Survey on Various Security Issues and prevention method in Vehicular Ad hoc Networks

P.Dharani[1], Pravin R. Patil[2], C.Mahesh[2#]

[1]*M Tech Scholars, Dept. of Information Technology*
[2#]*Assistant professor, Dept.Of Information Technology VelTech Dr.RR & Dr.SR Technical University, Chennai*
[2] *Assistant professor, Dept. Of Computer Science and EngineeringPune Institute of Computer technology, Pune*

Abstract: *Vehicular adhoc networks are a subset of mobile adhoc networks. This forms wireless network between vehicles for better communications and to break away from the hindrance caused by attackers. Various security architectures and methods are proposed. In this paper, we focused on the survey for various security issues and preventive methods from works for vanets*

I. Introduction

With the emergence of mobile ad-hoc networks (MANETs), scientists need conceptualized the idea of communing vehicles, giving increase to vehicular ad hoc networks (VANETs), which are the major heart of engineers longing to turn cars into intelligent machines that commune for safety and comfort purposes. A VANET is formed by vehicles that are equipped with wireless communication devices, positioning systems, and digital maps. VANETs too permit vehicles to connect the roadside units (RSUs), which are connected to the Internet and may also be connected with each other via a high-capacity mesh network. Most research on routing in VANETs is limited to vehicles a few hops away. However, here various requests, it stands significant to send data towards its far vehicles, thus necessitating a multi-hop routing protocol [1]. Several researchers have developed unicast routing protocols for VANETs [2,3,4,5,6] certain of which use a position based greedy approach that uses the geographic coordinates of vehicles to find a correct path [2], [6]. Alternative set of procedures, which make use of carry-and-forward approaches and aim to route packets in scant VANETs, are named delay-tolerant algorithms [1], [5]. Finally, quality-of-Service protocols focus on finding routes that last for the longest possible time [4]. Each of the foregoing protocols has its conditions to provide fine performance. Position-based protocols assume opaque conditions in which a vehicle always finds a neighbor to forward to. In contrast, delay-tolerant algorithms do not perform well in dense cases. In this paper, we propose to utilize RSUs to route packets to distant locations. A vehicle Source (S) requesting to send a packet P to a distant vehicle D can send P to its adjacent RSU (R1), which in turn, sends Packet (P) to the adjacent RSU (R2) to Destination (D) through the RSU network. R2 then sends P to D during multi-hop. Note down that other works, similar to [7], used RSUs to route messages but most of them are suited for dense or sparse conditions, and not both. In our system, we combine position based routing and carry and forward to opportunistically route messages to and from RSUs. The basic motivation behind using RSUs to route packets is that RSUs are a fixed infrastructure. It is much easier to send a packet to a fixed target than to a remote moving item. In addition, the delay of distribution the packet through the fixed RSU network is much less than through the VANET. We request our approach Carry then forward mechanisms for Dependable message delivery in Vanets using RSUs. The plan of our system is divided into two basic parts: the initial part governs routing from a vehicle to its neighboring RSU, and then the next part handles routing from RSUs to vehicles. Mainly earlier routing approaches for VANETs take for granted that the sender knows the location of the receiver. In contrast, our system assumes that the sender is interested in sending data to the receiver or requesting information from him without necessarily knowing his position. An instance is customer's scattering multimedia accounts. A next case is where customers are questioning about positive services, like trying to find a list of Italian restaurants in the city along with their menus. In such cases, the requester might know the identity of the receiver who has the data (e.g., a friend or a co-worker) but not his current location. Other important applications that benefit from our routing scheme include queries about road conditions in far-away locations. For example, consider a vehicle heading from a coverage area toward another, the vehicle driver might request from an RSU inside the coverage area he is heading to information about the road condition and the amount of traffic in certain streets or information about some weather variables, or even request road navigation information from a point to another inside the district based on the expected traffic conditions. Generally, each driver tries to plan his trip in the best probable method, and then he might request exact requests from vehicles that are far away. Another application concerns societal networks, anywhere, on behalf of illustration, in paper [8], building societal networks confidential VANETs and exchanging private messages among their members has been proposed. Finally, [9] proposes that likeminded users in their vehicles can chat with each other using VANET infrastructures. While these applications are limit themselves to short distances, CAN DELIVER serves to extend these applications through allowing members to exchange messages by relaxing the distance limit. The contributions of this effort are précised as follows:

1) Offering a routing protocol suitable for both opaque and thin conditions. To the most excellent of our information, maximum previous routing etiquettes for VANETs are not designed to work well in both dense and thin conditions. Otherwise, we show in Section IV to CAN DELIVER performs well under all considered VANET conditions.

2) Predicting the location of the destination in a precise manner and making use of all available nodes to reach the destination. We compare our prediction method with others and prove, through simulations, that our method is more suitable to VANET scenarios than others.

3) Routing messages through RSUs to enable distant users to communicate through each other. Our system differs from previous mechanism in two aspects. First, we do not execute route discovery. Second, we use the username to search for the RSU of the destination. Usernames be dispersed amongst RSUs via a distributed hash table (DHT) that renders the process of locating the target very fast and efficient.

Several wireless technologies can be used to provide connectivity in vehicular networks. Inside [10], a discussion about these technologies is provided. According to [10], dedicated short-range communications (DSRC) is better suited to inter vehicle communication than third-generation (3G) and fourth generation (4G) for several reasons: 1) 3G and 4G have higher latencies, and 2) 3G and 4G require precise information about locations of vehicles to ensure successful communication. Inside [11], it be acknowledged that the rate of cellular data communication is restrictively high, and even expensive "unlimited" plans are usually capped to a few hundred megabytes per month, making large-scale communication (such as real-time fine-grained traffic information) between thousands of vehicles unfeasible. Furthermore, although 3G connections can support up to 128 kb/s, the bandwidth be shared flanked by users inside the cell. Even today, when 3G is not broadly used, the network is busy by traffic, resulting in very low throughput in thickly populated areas [11]. In Section IV, we simulate a custom-built universal mobile telecommunications system (UMTS) routing protocol that provides the same functionality of CAN DELIVER, and provide a comparative analysis of the two systems.

II. Previous Work

This paper [1] proposes an asymmetric profit-loss Markov (APLM) model to measure the integrity level of security schemes for VANET substance deliverance. Turnover defines integrity gain toward a system by its devices detecting and disregarding corrupted information fragments. Failure represents negative result to a system at receiving a corrupted information fragment. Markov chain records modify of system performance that reacts to profit and loss irregularly. The benefit of APLM model is its black-box approach that measures the integrity level without the need to examine the implementation details of a particular security plan, depiction the model possible intended for actual humanity purposes. Taking keen on account the special characteristics of integrity plans in VANET, APLM model be tested on five scenarios. The measuring outcomes show meaningfulness, repeatability, as well as feasibility of APLM form. APLM form too supports optimization of protection scheme design for VANET content delivery.

The whole number of vehicles in the world has practiced an extraordinary development, [2] increasing traffic density which results in more and more accidents.

Therefore the manufactures, researchers and government is shifting focus towards improving the on road safety rather than improving the quality of the infrastructures. The good quality improvement in the wireless technologies emerged various new type of networks, such as Vehicular Ad Hoc Network (VANET), which provides communication between vehicles themselves and between vehicles and RSUs. A variety of innovative concepts such like smart cities and living labs [1] are introduced in the recent years where VANETs plays a vital role. A study of various Intelligent Traffic Systems (ITS) and various routing protocols with respect to our proposed scheme is described inside this article. It too introduces a new method consist of a smart city framework that transmit information about traffic conditions that will help the driver to take fitting decisions. It consists of a caution message part composed of Intelligent Traffic Lights (ITLs) which provides information to the driver about current traffic conditions.

In this paper [3], we first discuss the challenges for trust management caused by the important characteristics of VANET backgrounds. We after that survey obtainable trust models in multi-agent systems, mobile ad-hoc networks (MANETs) as well as VANETs, and point out their input issues. Based on top of these studies, we propose desired properties towards effective trust management within VANETs, setting up clear goals used for researchers in this area.

In this paper [4], we propose the signature scheme which resolves the key update problem in VANETs using tamper-proof device. By the scheme like a building block, we also propose the vehicle-to-vehicle communication protocol which provides desirable but conflicting functionalities such as anonymity, authenticity, unlink ability, non-refutation, as well as traceability.

In this paper [5], we analyse the transport capacity characteristic of Vehicular adhoc network in 802.11. Based on these, the accident and interference of VANET are too studied. A possibility analysis model is applied in VANET. The number of accident/interference resource impacted packets transmission-receive according to the probability model. A new scheme –one hop one channel, be projected for multi-interface routing in VANET. One hop one channel is able to reduce collision /interference foundation efficiently.

The simulation too proved so as to the probability of one hop one channel is lower. As it, delay of one hop one channel is shorter.

In this paper [6], we propose the application of cryptography algorithm to ensure secure communication across the virtual networks. Inside cryptography, encryption is the procedure of encoding messages or information in such a way that hackers cannot study it. In an encryption method the message or information is encrypted using an encryption algorithm, rotating it into an unreadable cipher text (CT). This is regularly done with the use of an encryption key. Any adversary that can see the cipher text should not know anything about the original message. To decode the cipher text using an algorithm that typically requires, a clandestine decryption key. An encryption method usually needs a key generating algorithm to randomly produce keys. Pseudo Random Number Generator (PRNG) is an algorithm for generating a series of numbers. Owing to speed in number generation pseudorandom numbers are very important. The output sequence of RM-PRNG is used as a key to the encryption and decryption parts. The simulation outcomes are obtained through using modelsim 6.3g_p1.

In this paper [7] we improve location privacy of mix-zones via extensions to the CMIX procedure. Through carrying out widemodels, we investigate thenrelate the effective location privacy provided by the proposed approach.

In this paper [8] we introduce a new routing technique designed exclusively for VANETs and present a few initial performanceoutcomes. The algorithm remains named Junction-based Multipath Source Routing (JMSR). Its main characteristics comprise the multiple routes towards destination, junction-centric logic and the acceptance of source routing mechanisms.

This paper [9] presents several existing security attacks and approaches to defend against them, and discusses possible future security attacks with critical analysis and future research possibilities.

This paper [10] presents a class of routing protocols called road-based using vehicular traffic (RBVT) routing, which outperforms obtainable routing protocols in city-based vehicular ad hoc networks (VANETs). RBVT protocols leverage real-time vehicular traffic information to create road-based paths consisting of successions of road intersections to have, by means of high probability, network connectivity along with them. Geographical forwarding is used toward transfer packets between intersections on the pathway, reducing the path's compassion toward individual node travels. Intended for opaque networks with high controversy, we optimize the forwarding by means of a scattered receiver-based election of next hops based on a multi criterion prioritization function that takes non uniform radio propagation keen on account. We planned and implemented a reactive protocol RBVT-R and a proactive protocol RBVT-P and compared them with protocols representative of mobile ad hoc networks as well as VANETs. Simulation outcome in metropolitan settings demonstrate that RBVT-R performs best in terms of average delivery rate, with up to a 40% increase compared with some presented protocols. Inside provisions of average holdup, RBVT-P performs best, with as much as an 85% decrease compared with the other protocols.

In this paper [11], we investigate the problem of alleviating unauthorized tracking of target vehicles by adversaries within VANETs. We suggest a vehicle density-based location privacy (DLP) scheme which can provide location privacy by utilizing the neighboring vehicle density as a threshold to change the pseudonyms. We derive the delay sharing as well as the average total delay of a vehicle within a density region. Given the holdup information, an opponent may still be available to track the target vehicle by a choice rule. We investigate the efficiency of DLP based on extensive imitation study. Imitation outcome demonstrate that the probability of successful location tracking of a target vehicle by an adversary is inversely proportional to both the traffic arrival rate and the variance of vehicles' pace. Our proposed DLP scheme too has a better performance than both Mix-Zone scheme and AMOEBA with random silent period.

This paper [12] presents the Zone Routing Protocol. Initially, we talk about the trouble of routing in ad-hoc networks and the incentive of ZRP. We illustrate the structural design of ZRP, which consists of the three sub-protocols. We explain the routing procedure and illustrate it by means of an example. Additional, we describe the query control mechanisms, which be used toward reduce the traffic quantity in the route detection process. ZRP does not define the real implementation of the protocol components. So, we there the guidelines used for implementation, as well as example implementations provided inside the draft stipulation. We talk about the problem of routing inside networks with unidirectional links, and the suggestion for a solution toward it. The overhead of the routing protocol be important in the power and bandwidth limited adhoc networks. We talk about the factors influencing on the traffic amount based on measurements performed in a number of documents. We describe the important issue of choosing an optimal region radius, with two algorithms used for automatic selection of the radius. Lastly, we draw various conclusions concerning the performance of the protocol. The paper is based on top of literature research.

III. Challenges Of Vanet Security

Where Roadside Equipment's (RSEs) operate in two modes: infrastructure and ad operating in infrastructure mode, cone infrastructure such as the Internet or cellular networks for services provided by external components like travel advertisement and electronic toll collection. A RSE communicates with vehicles' On-Board Equipment's sporadically in ad-hoc mode. OBEs communicate among themselves also in ad-hoc mode. An OBE contains OBD a set of sensors to measure the vehicles own status such as its brake, GPS to identify its location, Radar to detect other vehicles near, then Transceiver (combination of Transmitter and Receiver) toward communicate RSEs and other On Board Equipment. These mechanisms feed information to Co-Driver, a special purpose workstation, which screens road safety and processes mobile services. The VANET although very well-organized, faces hard challenges to protect its applications due to his spread, open, then movable nature. For example, conventional information assurance relies on authentication centers that are not within reach in distributed infrastructure Wireless communications offer open access, vulnerable to malicious attacks. Process time constrains the applicability of the current cryptography-based technology on ordinary mobile devices to high-speed moving vehicles. VANET security becomes an emerging research field, and several promising secure mechanisms have been proposed and deployed for VANET [3, 4, 5, and 6]. There is urgent need for security metrics development. Standardized security measurement builds consumer confidence towards VANET requests then promises predictability by way of well as answerability aimed at a VANET safety mechanism. However, security measure is hard. Pfleeger then Cunningham, now their paper [7], list nine major reasons why security measurement is dissimilar since and tougher than additional kinds of measurement. Computing VANET safety stances extra challenges due to its top level of anxieties happening road safety then its nature.

IV. VANET Communication Methods:

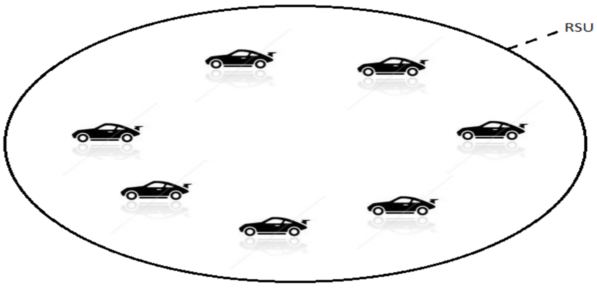
4.1 Hop by Hop Communication:

The hop to hop communication is an old and initial method can be having each vehicle to vehicle transfer the data for an emergency time. The vehicle transfer the data in beacon packets and it will take andcommunicate for critical situation. But, it have more cost and not efficient to all. Nowadays, each vehicle communication is not possible.so we avoid the one to one communication and wireless technology is far for broadcasting techniques.

Hop-by-Hop Communication

4.2 Zone based communication:

The zone can be having a number of nodes and it can communicate with help of Road Side Unit (RSU). Here zone to zone communication also using and it take more key updating cost that's why the data will be lost. If one zone to zone data transfer mean, it want a key updating for a zone. That's why it can't efficient.



Zone based Communication

4.2.1 Zone Routing Protocol (ZRP):

Motivation:

As seen, [12] proactive routing uses excess bandwidth to maintain routing information, as immediate routing involves extended route request delays. Immediate routing also ineffectually floods the entire network for route determination. The Zone Routing Protocol (ZRP) [11]–[13] aims to address the problems by combining the best properties of both approaches. ZRP can be classed as a crossbreed reactive/proactive routing protocol. [10] In an ad-hoc network, it can be assumed that the largest part of the traffic is directed toward near nodes. So, ZRP reduces the proactive range to a zone centered on every node. Within a limited zone, the preservation of routing information is simple. Additional, the quantity of routing information that is never used be minimized. At rest, nodes past away can be reached with immediate routing. As every node proactively store local routing information, route requests can subsist more efficiently performed without querying all the network nodes. [10] Despite the make use of zones, ZRP has a horizontal view more than the network. Within this way, the organizational in the clouds related to hierarchical protocols are able to be avoided. Hierarchical routing protocols depend on the strategic assignment of gateways otherwise landmarks, therefore that every node be able to access every level, particularly the top level. Nodes belonging to different subnets must send their communication to a subnet that is common toward both nodes. This might obstruct part of the network. ZRP can be categorized like a horizontal protocol because the zones overlie. Therefore, best routes can be detected as well as network congestion can be reduced. [15] Further, the behavior of ZRP is adaptive. The performance depends on top of the existing pattern of the network and the performance of the user's only authenticated.

V. Problem Statement:

However, existing unidentified routing protocols depends on either hop-by-hop encryption or unnecessary traffic whichever makes high cost or cannot provide full privacy protection to zone based encryption. The high cost intensifies the essential resource constraint problem in vanet.

VI. Future Enhancement

To offer high privacy protection at a low cost, we propose a mix zone encryption based routing the message. One of them is, a unique identifier (called ID) is assigned to each vehicle, and all the communicated messages have this ID. Here using digital signatures &PKI (Public Key Infrastructure) and mix zone based security to protect message integrity is sufficient taking into account multilateral security.

VII. Conclusion:

In this paper we investigate several security architectures and preventing methods against attackers. The advantages and disadvantages of surveyed securing architecture are described and the same have been analyzed in terms of security measures.

References:

[1] Globecom 2012 - Communication and Information System Security Symposium A Security Metric for VANET Content DeliveryIkecukwu K. Azogu, Michael T. Ferreira, Hong Liu, Department of Electrical and Computer Engineering University of Massachusetts Dartmouth 285 Old Westport Road. N. Dartmouth, USA Email: U_Iazogu, MFerreira, HLiu@umassd.edu

[2] A Smart City Framework for Intelligent Traffic System Using VANET Ganesh S. Khekare Department of Computer Science and Engineering G. H. RaisoniCollege of Engineering Nagpur, India. khekare.123@gmail.com, Apeksha V. Sakhare Department of Computer Science and Engineering G. H. RaisoniCollege of Engineering Nagpur, India. apeksha7777@gmail.com.

[3] 2011 International Conference on Advanced Information Networking and Applications A Survey on Trust Management for VANETs Jie Zhang School of Computer Engineering, Nanyang Technological University, Singapore, zhangj@ntu.edu.sg

[4] 2007 International Conference on Convergence Information Technology Anonymous and Traceable Communication Using Tamper-Proof Device for Vehicular Ad Hoc Networks Bum Han Kim_1, Kyu Young Choi1, Jun Ho Lee1, and Dong Hoon Lee2Center for Information Security Technologies Korea University, Seoul, Korea{anewholic, young, jhlee}@cist.korea.ac.kr1, donghlee@korea.ac.kr2

[5] First International Conference on Intelligent Networks and Intelligent Systems Capacity, collision and interference of VANET with IEEE 802.11 MAC Wu Ming1), Yang Lin-tao2), Li Cheng-yi2), Jiang Hao2)1) (Wuhan Maritime Communication Research Institute, Wuhan 430079, China)2) (Department of Electronic Information, Wuhan University, Wuhan 430079, China)

[6] International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013 Design of a New Cryptography Algorithm using Reseeding-Mixing Pseudo Random Number Generator S. DilliBabu, Madhu Kumar Patnala

[7] Improving Location Privacy in Mix-Zones for VANETs Antonio M. Carianha, Luciano Porto Barreto, George LimaFederal University of BahiaDistributedSystems Laboratory (LaSiD) - Computer Science Department40170-110, Salvador-BA, Brazilcarianha@ymail.com, {lportoba, gmlima}@ufba.br

[8] IEEE COMMUNICATIONS LETTERS, VOL. 17, NO. 3, MARCH 2013 Investigating a Junction-Based Multipath Source Routing Algorithm for VANETs PavlosSermpezis, GeorgiosKoltsidas, and Fotini-NioviPavlidou, Senior Member, IEEE

[9] Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs) Mohammed Saeed Al-kahtaniComputer Engineering Dept., Salman bin Abdulaziz University, Saudi Arabiaalkahtani@sau.edu.sa

[10] IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 7, SEPTEMBER 2009 VANET Routing on City Roads Using Real-Time Vehicular Traffic Information JosianeNzouonta, NeerajRajgure, Guiling (Grace) Wang, Member, IEEE, and Cristian Borcea, Member, IEEE

[11] Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung Department of Electrical and Computer Engineering the University of British Columbia, Vancouver, BC, Canada, V6T 1Z4 E-mail: {joohans, vincentw, vleung}@ece.ubc.ca

[12] Zone Routing Protocol (ZRP) NicklasBeijarNetworking Laboratory, Helsinki University of Technology P.O. Box 3000, FIN-02015 HUT, FinlandNicklas.Beijar@hut.fi

[13] Mix-Zones for Location Privacy in Vehicular Networks Julien Freudiger, Maxim Raya, MárkFélegyházi,PanosPapadimitratos and Jean-Pierre HubauxEPFL, Switzerlandfirstname.lastname@epfl.ch

[14] IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 13, NO. 3, SEPTEMBER 2012 1099 We Can Deliver Messages to Far Vehicles KhaleelMershad, Hassan Artail, and Mario Gerla

[15] International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 9, September 2013 www.ijsr.netSecurity in Vehicular Ad Hoc Networks through Mix-Zones Based Privacy1S. Kavitha, 2M.ParveentajResearch Scholar, Sri JayendaraSaraswathyMahaVidayala College of Arts and Science, Coimbatore- 05, India M.C.A., ADCA, M. Phil, Assistant Professor,Sri JayendaraSaraswathyMahaVidayala College of Arts and Science, Coimbatore- 05, India