A Research Paper on Vehicular Ad-Hoc Network

Article *in* Journal of Scientific Research and Development · December 2018

CITATION
1

READS
1,600

3 authors, including:

Kundalakesi Mathivanan
Sri Krishna College of Arts and Science
11 PUBLICATIONS **23** CITATIONS

SEE PROFILE

A Research Paper on Vehicular Ad-Hoc Network

M. Kundalakesi[1] S. Meghala[2] S. VidhiyaLakshmi[3]
[1,2,3]Department of Computer Application & MSc SS
[1,2,3]Sri Krishna Arts and Science College, India

Abstract— The Vehicular Ad-Hoc Network, or VANET, is a technology that uses and moves cars as nodes in a network to create a mobile network. VANET is a special form of MANET (mobile ad hoc network). VANET makes every involving car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. Mechanism used to protect privacy requires two key ingredients: 1. a precise definition of privacy that reflects citizens' concern and perceptions, and 2. an upstanding of the type of attacks in VANETs. VANET introduces more challenges aspects as compare to MANET because of high mobility of nodes and fast topology changes in VANET. It covers applications, privacy and characteristics prevailing in VANETs.

Key words: MANET, Privacy, Challenges, Applications

I. INTRODUCTION

As per the report of World Health Organization (WHO) statistics, more than 1.3 million people worldwide are likely to be killed each year out of road accidents. According to an online article printed in Deutsche Welle [4] by Murali Krishnan dated 29.04.2010, "India's record in deaths has touched a new low, as toll rose to at least 14 deaths per hour in 2009 against 13 the previous year". While trucks/lorries and two-wheelers were blamable for over 40% deaths, the rush during afternoon and evening hours were the most fatal phases.[4,5]. Also, as per another article of WHO India leads the world in road deaths. Common problems to tackle with are the "Miles of Traffic Jam" on highway & the "Search for best Parking Lot" in an unknown city.[3]

Increasing number of vehicles on the road has brought focus on improving road safety as well as in-vehicle entertainment. So we are witnessing a rise in development of new applications and services for vehicular environments. Some common examples include applications for accident avoidance, safety and traffic secured monitoring, multimedia streaming, data gathering for smart cities in synergy with wireless sensor networks [2], vehicle-to-vehicle communication (V2V), etc. VANET has raised as a recent technology that can support such emerging vehicular applications.

According to configuration of network, VANET can be divided into three streams namely: Wireless Wide Area Network (WWAN), Hybrid Wireless Architecture, and Ad Hoc V2V communication. In the WWAN, the access point of the cellular gateway are fixed, which permit the direct communication between the vehicle and the access point. The Hybrid wireless Architecture uses WWAN access points at some points in the network, while the communication in between those terminal points in the Hybrid Wireless Architecture are achieved with the use of Ad Hoc communications. The third category is the Ad Hoc Vehicle-to-Vehicle communication; this don't need any fixed access point for the vehicles to communicate. Vehicles are designed with their own wireless network card and the setting up of an Ad Hoc network can be actualized for each vehicle. VANET is a subsystem of MANET, VANET communicates with the MANETlike technology with the equipment nearby along the road side, and also to communicate between vehicles. Their characteristics are different from that of other networks [5]-[6]. Unavailability of road information can create a possibility of accurately stating the position of the vehicle at that time. The vehicle is an entity in VANET and the nodes are limited to a particular type of topology while in motion which is the road topology. The nodes can provide power for data processing and information transmission to sustain the functioning of the node. [7]-[8]

VANET inculcate sufficient potential in vehicles to transmit warnings about environmental hazards, traffic conditions and regional information to other vehicles. The major intend of VANETs is to absolute the user's choice on the road and build their drive safe and snug. Vehicles move at a high speed that it is harder to maintain a seamless handoff and a perfect connectivity to the Internet.

II. VEHICULAR AD-HOC NETWORK (VANET):

VANETuses cars as a mobile node to create a mobile network [23]. Vehicles act as a mobile node with the corresponding network. The basic aim of VANET is to enhance the safety on our roads and road users, comfort of passengers, and also aid the communication between vehicles and roadside equipment. The VANET communication medium is installed on each node (vehicle) [27]. As shown in Figure 1, each vehicle has its own communication wireless network card which allows ease of communication flow between vehicles and roadside units.

Figure 2 demonstratesthe different domains that exist in VANET. The Mobile Domain consists of (Vehicle and Mobile Devices) such as PDA, Smart Phones, and Laptop etc. The Generic Domain contains of (Internet Infrastructure and Private Infrastructure) such as nodes and servers. While the Infrastructure Domain consists of (Road Infrastructure or Units and the Central Infrastructure) such as the Road Side Units that link with the vehicle along the road, and the management center that communicates with the internet. The Mobile Domain communicates with this unique Infrastructure Domain and the Infrastructure Domain communicates with the Generic Domain and data flows between the different domain to provide effective and efficient use of the road by the peoples. Hence the communication is provided in two different way in VANET, there are some fixed node that act as a roadside unit or equipment which enables the ease of VANET to serve as a gateway to the internet and also in accessing geographical data [25]-[26]. Each node in the VANET doesn't only participate in data transmission and receiving, they also perform as a wireless router of the network as different nodes communicate via their separate communication range, permitting cars in the region of 100 to 300 meters of each other to join the network, and build a network with a wide

range. As cars moves apart of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created [25].

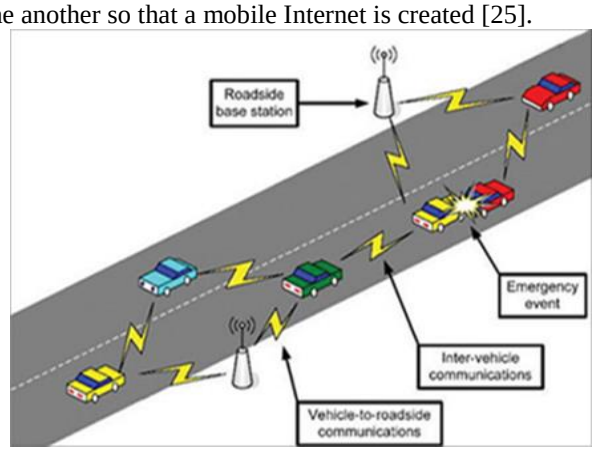

Fig. 1:

Components of VANET are onboard units and roadside units as shown in Figure 3, we can see how communication is transmitted from the roadside unit to the onboard unit in the vehicle, and also a peer to peer communication. This creates a better share of information between vehicles. VANET, vehicles act as nodes, unlike MANET that vehicles are set to move on a predefined road. The nodes must follow traffic rules and signals and their velocity relies on the speed sign [9]. Wireless devices such as; Personal Digital Assistant (PDA), Keyless Entry Device, Mobile Phones, Laptops etc. are used by VANET inside the vehicle [26]-[27]. Due to the increase of mobile wireless devices, the demand for the vehicle-to-vehicle, vehicle-to-roadside, and vehicle-to-infrastructure (V2I) communication will grow soon [28].

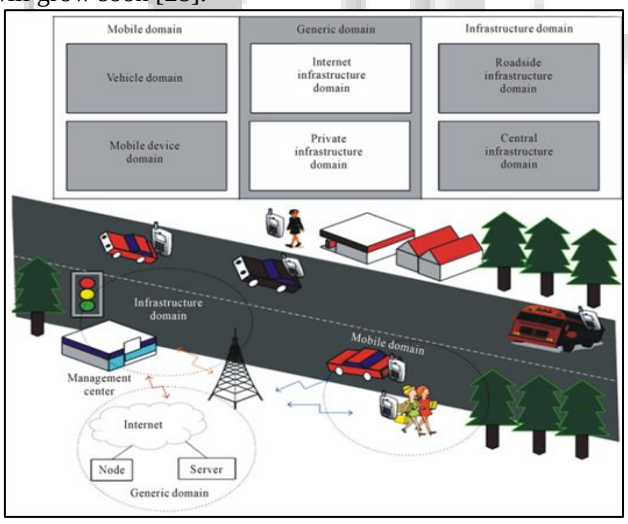

Fig. 2:

There are two type of communication infrastructure available by the VANET; first is the wireless ad hoc network, there exist communication between vehicles without infrastructural support. Secondly, the communication between the vehicle and the road side unit [24]. Due to the relatively high speed of nodes (vehicles) in the VANET and the clustering of vehicles in a particular location can result a very wide network at that time due to the independency of each node, a communication standard known as the Dedicated Short Range Communication (DSRC) was developed to resolve the issue. This standard meets the users requires the use of Road Side Units that are installed along the road as gateways between the infrastructure and the nodes (vehicles) and in converse [21]. The DSRC communicates through a 5.9 GHZ band and uses 802.11 access methods. USA allocated 75 MHZ of spectrum in the 5.9 GHZ, while Europe allocated 30 MHZ of spectrum in the 5.9 GHZ band for DSRC,this is to be utilized by the Intelligent Transportation Systems (ITS) [22].

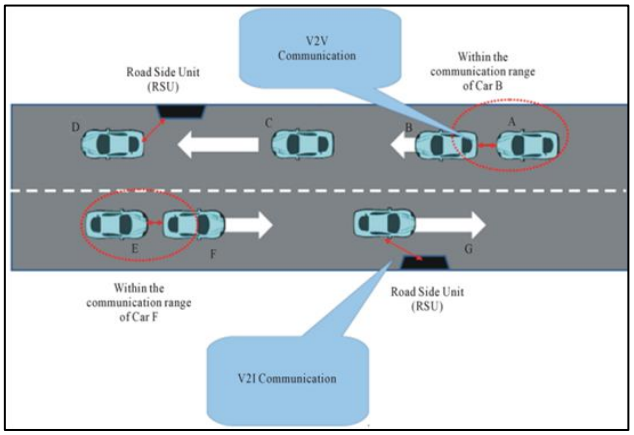

Fig. 3:

III. VANET APPLICATIONS & CHARACTERISTICS

To develop VANETs, there must be some useful applications that benefit from them. The applications where VANET can play major role can be categorized into two broad categories

- Safety Related Application
- User based Application

A. Safety Related Application

These applications are used to increase the safety on the roads. These applications can be further categorized in following way.

1) Collision Avoidance

According to some reviews, 60% accidents will be avoided if drivers were provided a signal half a second before collision [5]. If a driver get a signalon time collision can be avoided.

2) Cooperative Driving

Drivers can get signals for traffic related signals like curve speed signal, Lane change signal etc. These signals can co-operate the driver for an uninterrupted and safe driving.

3) Traffic optimization

Traffic can optimized by the use of sending signals like jam, accidents etc. to the vehicles so that they can choose their alternative path and can save time.

B. User Based Application

These applications provide the user infotainment. A VANET can be utilized to provide following services for the user apart from safety:

1) End to End application

These application are useful to provide services like sharing music, movies etc. among the vehicles in the network.

2) Internet Connectivity

People always wish to be with the Internet all the time. Hence VANET provides the connectivity of the Internet to the users.

3) Other Services

VANET can be utilized in other user based application such as payment service to collect the toll taxes, to locate the fuel station, restaurant etc.

C. Characteristics of VANET

Vehicular Ad-Hoc Networkis an application of MANET but it has its own unique characteristics which can be summarized as: [21]

1) High Mobility

The nodes in VANETs usually move's at a very high speed. These moving nodes can be protected and saved from attacks and other security threats only if their location is predicable. This makes harder to predict a node's position and making safe guard of node privacy [2].

2) Frequently Changing Network Topology

Due to high node mobility and unsystematic speed of vehicles, the position of node changes often. As a result of this, topology in VANETs represents to change frequently.

3) Unbounded Network Size

VANET can be implemented for one city, several cities or for countries. The network size in VANET is geographically unbounded because it is generated for one city or one country

4) Frequent Exchange of Information

The ad hoc nature of VANET inspires the nodes to gather information from the other vehicles and road side units. As vehicles move and change their path, information related to traffic and environment also changes very rapidly.

5) Wireless Communication

VANET is designed for the wireless society. Nodes are inter connected and exchange their information via wireless. Therefore some security ration must be considered in communication.

6) Time Critical

The information in VANET has be sent to the nodes within the limit so that a verdict can be made by the nodes and perform action accordingly.

7) Sufficient Energy

The VANET nodes have no problem of power and resources. This allows VANET to demanding techniques such as RSA, ECDSA application and also provides unlimited transmission power.

8) Better Physical Protection

The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to cooperate physically and reduce the effect of infrastructure attack.

IV. PRIVACY

Globally there is no set definition for privacy, causing some hitches to study what should be kept private. According to the Leading Surveillance Societies in EU (European Union) and the World 2007 proves that the United States has little policies and it is under complete secure surveillance.

There are rules to protect human rights, but nothing of the sort to define privacy. The definition used here is from Dr. Standler research. He defined privacy as "the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause distress to a person [10]." With an accumulation, from the US Code Collection from Cornell University Law School, personal information that can be used as ID should be kept private as well [11]. With a working definition of privacy, we will discuss what should be kept private relating to VANET.

The privacy information is categorized into two groups

- Motor vehicle records
- Personal information

A. Motor Vehicle Records

Motor vehicle records are defined as any record that pertains to a motor vehicle operator's permit [11]. A few examples of motor vehicles records include, but not limited to: motor vehicle title, motor vehicle registration, and identification card issued by a department of motor vehicles.

B. Personal Information

Personal information is defined as information used as identification. A few examples of personal information include, but not limited to: photograph, full name, routine routes and time of travel, bills, and private keys.

Some may think to have VANET with anonymity, but in reality the network would fail if anonymity was introduced to the whole network for every vehicle all the time. First, it would compromise the entire idea of a secure network. Untrue messages could be sent, such as "some pranksters might send bogus warning messages to other cars, pretending that there are dangerous road conditions ahead. This might lead to cars slowing down or breaking, resulting in traffic jams or even accidents [12]."

VANET would only be a success if users feel it can be trusted and utilized it for what is was made for. Second anonymity, would not allow law enforcement to track vehicles. The law implementation may need to track vehicles using VANET as an aid in an investigation of a stolen car or hit-and-run accidents [13]. Therefore, VANET must have a way to validate transmissions and keep security while retaining privacy, ruling out anonymity. Some researched ways to help keep privacy are pseudonyms and keys. Pseudonyms are fictitious names given to vehicles to prevent tracking. There is research to have a "vehicle generate its own pseudonyms, in order to eliminate the need of pre-loading, storing and refilling pseudonyms... [14]." Keys are types of pseudonyms that secure the communication between the sender and receiver.

There are two methods to encrypt and decrypt messages.

- Foremost is the Asymmetric key consisting of a private and public pair of keys that correlate with one another. Public keys can signify mailbox addresses that all the members in the network can see. Private keys is a key that can access the mailbox mentioned above. This key can open any messages that are encrypted with the corresponding public key. For the encryption public key is required. To decrypt the message, the private key is used to decrypt and corresponds to the public key. The pros of public and private keys are the ability to authenticate messages. The disadvantages are: high security overhead [15] [16] [17] and computationally costly storing large number of key pairs and keys must be changed frequently [18].

– Second type of key is the Symmetric key that consists of a key to encrypt and decrypt messages. This key can only be seen by certain individuals with some kind of mutual agreement. The advantages to asymmetric keys are: more efficiency over asymmetric keys, less computational effort, and less vulnerable cryptanalytic advance [16] [17] [19]. The disadvantage is the key distribution process is currently unknown.

V. CONCLUSION

VANET are very effective worth of communication between moving vehicles. In this paper we have seen about various applications, characteristics and about privacy. It gives a clear idea about how it works and what it is for. It has been found that various schemes and techniques have been proposed to overcome these challenges but still various loopholes are remaining in this field and solutions are yet to be discovered. VANET is used to move cars as joint in network to make a transportable network. It improves safety of vehicles by intelligent transportation system. VANET would provide better stand and effective communication between vehicles with further progression and evolution of new approaches.

REFERENCES

[1] Vehicular Ad hoc Network (VANETs): A Review by Divya Chadha1 , Reena2 Assistant Professor, MMICT&BM, Maharishi Markandeshwar University, Mullana, Ambala, Haryana, India M. Phil Scholar, M.M.I.C.T&B.M, Maharishi Markandeshwar University, Mullana, Ambala, Haryana, India
[2] P Rawat, K Deep Singh, H Chaouchi, J-M Bonnin, Wireless sensor networks: a survey on recent developments and potential synergies. J. Supercomput, 1–48 (2013). doi:10.1007/s11227-013-1021-9
[3] Nidhi&Lobiyal, D.K., (2012) "Performance Evaluation of VANET using realistic Vehicular Mobility", N. Meghanathan et al. (Eds.): Vol. 84, CCSIT , Part I, LNICST 84, pp. 477–489.
[4] DW World-de: Deutsche Welle, http://www.dw-world.de/dw/article/0,,5519345,00.html
[5] Khairnar, V.D., Pradhan, S.N,(2010) " Comparative Study of Simulation for Vehicular Ad-hoc Network" , IJCA (0975 – 8887) Volume 4– No.10.
[6] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. International Journal of Communications, Network and System Sciences, 8, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003
[7] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. Transactions on Networks & Communications, Society for Science and Education, United Kingdom, 2, 1-6.
[8] (2011) Vehicular Ad Hoc and Sensor Networks—Principles and Challenges. International Journal of Ad Hoc, Sensor & Ubiquitous Computing (IJASUC), 2.
[9] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad Hoc Networks. International Journal of Science and Advanced Technology, 2, 188-191.
[10] Privacy International, http://www.privacyinternational.org/indexs.html, Clerkenwell, London, (1990).

