ISSN No. 0976-5697

Volume 3, No. 1, Jan-Feb 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

VANET and its Security Issues: An Overview

Dipti M. Jawalkar*
B.E (Computer Sci Engg)
JDIET, Computer Science & Engg
Yavatmal, India
diptifriends06@gmail.com

Suraj N. Chute
B.E (Computer Sci Engg)
JDIET, Computer Science & Engg
Yavatmal, India
suraj1.chute@gmail.com

Avinash P. Jadhao
Assistant Professor
JDIET, Computer Science & Engg
Yavatmal, India
apjadhao@gmail.com

Abstract: Vehicular is infrastructure precise to the next pace in rising transportation safety and comfort. The perverse value of equipped trial beds revenue that computer simulations are only feasible answer for analyzing the concert of dissimilar protocol and architecture. Though imitation frameworks used in vehicular ad hoc network research are still highly diverse and as outcome many of the planned ideas cannot be compared and validated. In this paper we focused on the challenges faced when modeling the vehicular location and the solutions adopted in central simulation tools. As the research neighbourhood is troubled with many diverse troubles from security related issues to traffic efficiency and from intersection management to Internet access we consider that every study should choose the appropriate simulator based on its requirements. Consequently we make some recommendations which take into account the scope of the simulated scenario and the properties of the simulation frameworks

Keywords: VANET, Ad hoc network, DSRC, FCC, V2V, V2I, ITS, RSU, ECC, GPSR.

I. INTRODUCTION

Millions of people around the world die every year in car accidents and many more citizens are indignant. Implementations of security information such as pace limits and road situation are used in many parts of the world but still supplementary work is required. Vehicular Ad Hoc Networks (VANET) should be valid and assemble, deal out safety information to mainly reduce the number of accidents by caveat drivers about the hazard before they actually visage it. (VANET) are budding as preferred system design for smart transportation system. Such networks consist of sensors and On Board Units (OBU) installed in the car as well as Road Side Units (RSU). The data collected from the sensors on the vehicles can be displayed to the driver. It can be sent to the RSU or even broadcasted to other vehicles depending on its nature and importance.

The RSU distributes the data with road sensors, weather centers, traffic control centers, etc to the vehicles and also provides marketable services such as parking space booking, Internet access and gas payment. The network makes broad use of wireless communications to attain its goals but even though wireless infrastructure reached a level of development, a lot more is required to apply to such a complex system. Most available wireless systems rely on a base station for management and other services; However using this approach means covering all roads with such communications which is impractically too pricey. Ad hoc networks have been studied for some time but VANET will form the major ad hoc network ever implemented, therefore issues of constancy, consistency And scalability is of anxiety. VANET therefore is not an architectural network and not an ad hoc network but a combination of both. This exceptional feature combined with high speed nodes complicates the purpose of the network.

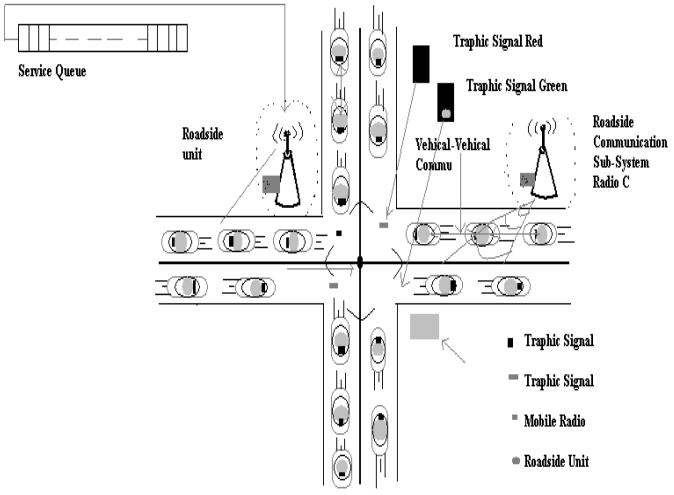

Figure 1. Vehicular Ad hoc Network

Vehicular Ad-hoc Networks (VANETs) are promising as the ideal network design for intelligent transportation systems. VANETs are based on petite range wireless communication (e.g., IEEE 802.11) between vehicles [1]. The Federal Communications Commission (FCC) has allocated 75 MHz in

the 5.9 GHz band for qualified Dedicated Short Range Communication (DSRC) [2] meant at attractive bandwidth and dropping latency for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Unlike infrastructure-based networks (e.g., cellular networks), VANETs are constructed and do not require any speculation besides the wireless network interfaces that will be a standard mark in the next production of vehicles. Furthermore, VANETs facilitate a new set of applications that require time-critical responses (less than 50 ms) or very elevated data transfer rates (6-54 Mbps). VANETs have sole characteristics as: very lofty mobility, theoretically inestimable extension, nonexistence of a centralized control, and blinking connectivity through the meager infrastructure. These characteristics give augment to challenges in information swap and data scheduling. In this paper we endow with an indication of the technologies and enduring research related to VANET. The history and the primary cohort VANET systems around the world are reviewed in the next section [3].

II. BACKGROUND OF VEHICULAR COMMUNICATIONS

The innovative motives behind vehicular communications were safety on the road, numerous lives were lost and much more injuries have been incurred due to car crashes. A driver realizing the brake lights of the car in obverse of him has only a few seconds to respond, and even if he has responded in moment cars behind him could crash since they are naive of what is going at the front. This has provoked one of the first applications for vehicular communications, namely supportive collision warning which uses vehicle to vehicle communication [4]. Other safety applications rapidly emerged as well as applications for more competent use of the transportation network, less clogging and faster and safer routes for drivers. These applications cannot function competently using only vehicle to vehicle communications therefore an infrastructure is needed in the structure of RSU. Although safety applications are vital for governments to assign frequencies for vehicular infrastructure, non safety applications are as important for Intelligent Transportation Systems (ITS) for three reasons:[5] 1) ITS systems rely on crucial equipment which should be installed in every car and is broadly available to the users.

However, it is doubtful that individuals can afford such classy equipment. 2) Safety applications generally necessitate limited bandwidth for short intervals of time. Since bandwidth efficiency is an important factor, non safety applications are important to boost bandwidth efficiency. 3) The availability of RSU provides an infrastructure which can be used to provide a set of services with only a little raise in cost. Besides road safety, new applications are proposed for vehicular networks, among these are Electronic Toll Collection (ETC), car to home communications, travel and tourism information distribution, multimedia and game applications just to name a few. However these applications need reliable communication equipment which is capable of achieving high data rates and constant connectivity between the transmitter and the receiver under high mobility conditions and different surroundings. Different frequencies for VANET were allocated in varied parts of the globe. In North America the Dedicated Short Range Communications (DSRC) band 902928 MHz was allocated. It provided short range communications (30m) and short data rates (500 kbps). It is still used for some types of electronic toll assortment systems but its concert is too limited to satisfy the demanding requirements of ITS applications.

The system relies on road architecture, as with DSRC, and provides ETC service. The standard uses ASK modulation for a data rate of 1Mbps with 8 slots TDMA/ FDD to provide service for a maximum of 8 cars within a range of 30m. Currently a new standard (ARIB STDT75) is being developed. These systems can be regarded as the first generation for vehicular communications. The different standards and frequencies hindered the implementation of ITS systems since each country has its own specifications and operating systems. Moreover the low data rates and short distances were only suitable for a limited number of applications [6].

III. HOW VANET WORKS

Vehicular Networks System consists of large number of nodes, approximately number of vehicles exceeding 750 million in the world today , these vehicles will require an authority to govern it, each vehicle can correspond with other vehicles using short radio signals DSRC (5.9 GHz), for range can reach 1 KM, this communication is an Ad Hoc communication that means each linked node can move freely, no wires required, the routers used called Road Side Unit (RSU),the RSU works as a router between the vehicles on the road and connected to other network devices. Each vehicle has OBU (on board unit), this unit connects the vehicle with RSU via DSRC radios, and another device is TPD (Tamper Proof Device), this device holding the vehicle secrets, all the information about the vehicle like keys, drivers identity, trip details, speed.

IV. VANET ATTACK

In this paper, we are concentrating on attacks [7] perpetrated against the message itself rather than the vehicle, as physical security is not in the scope of this paper. Maintaining the integrity of the specifications.

A. Denial of Service Attack:

This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel Used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application's information. For instance, if a malicious wants to create a massive pile up on the highway, it can make an accident and use the DoS attack to prevent the warning from reaching to the approaching vehicles. Authors in [8] discussed a solution for DoS problem and saying that the existing solutions such as hopping do not completely solve the problem, the use of multiple radio transceivers, operating in disjoint frequency bands, can be a feasible approach but even this solution will require adding new and more equipments to the vehicles, and this will need more funds and more space in the vehicle .The authors in [9], proposed a solution by switching between different channels or even communication technologies (e.g., DSRC, UTRA-TDD, or even Bluetooth for very short ranges), if they are available, when one of them (typically DSRC) is brought down.

B. Message Repression Attack:

An attacker selectively dropping packets from the network, these packets may hold decisive information for the receiver, the attacker suppress these packets and can use them again in other time. The goal of such an aggressor would be to prevent registration and insurance authorities from learning about collisions involving his vehicle or to avoid delivering collision reports to roadside access points. For instance, an attacker may restrain a blocking warning, and use it in another time, so vehicles will not obtain the warning and forced to wait in the traffic.

C. Fabrication Attack:

This attack happens when attacker alters an existing data, it includes delaying the communication of the information, replaying earlier transmission, or varying the actual entry of the data transmitted .For instance, an attacker can change a message telling other vehicles that the current road is clear while the road is congested

D. Modification Attack:

This attack happens when attacker alters an existing data, it includes delaying the communication of the information, replaying earlier transmission, or varying the actual entry of the data transmitted .For instance, an attacker can change a message telling other vehicles that the current road is clear while the road is congested

E. Reply Attack:

This attack happens when an attacker rerun the transmission of an earlier information to take advantage of the situation of the message at time of sending.

V. SECURITY REQUIREMENTS

A. Endorsement:

In Vehicular Communication every message must be authenticated, to make sure for its origin and to control authorization level of the vehicles, to do this vehicles will assign every message with their private key along with its certificate, at the receiver side, the receiver will receive the message and check for the key and certificate once this is done, the receiver verifies the message[8][9] .Signing each message with this, causes an overhead, to reduce this overhead we can use the approach ECC(Elliptic Curve Cryptography), the efficient public key cryptosystem, or we can sign the key just for the critical messages only

B. Accessibility:

Vehicular network must be available all the time, for many applications vehicular networks will require real time, these applications need faster response from sensor networks or even Ad Hoc Network, a delay in seconds for some applications will make the message meaningless and maybe the result will be devastating. Attempting to meet real-time demands makes the system vulnerable to the DoS attack. In some messages, a delay in millisecond makes the message meaningless the problem is much bigger, where the application layer is unreliable, since the potential way to recover with unreliable transmission is to store partial messages in hopes to be completed in next transmission [5].

C. Non-Repudiation:

Non-repudiation will facilitate the ability to identify the attackers even after the attack happens. This prevents cheaters from denying their crimes. Any information related to the car like: the trip rout, speed, time, any violation will be stored in the TPD, any official side holding authorization can retrieve this data

D. Privacy:

Keeping the information of the drivers away from unauthorized observers, this information like real identity path, speed. The privacy could be achieved by using temporary (anonymous) keys, these keys will be changed frequently as each key could be used just for one time and expires after usage, all the keys will be stored in the TPD, and will be reloaded again in next time that the vehicle makes an official checkup

VI. RELATED WORK

Jie Luo Xinxing Gu Tong Zhao Wei Yan proposed [11] that traditional wireless ad-hoc networks routing protocols, such as DSR and AODV, are not suitable for VANET. To deal with the rapidly changing network topology, a new routing technique based on location information has been developed. One famous strategy is GPSR . GPSR selects the node that is the closest to the destination among the neighboring nodes. When local maximum occurs, the algorithm recovers by routing around the perimeter of the region. Due to local maximums are common in urban VANETs, GPSR seems not the best choice. Recently, some other routing protocols for VANETs have been proposed. The Geographical Source Routing [12] protocol combines position-based routing with topological knowledge. GyTAR [13] is another protocol, in which time road traffic variation is taken into account.

The carry-and-forward mechanism is used in most of these protocols which introduces a large packet delay. Other method is required to deal with network disconnection. There are also several VANET routing protocols based on infrastructure or road side unit (RSU). SADV utilizes some static nodes at road junctions. With the assistance of static nodes at junctions, a packet can be stored in the node for a while and wait until there are vehicles within communication range along the best delivery path. RAR is a vehicular hybrid network routing protocol in which roads are divided into sectors by RSUs, and the route consists of vehicles and RSUs. The drawback of these protocols is the requirement and distribution of static node or RSU. To evaluate routing protocols for VANETs by simulation, various traffic mobility models have been studied. VanetMobiSim [9] is a well known and validated traffic generator, which is developed by Eurecom. We use this traffic generator in our simulation studies.

In VANET many security solutions been proposed, and large number of papers were introduced to solve the problems, the authors Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures suggested the use of VPKI (Vehicular Public Key Infrastructure) as a solution, where each node will have a

public/private key. When a vehicle sends a security message, it signs it with its own private key and adds the Certificate Authority (CA's) certificate as follows:

V → r: M, SigPrKV [M|T], Certv [9]

Where V is the sending vehicle, r represents the message receivers, M is the message, | is the concatenation operator, and T is the timestamp to ensure message freshness (it can be obtained from the security device).The receivers of the message will obtain the public key of V using the certificate and then verify V's signature using its certified public key. In order to do this, the receiver should have the public key of the CA.

The authors W Ren, K Ren, W Lou, Y Zhang, suggested an idea of using the group signature, but this idea has a major drawback that it is causing a great overhead, every time that any vehicle enters the group area, the group public key and the vehicle session key for each vehicle that belongs to the group must be changed and transmitted, another issue must be considered that the mobility of the VANET prevents the network from making a static group, so the group is changing all the time, and the signatures and keys frequently changed and transmitted, group signature as the authors proposed a protocol for guarantee the requirements of the security and privacy, and to provide the desired trace ability and liability, but the result of the study was not quit encouraging, After 9 ms for group signature verification delay, the average message loss ratio was 45%, another result was the loss ratio reaches as high as68% when the traffic load is 150 vehicles.

The other solution been suggested is the use of CA and this requires infrastructure for it. VANET requires a large number of CA to govern it.until now we don't have a real authoritythat govern the world of VANET. Thus, when another vehicle receives this message, it verifies the key used to sign the message and if everything is correct, it verifies the message, and they have proposed the use of ECC to reduce the overhead. Another way to use the keys, by using short term certificates and long term, long term certificates are used for authentication while short term certificates are used for data transmission using public/private key cryptography. Safety messages are not encrypted as they are intended for broadcasting, but their validity must be checked; therefore a source signs a message and sends it without encryption with its certificate; other nodes receiving the message validate it using the certificate and signature and may forward it without modification if it is a valid message, so any adversary can inject false information as a safety message, as it doesn't to be encrypted, it also can steal the certificate from any other safety message and send unencrypted message contains false information along with the stolen certificate claiming that the safety message originated from another vehicle.

The most common way to revoke certificates is the distribution of CRLs (Certificate Revocation Lists) that contains all revoked certificates but this method has some drawbacks: First, CRLs can be very long due to the enormous number of vehicles and their high mobility. Second, the short lifetime of certificates still creates a vulnerability window and last one is that there is no infrastructure for the CRL. Each key can be used only once and expires after its usage; only one key can be used at a time. These keys are preloaded in the vehicle's TPD for a long duration; each key is certified by the issuing CA and has a short lifetime (e.g., a specific week of the year). In addition, it can be traced back to the real identity of the vehicle ELP, the drawback of this solution that the keys need storage.

VII. ACKNOLEDGEMENT

We express our thanks and sincere gratitude to our guide Mr. Avinash P. Jadhao Assistant Professor of Computer Science & Engineering Department for providing his valuable guidance for successful completion of this paper. I also thank to Mr. M. V. Sarode the Head of Department Computer Science and Engineering for being constant source of inspiration.

VIII. CONCLUSION AND FUTURE

In this paper we first gave description of vehicular ad hoc network. Vehicular Ad Hoc Networks is promising technology, which gives copious chances for attackers, who will try to dare the network with their malevolent attacks. This paper gave a broad analysis for the recent challenges and solutions, and critics for these solutions, in our upcoming work we will propose new solutions that will help to maintain a securer VANET network, and test it by simulation

IX. REFERENCES

[1] J. Ott and D. Kutscher, "Drive-thru Internet: IEEE 802.11b for Automobile Users", *In IEEE Infocom*, 2004.

[2] R. Gass, J. Scott, and C. Diot, "Measurements of In-Motion 802.11 Networking", In IEEE Workshop on Mobile Computing System and Applications (Hotmobile 2006), April 2006.

[3] Data Scheduling in VANET : A Review by Vishal 1Kumar and Narottam Chand International Journal of Computer Science & Communication Vol.1 , No.2 July-December 2010, pp 399-403

[4] "ITS Applications Overview, "http://itsdeployment2.ed.ornl.gov/technolog_overview/.

[5] K. Matheus, R. Morich, and A. Lübke,"Economic Background of Carto Car Communication," http://www.network–on–wheels.de/documents.html, 2004.

[6] Current Trends in Vehicular Ad hoc Network by Ghassan M. T. Abdulla, Mosa Ali Abu-Rgheff and Sidi Mohammad Sinouci University of Plymouth School of Computing ,Communications & Electronics,UK.

[7] Security Analysis of Vehicular Ad Hoc Networks(VANET) by Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures National Advanced IPv6 Center, Universiti Sains Malaysia ,Penang, Malaysia in 2010 Second International Conference on Network Application Protocol and Services.

[8] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006

[9] M Raya, J Pierre Hubaux, "The Security of Vehicular Ad Hoc Networks ", Proc. of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2005.

[10] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of Hot Nets-IV, 2005.

[11] "A Mobile Infrastructure Based VANET Routing Protocol in the Urban Environment" ,2010 International Conference on Communications and Mobile Computing by, Jie Luo Xinxing Gu Tong Zhao Wei Yan School of Electronics Engineering and Computer Science, PKU, Beijing, China.

[12] B. Karp and H.T.Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. MobiCom2000: Proceeding of the 6th annual international conference on Mobile computing and networking, pages 243–254, August 2000.

[13] M. Jerbi, S.-M. Senouci, R. Meraihi, and Y. Ghamri-Doudane. An improved vehicular ad hoc routing protocol for city environments. ICC'07. IEEE International Conference on Communications, pages 3972–3979, June 2007.