visual conspicuity when driving at night,” Ophthalmic and Physiological Optics, vol. 22, no. 5, pp. 409–415, 2002.

[223] C. Edwards, J. Creaser, J. Caird, A. Lamsdale, and S. Chisholm, “Older and Younger Driver Performance at Complex Intersections: Implications for Using Perception-Response Time and Driving Simulation,” Proceedings of the 2nd International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design: Driving Assessment 2003, 2005.

[224] P. Choudhary and N. R. Velaga, “Modelling driver distraction effects due to mobile phone use on reaction time,” Transportation Research Part C: Emerging Technologies, vol. 77, pp. 351–365, 2017.

[225] Z. Christoforou, M. G. Karlaftis, and G. Yannis, “Reaction times of young alcohol-impaired drivers,” Accident Analysis & Prevention, vol. 61, pp. 54–62, 2013.

[226] rdmag.com, “Promising Vehicle Tech Will Detect Drunk Drivers Before They Hit the Road”,2018. [Online]. Available: https://www.rdmag.com/article/2017/08/promising-vehicle-tech-will-detect-drunk-drivers-they-hit-road. [Accessed:20 – Apr- 2019]

[227] X. Jiang, W. Wang, and K. Bengler, “Intercultural Analyses of Time-to-Collision in Vehicle–Pedestrian Conflict on an Urban Midblock Crosswalk,” IEEE Transactions on Intelligent Transportation Systems, pp. 1–6, 2014.

[228] J.Y. Wong, “Theory of Ground Vehicles”, 3rd Edition, 2008.

[229] A. Barua, L. S. Mudunuri, and O. Kosheleva, “Why trapezoidal and triangular membership functions work so well: Towards a theoretical explanation.”, Journal of Uncertain Systems, 8, 2014.

[230] N. Lubbe and E. Rosén, “Pedestrian crossing situations: Quantification of comfort boundaries to guide intervention timing,” Accident Analysis & Prevention, vol. 71, pp. 261–266, 2014.

[231] J. Scholliers, D. Bell, A. Morris, A. B. G. Meléndez, and O. M. Perez, “Improving Safety and Mobility of Vulnerable Road Users Through ITS Applications,” Traffic Safety, pp. 251–269, 2016.

[232] D. F. Blower, “Key pedestrian collision scenarios in the US for effective collision avoidance technologies”, 2014.

[233] V. R. Rengaraju and V. T. Rao, “Vehicle-Arrival Characteristics at Urban Uncontrolled Intersections,” Journal of Transportation Engineering, vol. 121, no. 4, pp. 317–323, 1995.

[234] F. Mannering, W. Kilareski, and S. Washburn, “Principles of highway engineering and traffic analysis (3th edition),” John Wiley & Sons, Inc, 2004.

[235] J. Huang, F. Qian, A. Gerber, Z. M. Mao, S. Sen, and O. Spatscheck, "A close examination of performance and power characteristics of 4G LTE networks," Proceedings of the 10th international conference on Mobile systems, applications, and services - MobiSys 12, 2012.

[236] F. Arena and G. Pau, "An Overview of Vehicular Communications," Future Internet, vol. 11, no. 2, p. 27, 2019.

[237] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," Proceedings of the first ACM workshop on Vehicular ad hoc networks - VANET 04, 2004.

[238] H. Li and M. Singhal, "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45–53, 2007.

[239] T. S. Dybedokken, "Trust Management in Fog Computing," MS thesis. NTNU, 2017.

[240] J.-H. Cho, A. Swami, and I.-R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," IEEE Communications Surveys & Tutorials, vol. 13, no. 4, pp. 562–583, 2011.

[241] Y. Wang and J. Vassileva, "Trust and reputation model in peer-to-peer networks," Proceedings Third International Conference on Peer-to-Peer Computing (P2P2003), 2003.

[242] Z. M. Aljazzaf, M. A. M. Capretz, and M. Perry, "Trust bootstrapping services and service providers," 2011 Ninth Annual International Conference on Privacy, Security and Trust, 2011.

[243] J. Guo, I.-R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," Computer Communications, vol. 97, pp. 1–14, 2017.

[244] I.-R. Chen, J. Guo, F. Bao, and J.-H. Cho, "Integrated social and quality of service trust management of mobile groups in ad hoc networks," 2013 9th International Conference on Information, Communications & Signal Processing, 2013.

[245] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving a Social Structure to the Internet of Things," IEEE Communications Letters, vol. 15, no. 11, pp. 1193–1195, 2011.

[246] V. L. Tran, A. Islam, J. Kharel, and S. Y. Shin, "On the Application of Social Internet of Things with Fog Computing: A New Paradigm for Traffic Information Sharing System," 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), 2018.

[247] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," Personal and Ubiquitous Computing, vol. 18, no. 1, pp. 163–175, 2012.

[248] A. Jøsang, "Decision Making Under Vagueness and Uncertainty," Artificial Intelligence: Foundations, Theory, and Algorithms Subjective Logic, pp. 51–82, 2016.

[249] I.-R. Chen, J. Guo, and F. Bao, "Trust management for service composition in SOA-based IoT systems," 2014 IEEE Wireless Communications and Networking Conference (WCNC), 2014.

[250] F. Bao and I.-R. Chen, "Trust management for the internet of things and its application to service composition," 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012.

[251] F. Bao, I.-R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems," 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), 2013.

[252] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," Proceedings of the 2012 international workshop on Self-aware internet of things - Self-IoT 12, 2012.

[253] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: A trust management model based on fuzzy reputation for internet of things," Computer Science and Information Systems, vol. 8, no. 4, pp. 1207–1228, 2011.

[254] U. Jayasinghe, N. B. Truong, G. M. Lee, and T.-W. Um, "RpR: A Trust Computation Model for Social Internet of Things," 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016.

[255] M. Khani, Y. Wang, M. A. Orgun, and F. Zhu, "Context-Aware Trustworthy Service Evaluation in Social Internet of Things," Service-Oriented Computing Lecture Notes in Computer Science, pp. 129–145, 2018.

[256] M. Chiregi and N. J. Navimipour, "Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms," Journal of Electrical Systems and Information Technology, vol. 5, no. 3, pp. 608–622, 2018.

[257] T. H. Noor, Q. Z. Sheng, S. Zeadally, and J. Yu, "Trust management of services in cloud environments," ACM Computing Surveys, vol. 46, no. 1, pp. 1–30, 2013.

[258] J. Huang and D. M. Nicol, "Trust mechanisms for cloud computing," Journal of Cloud Computing: Advances, Systems and Applications, vol. 2, no. 1, p. 9, 2013.

[259] S. Chakraborty and K. Roy, "An SLA-based Framework for Estimating Trustworthiness of a Cloud," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[260] P. Manuel, “A trust model of cloud computing based on Quality of Service,” Annals of Operations Research, vol. 233, no. 1, pp. 281–292, 2013.

[261] R. Hajizadeh and N. J. Navimipour, “A method for trust evaluation in the cloud environments using a behavior graph and services grouping,” Kybernetes, pp. 00–00, 2017.

[262] I.-R. Chen, J. Guo, D.-C. Wang, J. J. P. Tsai, H. Al-Hamadi, and I. You, “Trust-based Service Management for Mobile Cloud IoT Systems,” IEEE Transactions on Network and Service Management, pp. 1–1, 2018.

[263] F. H. Rahman, T. W. Au, S. H. S. Newaz, and W. S. Suhaili, “Trustworthiness in Fog: A Fuzzy Approach” Proceedings of the 2017 VI International Conference on Network, Communication and Computing - ICNCC 2017, 2017.

[264] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, “The Role of Trust Management in Distributed Systems Security,” Secure Internet Programming Lecture Notes in Computer Science, pp. 185–210, 1999.

[265] M. Wazid, A. K. Das, N. Kumar, and A. V. Vasilakos, “Design of secure key management and user authentication scheme for fog computing services,” Future Generation Computer Systems, vol. 91, pp. 475–492, 2019.

[266] P. Velloso, R. Laufer, D. D. O. Cunha, O. C. Duarte, and G. Pujolle, “Trust management in mobile ad hoc networks using a scalable maturity-based model,” IEEE Transactions on Network and Service Management, vol. 7, no. 3, pp. 172–185, 2010.

[267] S. Namal, H. Gamaarachchi, G. Myounglee, and T.-W. Um, “Autonomic trust management in cloud-based and highly dynamic IoT applications,” 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015), 2015.

[268] V. Paxson, “Empirically derived analytic models of wide-area TCP connections,” IEEE/ACM Transactions on Networking, vol. 2, no. 4, pp. 316–336, 1994.

[269] G. Hasslinger, O. Hohlfeld, “The Gilbert-Elliott model for packetloss in real time services on the Internet,” inProc. of GI/ITGConference on Measuring, Modelling and Evaluation of Computer andCommunication Systems (MMB), 2008.

[270] A. Bildea, O. Alphand, F. Rousseau, and A. Duda, “Link quality estimation with the Gilbert-Elliot model for wireless sensor networks,” 2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2015.

[271] I.-R. Chen and J. Guo, “Dynamic Hierarchical Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection,” 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, 2014.

[272] J sang and S.J. Knapskog, “A metric for trusted systems”, Global IT Security Wien: Austrian computer Society, pp.541-549, 199.

[273] A. Jøsang, “A Logic for Uncertain Probabilities,” International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 09, no. 03, pp. 279–311, 2001.

[274] A. Jøsang, S. Marsh, and S. Pope, “Exploring Different Types of Trust Propagation,” Lecture Notes in Computer Science Trust Management, pp. 179–192, 2006.

[275] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, “iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments,” Software: Practice and Experience, vol. 47, no. 9, pp. 1275–1296, 2017.

[276] M. Etemad, M. Aazam, and M. St-Hilaire, “Using DEVS for modeling and simulating a Fog Computing environment,” 2017 International Conference on Computing, Networking and Communications (ICNC), 2017.

[277] R. Mayer, L. Graser, H. Gupta, E. Saurez, and U. Ramachandran, “EmuFog: Extensible and scalable emulation of large-scale fog computing infrastructures,” IEEE Fog World Congress (FWC), 2017.

[278] A. Brogi and S. Forti, “QoS-Aware Deployment of IoT Applications Through the Fog,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1185–1192, 2017.

[279] Y. Wang, Y.C. Lu, I.R. Chen, J.H. Cho, and A. Swami, "LogitTrust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks," 6th ASE International Conference on Privacy, Security, Risk and Trust, Boston, MA, Dec. 2014.

[280] M. Nitti, R. Girau, and L. Atzori, “Trustworthiness Management in the Social Internet of Things,” IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 5, pp. 1253–1266, 2014.

[281] M. Moussaïd, N. Perozo, S. Garnier, D, Helbing, and G. Theraulaz, “The walking behaviour of pedestrian social groups and its impact on crowd dynamics”, PloS one, 5(4), p.e10047m 2010

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

- AEB: Autonomous Emergency Braking. 13
- A-GPS: Assisted-GPS. 67
- BLE: Bluetooth Low Energy. 15
- BSA: Ballot-Stuffing Attack. 129
- CAM: Cooperative Awareness Message. 3, 6, 15, 35, 36, 38, 41, 42, 84, 87, 105, 129
- Car2X: Car-to-Everything. 19
- C-ITS: Cooperative ITS. 13, 14, 34
- DCRL: D_{min} based Collision Risk Level. 95 – 98.
- DENM: Decentralized Environmental Notification Message. 3, 36, 38, 84, 105, 130
- DR: Dead Reckoning. 52, 68, 69
- DSRC: Dedicated Short-Range Communications. 19
- DTW: Dynamic Time Warping. 50, 51, 53 – 55, 57, 61, 63, 64
- ETSI: European Telecommunication Standard Institute. 3, 17, 18, 35, 40, 43, 47, 48, 66, 69, 87
- FIS: Fuzzy Inference System. 85, 86, 91 – 95, 97
- GCS: Global Coordinate System. 74
- GDP: Gross Domestic Product. 1, 8
- GISP: GPS and INS Sensor based Prediction. 75 – 77, 81 - 83
- GNSS: Global Navigation Satellite System. 17, 49
- HMI: Human Machine Interfaces. 31, 34
- I2VRU: Infrastructure-to-VRU. 13
- INS: Inertial Navigation Systems. 6, 68, 69, 70, 71, 74, 75, 78 - 83
- IoT: Internet of Things. 20, 21, 23 – 27, 105, 108 - 110, 121, 127
- ISA: Intelligent Speed Adaptation. 13
- ITS: Intelligent Transportation Systems. 2, 8, 12 - 15, 19, 20, 23, 27, 31, 40, 49, 52, 65, 6, 83, 87
- LAN: Local Area Network. 21, 40
- LBS: Location Based Services. 87, 88
- LCS: Local Coordinate System. 74
- LOS: Line of Sight. 13, 30, 33
- LTE: Long-Term Evolution. 3, 19, 41 - 43, 45 – 47, 91, 99
- MTTM: Modified Two-way Trust Management. 125 - 127
- OSA: Opportunistic-Service Attack. 121