UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles

Sahil Garg, Amritpal Singh, Shalini Batra, Neeraj Kumar, and Laurence T. Yang

Abstract

Over the last few years, we have witnessed an exponential increase in the computing and storage capabilities of smart devices that has led to the popularity of an emerging technology called edge computing. Compared to the traditional cloud-computing-based infrastructure, computing and storage facilities are available near end users in edge computing. Moreover, with the widespread popularity of unmanned aerial vehicles (UAVs), huge amounts of information will be shared between edge devices and UAVs in the coming years. In this scenario, traffic surveillance using UAVs and edge computing devices is expected to become an integral part of the next generation intelligent transportation systems. However, surveillance in ITS requires uninterrupted data sharing, cooperative decision making, and stabilized network formation. Edge computing supports data processing and analysis closer to the deployed machines (i.e., the sources of the data). Instead of simply storing data and missing the opportunity to capitalize on it, edge devices can analyze data to gain insights before acting on them. Transferring data from the vehicle to the edge for real-time analysis can be facilitated by the use of UAVs, which can act as intermediate aerial nodes between the vehicles and edge nodes. However, as the communication between UAVs and edge devices is generally done using an open channel, there is a high risk of information leakage in this environment. Keeping our focus on all these issues, in this article, we propose a data-driven transportation optimization model where cyber-threat detection in smart vehicles is done using a probabilistic data structure (PDS)-based approach. A triple Bloom filter PDS- based scheduling technique for load balancing is initially used to host the real-time data coming from different vehicles, and then to distribute/collect the data to/from edges in a manner that minimizes the computational effort. The results obtained show that the proposed system requires comparatively less computational time and storage for load sharing, authentication, encryption, and decryption of data in the considered edge-computing-based smart transportation framework.

Introduction

The world is experiencing an evolution of smart cities that are paramount for unprecedented improvements in quality of life. City infrastructures and services are evolving at a rapid pace with interconnected systems used for monitoring, control, and automation. The emergence of connectivity in information technology poses challenges to our security and expectations of privacy. Today, cities have become more overcrowded with vehicles causing several problems like traffic congestion, unpredictable emergencies, and even threats to human life. In an era of smart environment, such inefficiencies cause enormous losses with respect to time, degrade vehicles' safety, and lead to high pollution. With the prediction that by 2050, 70 percent of the world's population will be living in cities, an enormous amount of effort needs to be put forth to make cities better and smarter [1].

Transportation is considered as a backbone of every city, and any disruptions in such systems can result in incidents ranging from annoyance to cyber-security abuse. The growing demand with respect to mobility has led to immense developments and variations in the transportation domain. Intelligent transportation systems (ITS) have become an effective way of advancing the performance of transportation systems [2]. Today, connected and autonomous vehicles can be found in every developed country, whereas developing countries are racing to bring them to the market. They provide an extensive array of communications-oriented applications intended to enhance travel safety, emend traffic management, curtail environmental impact, and exaggerate the use of transportation for both commercial users and the general public. Since they support the population and economy of every country around the globe, any threat to this network can cause significant impacts on its security and operations.

Surveillance in ITS requires coordinated decision making, continuous data sharing, and sustainable network formation. Until now, pre-installed cameras have been the most appropriate means of providing surveillance, but the advent of unmanned aerial vehicles (UAVs) in the next generation cellular networks have enhanced the connectivity manifold [4]. UAVs were initially introduced for military missions, and their use in modern-day networking has been recently expanded to civil applications. According to the U.S. Department of Transportation, dedicated short-range communications (DSRC) spectrum is allocated for the development of a network exclusively used for transportation. The Federal Communications Commission has set aside 75 MHz of spectrum for this very high data trans-

Digital Object Identifier:
10.1109/MNET.2018.1700286

Sahil Garg, Amritpal Singh, Shalini Batra, and Neeraj Kumar are with Thapar University; Laurence T. Yang is with St. Francis Xavier University.

0890-8044/18/$25.00 © 2018 IEEE

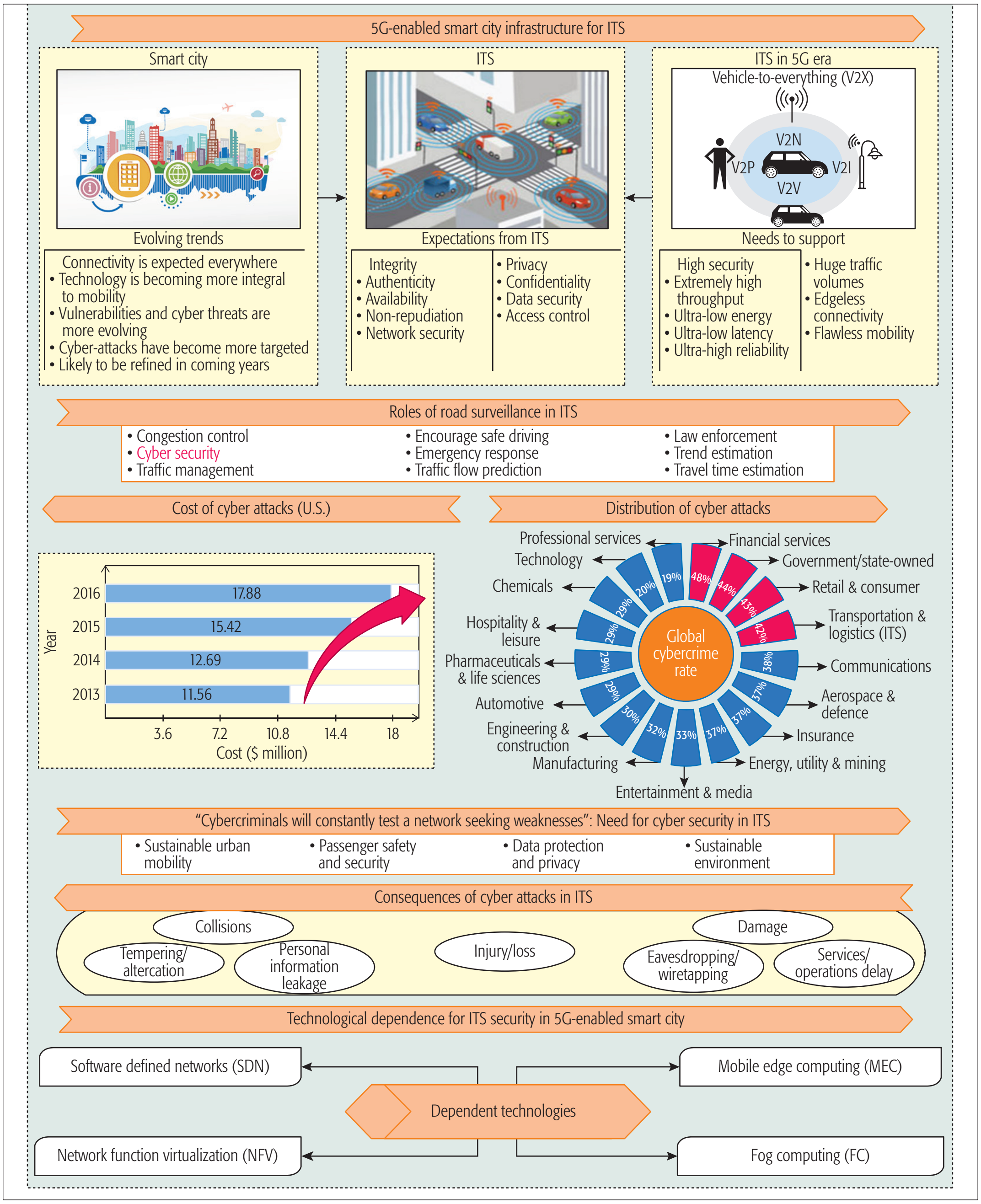

5G-enabled smart city infrastructure for ITS
Smart city
Evolving trends
Connectivity is expected everywhere
• Technology is becoming more integral to mobility
• Vulnerabilities and cyber threats are more evolving
• Cyber-attacks have become more targeted
• Likely to be refined in coming years
ITS
Expectations from ITS
Integrity
• Authenticity
• Availability
• Non-repudiation
• Network security
• Privacy
• Confidentiality
• Data security
• Access control
ITS in 5G era
Vehicle-to-everything (V2X)
V2N
V2P
V2I
V2V
Needs to support
High security
• Extremely high throughput
• Ultra-low energy
• Ultra-low latency
• Ultra-high reliability
• Huge traffic volumes
• Edgeless connectivity
• Flawless mobility
Roles of road surveillance in ITS
• Congestion control
• Cyber security
• Traffic management
• Encourage safe driving
• Emergency response
• Traffic flow prediction
• Law enforcement
• Trend estimation
• Travel time estimation
Cost of cyber attacks (U.S.)
Year
2016
17.88
2015
15.42
2014
12.69
2013
11.56
3.6
7.2
10.8
14.4
18
Cost ($ million)
Distribution of cyber attacks
Global cybercrime rate
Professional services
19%
Financial services
48%
Government/state-owned
44%
Retail & consumer
43%
Transportation & logistics (ITS)
42%
Communications
38%
Aerospace & defence
37%
Insurance
37%
Energy, utility & mining
37%
Entertainment & media
33%
Manufacturing
32%
Engineering & construction
30%
Automotive
29%
Pharmaceuticals & life sciences
29%
Hospitality & leisure
29%
Chemicals
29%
Technology
20%
"Cybercriminals will constantly test a network seeking weaknesses": Need for cyber security in ITS
• Sustainable urban mobility
• Passenger safety and security
• Data protection and privacy
• Sustainable environment
Consequences of cyber attacks in ITS
Collisions
Tempering/ altercation
Personal information leakage
Injury/loss
Damage
Eavesdropping/ wiretapping
Services/ operations delay
Technological dependence for ITS security in 5G-enabled smart city
Software defined networks (SDN)
Mobile edge computing (MEC)
Dependent technologies
Network function virtualization (NFV)
Fog computing (FC)

FIGURE 1. Architecture of smart city with respect to ITS [3].

mission wireless communication medium. Since DSRC can support fast network acquisition and secure transmissions with low latency, UAVs can be enabled with this technology to provide vehicle-to-everything (V2X) communications.

Developing a sustainable ITS requires seamless integration and interoperability with emerging technologies such as connected vehicles, cloud computing, and the Internet of Things. Due to rapid urbanization, the next generation mobile systems, commercially known as fifth generation (5G), aims to accelerate the development of ITS. The technological advancements such as software defined networks (SDN) and network functions virtualization (NFV) have changed the communication paradigm. Although data processing velocity has accelerated rapidly, bandwidth of the networks has not expanded appreciably. In order to fulfill the stringent low-latency requirement of 5G networks, computing technologies such as mobile edge computing (MEC) and fog computing are required to support this virtualized infrastructure. This is highlighted in Fig. 1. The processing of data at the edge yields more client processing, smaller response times, and less pressure on the network. Therefore, MEC is perceived as one of the indispensable technologies for 5G networks by the European 5G Infrastructure Public Private Partnership (5G PPP) research body. In addition, backed by industry leaders (e.g., Intel, Nokia, Huawei, and Vodafone) who participate in the European Telecommunications Standards Institute (ETSI) MEC Industry Specification Group (ISG), MEC is expected to provide a standards-based approach for significant progress toward 5G [5].

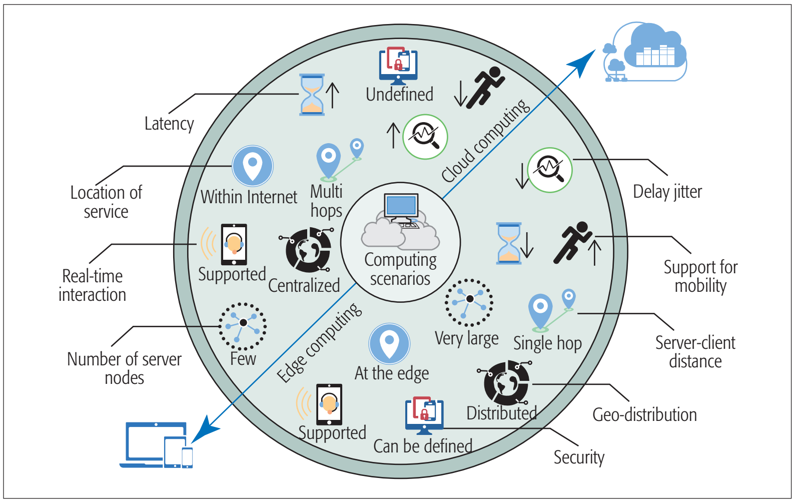


FIGURE 2. Edge computing vs. cloud computing.

In order to proceed further, the Open Edge Computing (OEC) initiative was launched by Vodafone, Intel, and Huawei in association with Carnegie Mellon University (CMU) in June 2015. Similarly, giants Cisco, Microsoft, Intel, Dell, and ARM partnered with Princeton University in November 2015 to launch the Open Fog Consortium (OFC) [6]. A global leader, Nokia, a member of the Multi-Access Edge Computing ETSI ISG, also proposed a solution named multi-access edge computing (MEC) by taking advantage of its telco cloud platform. This platform rapidly processes the data at the very periphery of the mobile network, which thereby delivers flexibility, scalability and efficiency to multiple base stations of the mobile network. Similarly, an edge computing architecture has been developed by Dell that helps to perform edge analytics with multiple power sources. Recent transition from client/server to distributed computing architectures convinced leading companies like Microsoft, Sun, IBM, and Oracle to work on the evolution of cloudlets (micro data centers) for latency-sensitive computing [7].

Edge Computing vs. Cloud Computing

Cloud computing is the transmission of on-demand computational resources over the Internet. It facilitates users with a wide range of services and virtually unlimited available resources. In traditional cloud architectures, all data from physical assets is transported to the cloud for storage and advanced analysis. Since cloud has more computing power compared to the devices at the network edge, shifting computation-intensive tasks to the core cloud computing platform is an effective approach for data processing. However, transmission of massive loads of data over a network puts immense load on network resources. Further, it is also unable to meet the requirements of location awareness, low latency, and mobility support. Cloud computing has been a phenomenal service provider where delay-tolerant applications can be served with ease. However, in some cases, it is essential to process data near its source. For example, in safety-critical applications including ITSs, healthcare, and so on, a delay of even milliseconds can be injurious.

Edge computing, which supports data computation in proximity of the data sources, is an emerging computing paradigm that generalizes and extends the content delivery networking (CDN) concept by leveraging cloud computing infrastructure. Computation in proximity addresses many challenges that are faced while running data-centric workloads on the cloud:

- It reduces the data flow between the data center and the central cloud.
- It uses the benefits of the central cloud to retain sensitive data on premises.
- It reduces the latency involved in dealing with central cloud platforms [8].

Additionally, bandwidth utilization could be tremendously reduced by processing the larger chunks of data at the edge rather than redirecting them to the cloud.

The devices deployed at the edge of the network request information and services from the cloud platform. Additionally, they also handle numerous computational tasks in terms of storage, caching, processing, and load balancing. Due to the ability of this technology to bring bandwidth-demanding data and latency-sensitive applications closer to the user, there has been a drastic increase in the use of this technology in data-driven and intelligent applications.

Shifting a lot of computational effort from the centralized cloud to the network's edge reduces the latency and local processing of data. Edge clouds are not going to replace traditional clouds, as the amount of processing power and storage they have is far below those of traditional clouds. Instead, the aim is to complement the traditional cloud data centers by running some delay-sensitive applications at the edge of the network [6]. The contrast of edge computing with respect to cloud computing is shown in Fig. 2.

Advent of Cyber-Attacks in ITSs

According to the IBM X-Force Research report "Security Trends in the Transportation Industry," vehicles are a high-value target of cyber-criminals [9]. Another report, "Cyber Security and Intelligent Mobility" by Transport Systems Catapult, also says that the world of mobility is undergoing significant change [10]. The rapidly changing mobility landscape is likely to introduce more cyber-attacks, more often, and potentially with more severe consequences.

Last year, security researchers in the United States discovered a malicious cyberattack on a vehicle equipped with a "U-connect" in-vehicle connectivity system. It enabled hackers to remotely control a Jeep and drive it off the highway. The electrical component units (ECUs) used in these vehicles are interconnected via an internal network. Hence, an adversary can easily take control of safety-critical components such as brakes or engine if a vehicle's peripheral ECU, Bluetooth, or infotainment system is compromised. Since the technology continues to evolve rapidly, the consequences of a cyberattack on a moving vehicle could potentially be fatal [1].

Due to the ever increasing complexity of transportation systems and the evolving nature of autonomous software, traditional safety methods are failing. The protection of this infrastructure is necessary to ensure that it remains open, opera-

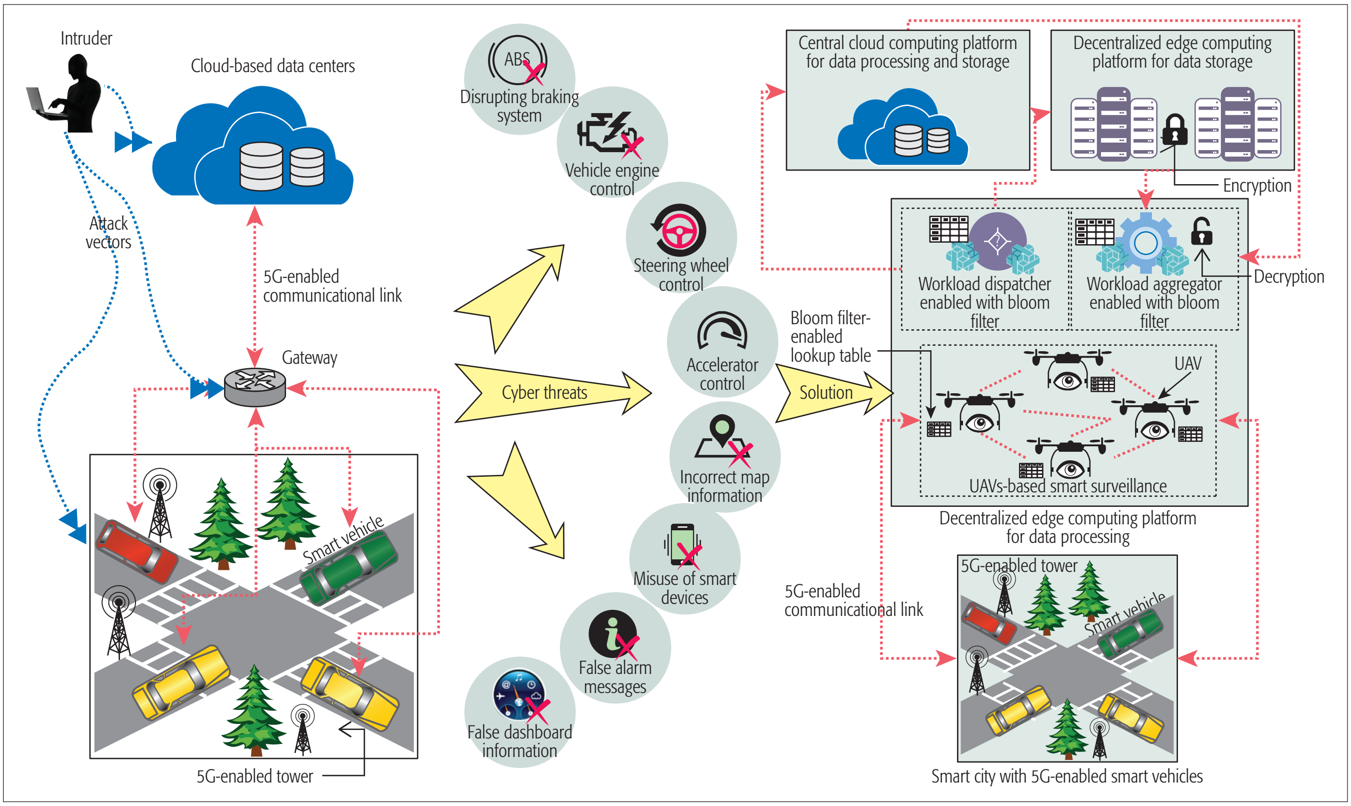

Intruder
Cloud-based data centers
Attack vectors
5G-enabled communicational link
Gateway
Smart vehicle
5G-enabled tower
ABS
Disrupting braking system
Vehicle engine control
Steering wheel control
Accelerator control
Incorrect map information
Misuse of smart devices
False alarm messages
False dashboard information
Cyber threats
Solution
Central cloud computing platform for data processing and storage
Decentralized edge computing platform for data storage
Encryption
Decryption
Workload dispatcher enabled with bloom filter
Workload aggregator enabled with bloom filter
Bloom filter-enabled lookup table
UAV
UAVs-based smart surveillance
Decentralized edge computing platform for data processing
5G-enabled communicational link
5G-enabled tower
Smart vehicle
Smart city with 5G-enabled smart vehicles

FIGURE 3. Need for secure ITS in 5G enabled smart city environment.

tional, and above all safe for the billions of people who depend on it.

Motivation

ITS is a main driving force for the expansion of smart cities. Due to the recent proliferation and deployment of heterogeneous technologies, security and privacy of smart vehicles are the most prominent concerns. We are fast approaching an era where vehicles and networks can seamlessly talk to each other and achieve complete interoperability — everything connected to everything. However, with the upsurge of cyberattacks against real-time systems and their increasing sophistication, a sustainable, efficient, and secure environment is a primary concern [9]. Since cyber-threats in ITS can cause long-term sociological and economic consequences, safety of current transportation systems cannot be ignored. To provide resilience to this critical infrastructure against cyber threats that could have a debilitating impact on security and economic stability, smart technologies can only be helpful.

Because a transportation system utilizes a wide variety of data, traditional data processing technologies are proving to be inefficient in processing rapid streams of data. Transmission of enormous data over a network incurs massive load on network resources. A highly responsive distributed environment is therefore required for more proactive and effective responses. Edge computing is one such technology that supports data processing at the network's periphery [6]. In this architecture, time-critical data can be processed in proximity to the data source, whereas less critical data is redirected to the central cloud for analytics and storage.

The deployment of smart ITS has several requirements like resource dynamicity to support on-the move computation, service dynamicity to fulfill the diverse needs of service requests, and traffic dynamicity to provide response to fluctuating traffic patterns. Further, smart management of failure and service windows, secure interoperability, edge processing, and at-scale deployment is required to minimize the impact of downtime, and provide more intelligent communication and processing power to the computational nodes. Due to the unique characteristics of ITSs like mobility, communication/processing capabilities, and autonomous operability, it can be tuned with UAVs, which can monitor the traffic in real time to detect vulnerable situations if any [11]. The presence of limited energy, storage capacity, and computational power in UAVs makes them unsuitable to make real-time decisions. Since data handling at the edge would result in shorter response times, more efficient processing, and less load on the network, the integration of a UAV-enabled ITS with the edge computing environment can solve this problem to the maximum extent. Thus, the need for secure ITS in 5G-enabled smart city environment along with a secure solution are portrayed in Fig. 3.

Contributions

The article makes the following contributions:

- We discuss the role of ITS surveillance in the 5G-enabled smart city along with the role of edge computing in providing a flexible and scalable computing environment for fast decision making.
- We design a hierarchical edge computing architecture by bringing the computing

Edge services running on edge servers can be deployed on 5G-enabled base stations to support the roadside functionality seamlessly. These edge services in turn analyze the messages received from the vehicles, and then relay (with extremely low latency) hazardous warning signals and other latency-sensitive messages to other vehicles in the proximity.

resources close to smart vehicles so that network congestion can be alleviated, and the end-to-end (E2E) delay between computing resources and vehicles is minimized. A triple-Bloom-filter-based [12] fast service processing platform is used to host the real-time data coming from different vehicles:
  - *In UAVs:* To validate whether data is coming from authenticated vehicles or not
  - *In Dispatcher:* To validate the authenticity of the data coming from UAVs and then to schedule the edge processing tasks
  - *In Aggregator:* In initial phase of decryption, to match the primary key that is generated by the decentralized edge computing platform during encryption.
- We demonstrate the promising benefits of integrating UAVs with connected and autonomous vehicles for cyber-threat detection in ITSs through simulated results.

Various Aspects Related to ITSs

Several aspects related to ITSs are discussed in the following subsections.

Transportation Challenges in the Era of 5G

Transportation systems are increasingly stressed all around the world. The scenario we expect over the next few years would provide a much safer driving experience and save countless lives. This influence has turned the design of 5G mobile network architecture into one of the pillars of the 2020 society [7]. To allow vehicles to exchange information and "talk" to each other, communication requires low latency, high reliability, and the ability to communicate out of range of the network.

Recent advances in technology aim to connect vehicles to all sensor-enabled objects. The need to share data anywhere, anytime by anyone and anything puts challenging functional and performance requirements on network platforms and devices. In order to assist drivers with safe and secure information, 5G architecture should support and coexist with trust-aware systems [8].

For a secure travel infrastructure, vehicles need to share the data in real time without any delay. Any sort of interruption in the network decreases the efficiency of transportation systems. The ever growing demands of transportation networks such as:
- Instant identification of threats and potential attacks
- Ultra-high latency
- Secure localization
- Congestion control

pose multiple challenges to research fraternities. Since the demand for ITS is intensifying, it is essential to provide efficient, reliable, and in-time communications to vehicles and their embedded sensors.

The Role of Edge Computing in ITSs

Smart transportation aims to resolve the fundamental problems witnessed by city dwellers with respect to transportation. These problems range from degraded traffic control systems and poor road conditions to inadequate parking places, public transportation facilities, and road safety.

Since the number of connected vehicles is rapidly growing, continuous monitoring is required to enhance the safety, efficiency, and convenience of the transportation sector. Any autonomous vehicle relying on the cloud for data would crash because of the latency associated with transmitting data between the vehicle and the cloud. From a pure latency and bandwidth perspective, it is impossible to transmit data from millions of vehicles back to a data center for decision processing. Therefore, speedy computation and faster decision making are required to deliver shorter response times, dynamic processing, and reduced dependence on the network. Edge computing extends the connected vehicle's cloud into the highly distributed network edges, which enables data and services to be available close to the vehicles [5].

The decentralization of cloud computing infrastructure to the edge delivers numerous advantages to the ITS: low latency, user privacy, and pooling of resources at different layers [8]. Edge services running on edge servers can be deployed on 5G-enabled base stations to support the roadside functionality seamlessly. These edge services in turn analyze the messages received from the vehicles, and then relay (with extremely low latency) hazardous warning signals and other latency-sensitive messages to other vehicles in proximity. This renders the approaching vehicles able to receive the messages within milliseconds, thereby allowing the drivers to instantly take the requisite action.

There can be several applications where edge computing can be deployed to make transportation more smarter and efficient. For instance, a traffic control system can be fully realized by gathering real-time data using cameras and sensors deployed along roadsides. These sensors in turn can recognize approaching entities in the form of pedestrians and vehicles. Additionally, the deployed sensors are also capable of measuring the relative distances and speeds of the approaching entities. On the basis of this sensed data, effective traffic control signals can be rerouted to the vehicles by relaying appropriate signals through a smart traffic light system. Along similar lines, a smart parking system can be modeled by gathering user context information and evaluating the available parking lots in and around the proximity of users by leveraging the benefits of the edge network. All such applications of an edge-enabled ITS indicates that edge computing is an ideal platform for ITS security.

The major objective of the edge-enabled ITS is to integrate new communication technologies in transportation systems so that traffic efficiency, environmental quality, time conservation, and safety and comfort of drivers, pedestrians, and other traffic groups can be provided in an efficient and timely manner. This transformative technology is posing new challenges and risks in addi-

Contributors	Year	Contributions	Evaluation Conducted	Experimental Environment
Yang *et al.* [13]	2012	A new vehicle detection approach by analyzing airborne video captured from a Quad-rotor UAV	Vehicle recognition (both static and moving) from an UAV based surveillance system for sparse highways	Quad rotor helicopter equipped with a Sony camera (resolution of 720 × 576) as the UAV platform
Liu *et al.* [14]	2013	A UAV allocation method for traffic surveillance in a sparse road network was proposed. Here a simulated annealing algorithm was used for without maximum flight distance constraint, whereas k-means algorithm was used with maximum flight distance constraint	Convergence of the shortest UAV cruise distance, accumulative frequency analysis of road, and comparison of total cruise distances in different UAV surveillance areas	Analysis on Korla-Kuqa expressway of Xinjiang, China's western regions and its road network; to compute the shortest UAV cruise routes, the simulated annealing algorithm was implemented in the MATLAB environment.
Liu *et al.* [11]	2014	A Pareto-algorithm-based multi-objective optimization model for UAV route planning and surveillance of road segments was proposed to minimize the cruise distance and the number of UAVs	UAV flight experiment was conducted to test UAV route planning effect and the effect of different road segments on UAV route planning was analyzed	UAV flight experiment using MD 4-1000 UAV was conducted on Cao'an road, Shanghai, China and UAV route planning optimization in MATLAB
Zhou *et al.* [15]	2015	A fast homography-based scheme was developed for efficient road detection and tracking framework in UAV videos; here, a graph-cut-based detection approach was used to accurately extract a specified road region	Experiments on UAV videos (real road scenes+ videos downloaded from the Internet) were conducted to check the real-road detection accuracy of the proposed scheme	To detect the drift error and zigzag contour problems, experiments were performed on image sequences acquired using UAV that was flown in different sessions near their center in Australia
Kingston *et al.* [4]	2016	An intermediate level of automation through a set of parameterized tasks for search and surveillance of patterns through UAVs; here, dynamics of UAV, sensor footprint geometry, and sensor imagery quality was considered to assist the operations	Several automated tasks such as point inspect, line search, area search, spiral search and sector search were used to plan the waypoint-based tasks; each task has certain parameters that provide a level of automation to UAVs	All the implementation details are addressed by considering Dubins vehicle dynamics, sensor footprints and ground sample distance of the sensored image
Menouar *et al.* [2]	2017	A complete description of possible ITS solutions for deploying UAVs and exploration of challenges related to UAV-enabled ITS for smart cities	Joint deployment of RSUs, UAVs, and recharge stations in ITS scenarios for intricate optimization	To optimize the deployment of UAVs in ITS scenarios simulations were conducted in MATLAB

TABLE 1. Analysis of UAV-based approaches for security in transportation systems.

tion to benefits, which include security due to the increase in the number of cyberattack vectors, resource management due to the presence of computing and storage resources, interoperability to collaborate with each other, mobility support for fast process migration, network accessibility regardless of their deployment, process migration on the basis of service demand, and so on.

UAVs in Smart Transportation

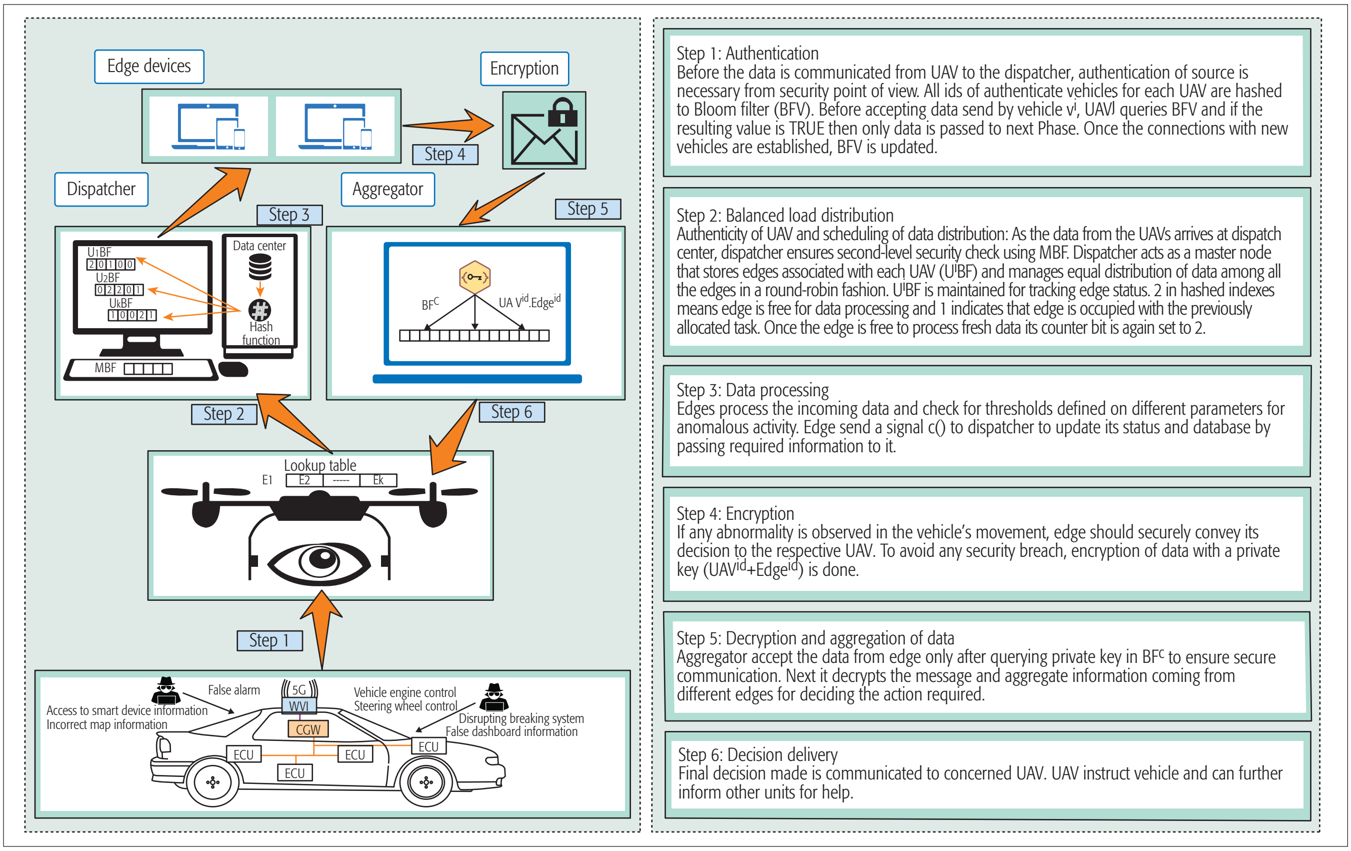
Security and privacy pose serious challenges to 5G-enabled ITS within a smart city environment. One particular challenge stems from the privacy and efficient processing of sensitive information from vehicles. UAVs are generally seen as an "eye-in-the-sky" solution to collect enormous trajectory data from road arterials. In particular, it can provide vision as a service (VaaS) [15]. However, they need a platform that can handle their mobility, provide security, and perform real-time data analysis. Edge devices are one such solution that can provide continuous support to the UAVs. Wireless communication by UAVs aids them to communicate with vehicles in proximity to better enforce road safety and support traffic efficiency.

UAVs have been designed to provide multiple functionalities such as autonomous operation at varying altitudes, plan preparation for achieving mission goals (locating, identifying, tracking, and monitoring different vehicle types), and construction of internal representations. UAVs have a wide range of applications in transportation operations like tracking vehicle movements, traffic management, emergency vehicle guidance, incident response, pollution monitoring, and efficient utilization of parking lots, all of which contribute greatly to the development of any smart city. Dynamic coordination and data routing UAVs may act as relaying nodes or traffic monitoring tools in ITS applications for smart cities. Several schemes have emerged to track moving objects and analyze traffic for the security of transportation systems. Some of them are listed in Table 1.

Proposed Technique

This article proposes a novel load balancing and authentication mechanism through Bloom filters [12]. Consider a smart city with n UAVs where $S_{UAV} = \{UAV_1, UAV_2, UAV_3, ..., UAV_n\}$ denote the set of UAVs and m vehicles (i.e., $S_V = \{V_1, V_2, ..., V_m\}$) where $m >> n$. It is assumed that there are k edges; $S_E = \{E_1, E_2, E_3, ..., E_k\}$ that act as data processing and decision making centers for the data received from the UAVs. Each UAV hovering over smart vehicles takes the data delivered by the vehicles within its vicinity. Data fetched by the respective UAV for all the vehicles within its domain is delivered to the dispatcher D, which acts as a workload distribution center and dispatches the data to the edge with minimum load at time t, where t denotes the time when the data is dispatched. The efficiency of the network will be enhanced if it is ensured that data processing is balanced at the edge, that is, every component of the network is playing equal role in the network.

After the data has been analyzed and a decision regarding the UAVs movement has been made by the respective edge, the decision is



Step 1: Authentication
Before the data is communicated from UAV to the dispatcher, authentication of source is necessary from security point of view. All ids of authenticate vehicles for each UAV are hashed to Bloom filter (BFV). Before accepting data send by vehicle v^i, UAV^j queries BFV and if the resulting value is TRUE then only data is passed to next Phase. Once the connections with new vehicles are established, BFV is updated.

Step 2: Balanced load distribution
Authenticity of UAV and scheduling of data distribution: As the data from the UAVs arrives at dispatch center, dispatcher ensures second-level security check using MBF. Dispatcher acts as a master node that stores edges associated with each UAV (U^iBF) and manages equal distribution of data among all the edges in a round-robin fashion. U^iBF is maintained for tracking edge status. 2 in hashed indexes means edge is free for data processing and 1 indicates that edge is occupied with the previously allocated task. Once the edge is free to process fresh data its counter bit is again set to 2.

Step 3: Data processing
Edges process the incoming data and check for thresholds defined on different parameters for anomalous activity. Edge send a signal c() to dispatcher to update its status and database by passing required information to it.

Step 4: Encryption
If any abnormality is observed in the vehicle's movement, edge should securely convey its decision to the respective UAV. To avoid any security breach, encryption of data with a private key (UAV^{id}+$Edge^{id}$) is done.

Step 5: Decryption and aggregation of data
Aggregator accept the data from edge only after querying private key in BF^c to ensure secure communication. Next it decrypts the message and aggregate information coming from different edges for deciding the action required.

Step 6: Decision delivery
Final decision made is communicated to concerned UAV. UAV instruct vehicle and can further inform other units for help.

FIGURE 4. Proposed model.

communicated to the UAVs through the aggregator, which ensures that the edge's decision is not hacked or leaked to any third party. The proposed model has been depicted in Fig. 4. Important issues that need major consideration in this scenario are:

- Processing at the UAVs should be minimum since it has limited battery.
- Load should be balanced among all edges.
- Security measures should be incorporated to ensure that data is communicated securely from:
  –UAVs to the dispatcher
  –Dispatcher to the edge
  –Edge to the aggregator

Optimization objective (Υ^O): To propose a framework that includes UAVs, dispatcher (D), edge nodes (E_i), and aggregator (A) to maximize the processing capabilities (Pc), minimize delay (De) for proactive decision making, and maximize the security (Se) of the 5G enabled ITS framework at different levels.

$$\Upsilon^O(Se^+,De^-)=\left[\sum_{i=1}^{n}\frac{(Se_{UAV_i})(Pc_{UAV_i})}{(Ee_{UAV_i})(De_{UAV_i})}\right]+\left[\frac{(Se_D)(Pc_D)}{(WT_D)}\right]+\left[(Se_A)(Pc_A)\right]+\left[\forall_{E_i\in SE}\frac{Av_E}{(De_E)}\right] \qquad (1)$$

where WT_D indicates the average waiting time for scheduling edge processing tasks and Av_E denotes the average mean time between failure (MTBF) for the reliability of edge nodes.

For secure communication and efficient load distribution among edges, the dispatcher uses probabilistic data structures called Bbloom filters. One Bloom filter is used to authenticate that the data received is from the trusted UAV, and each edge connected to the dispatcher maintains a Bloom filter with a special bit called a counter bit. Based on the value of the counter bit of the corresponding edge, the dispatcher distributes the load among the available edges. The Bloom filter (*BF*), a space-efficient probabilistic data structure, consists of an array of *m* bits. These bits are represented individually using $BF[i]\,|\;1 < i < m$, wherein their initial values are set to 0. In order to define the elements in the set, BF utilizes *k* independent hash functions (H_i), wherein their values (h_i) range between 1 and *m* (i.e., $({}_{i=1}^{k}(h_i(.) \leftarrow H_i)) \in \{1, m\}$). Here, it is has assumed that the considered hash functions independently map every element in the universe to a random number uniformly over the defined range. For all the elements $x \in S$, the corresponding bits ${}_{i=1}^{k}(BF[h_i])$ are instantiated to 1. Given an item *y*, its membership is checked by examining the *BF*[] to find whether the bits at positions ${}_{i=1}^{k}h_i()$ are set to 1. If all hash indices are set to 1, *y* is considered to be part of *S*; otherwise, *y* is definitely not a member of *S*: $(If(\forall_{i=1}^{k}h_i(y){=}{=}1)?(y \in S):(y \notin S))$.

As the data from UAVs arrives at the dispatch center, the dispatcher ensures that data has been received from a trusted UAV by maintaining a Bloom filter *MBF*. For every input ${}_{i=1}^{k}(MBF[h_i]{=}\;1) \Leftarrow (H_i(S_{UAV}))$ and if the id of UAV_i matches that of *MFB*[] (i.e., all bits are set to 1), the data is accepted for dispatch. Here, the dispatcher is acting as a master node, which efficiently identifies the load conditions of the edges with minimum computa-

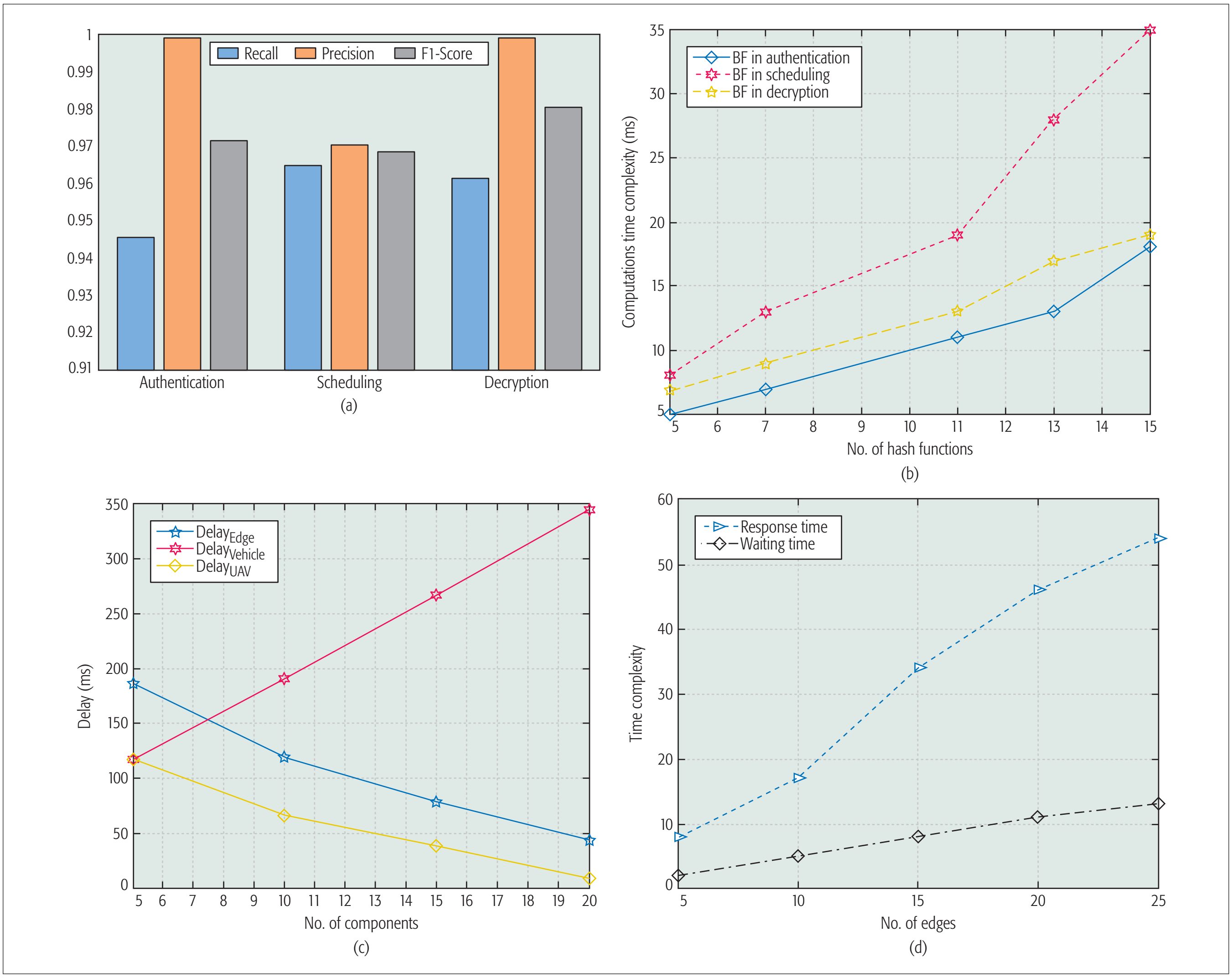


FIGURE 5. Performance evaluation: a) accuracy of Bloom filter during authentication, scheduling, and decryption; b) computational complexity of Bloom filter() vs. number of hash functions; c) time delay (ms) vs. number of components; d) evaluation of scheduling of data distribution.

tion and much less storage space. ζ denotes the duplex communication between the edge and the dispatcher. It stores edge associated with each *UAV* in a counting Bloom filter $BF_{UAV_i}[]$ with counter value $Max = 2$ for load balancing. Initially, when all edges are free, BF_{UAV_i} sets all hash indices to *Max*. The dispatcher distributes the data equally among all the edges in a round-robin fashion after a fixed time quantum *t*. After one distribution cycle, if the edge E_i is busy processing the data it received in the previous cycle, it communicates a signal $\chi(1)$ to dispatcher indicating that it is busy and cannot take more load; bits corresponding to that E_i are set to 1 in $BF_{UAV_i}[]$. Once the data has been processed by the edge (i.e., it is free to process fresh data), it will send a $\chi(2)$ signal to the dispatcher and its counter bit is again set to 2 in $BF_{UAV_i}[]$.

$$\zeta \Rightarrow \begin{cases} (Ei \Rightarrow D) = \begin{cases} {}_{j=1}^{k}(BF_{UAVi}[h_j] \leftarrow 2) & if(\chi(2)) \\ {}_{j=1}^{k}(BF_{UAVi}[h_j] \leftarrow 1) & if(\chi(1)) \end{cases} \\ (D \Rightarrow Ei) = \begin{cases} \forall(Ei \in S_E)(D(data)^t) & if(\forall^i(BF[h_i](E_i)) == 2) \\ wait & if(\forall^i(BF[h_i](E_i)) == 1) \end{cases} \end{cases} \quad (2)$$

If any edge (E_i) finds that some of the parameters of the particular vehicle are abnormal, that is, they have crossed the defined threshold, or, in other words, it is suspected that the movement of a particular vehicle is anomalous, the alarm signal is immediately transmitted to the concerned local authorities and aggregator (*A*) instantaneously directs the UAV to tract the images or activities of the anomalous vehicle.

Since this decision (D_E) is the most important from the surveillance point of view, it should be communicated securely because if an intruder intercepts the message, it may mislead the UAV to track some other vehicle. To avoid this situation a secure cryptographic mechanism C is provided. A private key (*pk*),which is combination of UAV_{id} and $edge_{id}$ is broadcasted along with the message (M_e) to the aggregator (*A*). This encrypted information is first decoded and is then passed to the concerned UAV. For decryption process, a Bloom of private keys BF_{pk} is maintained. If pk_i associated with message matches with the Bloom of them, only the information in the message is processed and decoded. Next, the message is decoded, and the

The proposed framework uses Bloom-filter-based security protocol during collection of the data at every stage. A novel Bloom-filter-based scheduling technique for load balancing is used to distribute the data to edges in a manner that minimizes the computational effort.

original decision(D_E) is passed to the concerned UAV_i for appropriate action.

$$\mathsf{C} \Rightarrow \begin{cases} (\text{Encryption})\left\{(M_e, pk_e) \leftarrow \underline{\triangleright}(D_E, (UAV_i + E_j))\right. \\ (\text{Decryption})\begin{cases} DE \leftarrow \underline{\triangleleft}(M_e, pk_e) \;\; if \forall (h_i)(BF_{pk}(pk_e) == 1) \\ Send(D_E, UAV_i) \end{cases} \end{cases} \quad (3)$$

To ensure flawless output, especially for real-time data analytics where decisions have to be made on the fly, load distribution in dynamic networks should be quite fast and efficient. Usage of a Bloom filter for load distribution reduces the calculation complexity as it reduces the time required to calculate the load at every edge and further reduces the space requirements as it is a memory-efficient membership query data structure.

Observation and Analysis

The proposed approach aims at improving the surveillance and security of vehicles using UAVs where data processing and decision making is done at edges. The proposed framework uses a Bloom-filter-based security protocol during collection of the data at every stage. A novel Bloom-filter-based scheduling technique for load balancing is used to distribute the data to edges in a manner that minimizes the computational effort. The detailed performance evaluation of the proposed framework is provided in this section. To authenticate the security features of the proposed model at various levels, analysis has been performed through network simulations. All the experiments have been performed on $i7 - 3612QM$ CPU @ 2.10 GHz with 8 GB of RAM. To maintain the uniformity in the results, the *CityHash* 64-bit library is used to calculate two hash functions in double hashing. For simulation of the proposed framework, MATLAB is used. During simulations, a four-layer setup is designed where the first layer indicates the vehicles that are primary sources of data transmission, the second layer includes UAVs that act as data forwarding nodes, the third layer act as a dispatcher that performs security check of data source and delivers the data to next the layer, and the final layer includes processing units (i.e., edges). Various parameters have been designed for evaluating the performance of the proposed approach.

Figure 5a depicts the accuracy parameters in scheduling, authentication, and decryption processes. To evaluate the accuracy of the proposed approach, a number of security attacks have been simulated at different layers. A vulnerable environment of around 100 attacks is considered to study the effect of Bloom-based security.

As mentioned earlier, the proposed model uses a Bloom filter at four different layers; Fig. 5b shows the change in computational time complexity with the change in number of hash functions used at different layers.

Delay in decision making affects the number of components at each layer. Figure 5c indicates the effect of delay on various components at each layer. Delay is reduced by increasing the number of processing units, that is, edges and transmitting units (UAVs). As the number of vehicles increases, the delay in decision making is prolonged.

Figure 5d shows the effectiveness of scheduling task on average response time and average waiting time where the effect on scheduling parameters is evaluated with the change in the number of edges.

Concluding Remarks

With the quick growth in smart vehicles and smart cities, smart technology, including the Internet of Things, MEC, 5G, and so on, is evolving rapidly; but all these new paradigms are under serious threat from potential hackers. The consequences of cyberattack on a moving vehicle could be fatal. The current solutions for ITSs have slanted the performance due to high demand for data on the move. These network formations are continuously under the threat of sudden failures. These failures in networks in turn can severely hamper the performance and reduce its functionality. To efficiently capture the data on the fly, analyze it, and make decisions at very high data rates (typically on the order of gigabits per second) with low latency, 5G wireless communications is essential. In this article, a novel model for surveillance in ITS has been proposed. Here, real-time analytics and application logic are run at various levels: UAVs, which capture the data from vehicles and act as data providers; aggregators, which provide secure load transfer to edges; edges, which perform data analytics; and a secure dispatcher. Using a triple Bloom filter not only decreases the computational cost; it also decreases the space requirement manifold. Such a model can ensure public surveillance of vehicles and track abnormal movements in real time.

Acknowledgment

The first and second authors would like to acknowledge the financial support given to them by the Department of Electronics and Information Technology (DeitY) under the Ministry of Communications and IT, Government of India, to complete doctoral studies.

References

[1] A. S. Elmaghraby and M. M. Losavio, "Cyber Security Challenges in Smart Cities: Safety, Security and Privacy," *J. Advanced Research*, vol. 5, no. 4, 2014, pp. 491–97.

[2] H. Menouar *et al.*, "UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 3, Mar. 2017, pp. 22–28.

[3] "Adjusting the Lens on Economic Crime-Preparation Brings Opportunity Back into Focus, " PwC, 2016; https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf, accessed Sept. 2017.

[4] D. Kingston, S. Rasmussen, and L. Humphrey, "Automated UAV Tasks for Search and Surveillance," *IEEE Conf. Control Applications*, 2016, pp. 1–8.

[5] B. P. Rimal, D. P. Van, and M. Maier, "Mobile Edge Computing Empowered Fiber-Wireless Access Networks in the 5G Era," *IEEE Commun. Mag.*, vol. 55, no. 2, Feb. 2017, pp. 192–200.

[6] M. Satyanarayanan, "The Emergence of Edge Computing," *Computer*, vol. 50, no. 1, 2017, pp. 30–39.

[7] "Building 5G End-to-end Technology-Considerations for 2020 and Beyond," Global Data, 2017; https://s3.amazonaws.com/assets.fiercemarkets.net/public/webinars/intel/2017+February/GlobalData-5G+white+paper-A-SD.pdf, accessed July 2017.

[8] Y. C. Hu *et al.*, "Mobile Edge Computing — A Key Technology Towards 5G," ETSI White Paper, vol. 11, 2015.

[9] "IBM X-Force Threat Intelligence, IBM Security, Mar. 2017; https://assets.documentcloud.org/documents/3527813/IBM-XForce-Index-2017-FINAL.pdf, accessed May 2017.

[10] 2016, November, "Cyber Security and Intelligent Mobility," Catapult Transport Systems, Nov. 2016; https://s3-eu-west-1.amazonaws.com/media.ts.catapult/wp-content/uploads/2016/11/24133246/3416 Cyber-Security Report Final-1.pdf, accessed July 2017.

[11] X.-F. Liu *et al.*, "An Optimization Model of UAV Route Planning for Road Segment Surveillance," *J. Central South Univ.*, vol. 21, no. 6, 2014, pp. 2501–10.

[12] S. Tarkoma, C. E. Rothenberg, and E. Lagerspetz, "Theory and Practice of Bloom Filters for Distributed Systems," *IEEE Commun. Surveys & Tutorials*, vol. 14, no. 1, 2012, pp. 131–55.

[13] Y. Yang *et al.*, "Vehicle Detection Methods from an Unmanned Aerial Vehicle Platform," *IEEE Int'l. Conf. Vehic. Electronics and Safety*, 2012, pp. 411–15.

[14] X.-F. Liu *et al.*, "A UAV Allocation Method for Traffic Surveillance in Sparse Road Network," *J. Highway and Transportation Research and Development* (English ed.), vol. 7, no. 2, 2013, pp. 81–87.

[15] H. Zhou *et al.*, "Efficient Road Detection and Tracking for Unmanned Aerial Vehicle," *IEEE Trans. Intelligent Transportation Systems*, vol. 16, no. 1, 2015, pp. 297–309.

Biographies

Sahil Garg [S'16] (garg.sahil1990@gmail.com) received his B.Tech degree from Maharishi Markandeshwar University, Mullana, Ambala, India, in 2012, and his M.Tech degree from Punjab Technical University, Jalandhar, India, in 2014, both in computer science and engineering. He is currently working toward a Ph.D. degree in computer science and engineering from Thapar University, Patiala, India. His research interests include machine learning, big data analytics, knowledge discovery, game theory, and vehicular ad hoc networks.

Amritpal Singh [S'17] (amritpal.singh203@gmail.com) received his M.E. degree from Thapar University with a minor in big data and advanced data structures in 2013. He has been working as a research scholar with the Computer Science Department at Thapar University since January 2015. He has served both industry and academia. His research interest includes probabilistic data structures, machine learning, and big data.

Shalini Batra [M'17] (sbatra@thapar.edu) received her Ph.D. degree in computer science and engineering from Thapar University in 2012. She is currently working as an associate professor with the Department of Computer Science and Engineering, Thapar University. She has guided many research scholars leading to Ph.D.s and M.E.s/M.Techs. She has authored more than 60 research papers published in various conferences and journals. Her research interests include machine learning, web semantics, big data analytics, and vehicular ad hoc networks.

Neeraj Kumar [M'16, SM'17] (neeraj.kumar@thapar.edu) is an associate professor in the Department of Computer Science and Engineering, Thapar University. He received his M.Tech. from Kurukshetra University, Haryana, followed by his Ph.D. from SMVD University, Katra (J&K). He was a postdoctoral research fellow at Coventry University, United Kingdom. He has more than 150 research papers in leading journals and conferences of repute. He is an Associate Editor of *IJCS*, Wiley, *JNCA*, Elsevier, and *Security & Communication*, Wiley.

Laurence T. Yang [M'97, SM'15] (ltyang@gmail.com) received his B.E. degree in computer science and technology from Tsinghua University, China, and his Ph.D. degree in computer science from the University of Victoria, Canada. He is currently a professor with the Department of Computer Science, St. Francis Xavier University, Canada. He has authored over 220 papers in various refereed journals (around 40 percent in top IEEE/ACM transactions and journals, others mostly in Elsevier, Springer, and Wiley journals). His research has been supported by the National Sciences and Engineering Research Council and the Canada Foundation for Innovation. His research interests include parallel and distributed computing, embedded and ubiquitous or pervasive computing, and big data.