ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review on Security Issues in VANET

Namarpreet Kaur
M. Tech Computer Science
Punjab Technical University, India

Aman Arora
H.O.D, M.Tech Computer Science,
Department of CSE,India

Abstract: Vehicular ad hoc networks (VANETs) are receiving increasing attentions from academia and deployment efforts from industry, due to the various applications and potential tremendous benefits they offer for future VANET users. Safety information exchange enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging, and thus, plays a key role in VANET applications. In a VANET, vehicles will rely on the integrity of received data for deciding when to present alerts to drivers. The communication between car to car, car to roadside unit done through wireless communication. That is why security is an important concern area for vehicular network application. For authentication purpose so many bandwidth is consumed and the performance becomes low. In VANET some serious network attacks such as man in middle attack, masquerading is possible. In this paper we are going to throw some light on the previous researches done in this area and will compare the various drawbacks of these researches. After that we are giving different issues on VANET and finally conclude with proposed algorithm.

.

Keywords: Security,Road side unit(RSU), Base Station unit (BSU) , Network Attack , Bandwidth

I. INTRODUCTION

Vanet – Vehicular Ad-Hoc Network is the network in which communication has been done in between road side units to cars , car to car in a short range of 100 to 300 m Existing authentication Protocols to secure vehicular ad hoc network raise challenges such as certificate distribution and communication Bottlenecks .Vehicular ad-hoc network receiving increase attention from academia and industry due to many beneficial futures it provided to future vanet users .Safety information exchange enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging, and thus, plays a key role in VANET applications . The communication between car to car, car to roadside unit done through wireless communication That is why security is an important concern area for vehicular network application. [1] A vehicular Ad hoc network (VANETs) can be used as an alert system. By this we get the alert about the traffic jam. It helps to create balance in traffic load to reduce travelling time. This system is also useful to broadcast emergency signal to the driver of the vehicle behind the accident. It also helps to send message to ambulance and traffic police in the case of traffic emergency[2].The no of features provided by Vanet is failed if we don't consider security and privacy into consideration. In security and privacy consideration the most important is message authentication but in this sometimes a large no of messages has been received by one vehicle results in message overhead thus a new technique is proposed called Client co-operative Authentication scheme in order to reduce authentication overhead on individual vehicle and shorten authentication delay.[3]

A. Security Architecture

All Generally includes use of public key signatures. In a public key infrastructure, certificate authorities(CAs) binds between public keys and the nodes. security and privacy are two critical concerns for the designers of VANETs that, if forgotten, might lead to the deployment of vulnerable VANETs. Unless proper measures are taken, a number of attacks could easily be conducted, namely, message content modification, identity theft, false information generation and propagation, etc. The following are examples of some specific attacks .

1. If message integrity is not guaranteed, a malicious vehicle could modify the content of a message that is sent by another vehicle to affect the behavior of other vehicles.

By doing so, the malicious vehicle could obtain many benefits while keeping its identity unknown. Moreover, the vehicle that originally generated the message would be made responsible for the damage caused.

2. If authentication is not provided, a malicious vehicle might impersonate an emergency vehicle to surpass speed limits without being sanctioned.

3. A malicious vehicle could report a false emergency situation to obtain better driving conditions (e.g., deserted roads), and if non-repudiation is not supported, it could not be sanctioned even if discovered.

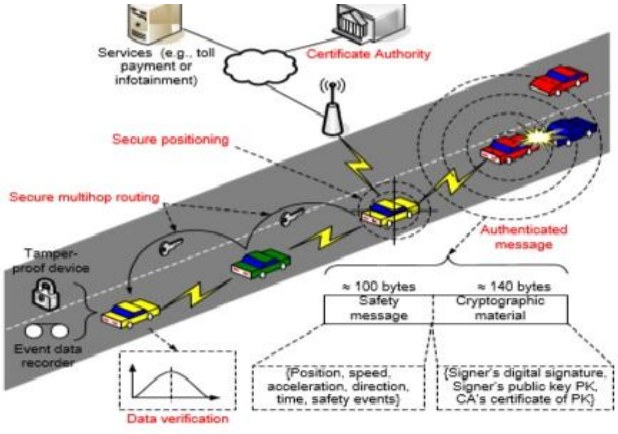


Fig.:1 General Security Architecture [1]

B. Attacks Or Threats Occurs in a Vanet

Several types of attacks have been identified and classified on the basis of layers used by the attacker. At the physical

and link layer, an attacker can disturb the network system by overloading the communication channel with useless messages. An attacker can inject false messages or rebroadcast an old message also. Some attackers can tamper with an OBU or destroy an RSU. At network layer, an attacker can insert false routing messages or overload the system with routing information. Privacy of drivers can be disclosed by revealing and tracking the position of drivers. Some of these attacks are briefly explained subsequently**.**

a. **Sybil Attack** :- In Sybil attack a malicious vehicle creates a large number of false identities in order to take over the control of whole VANET & inject fake information in the network to harm the legitimate vehicles. Sybil attack puts a great impact on the performance of the VANET by creating an illusion of existence of multiple vehicles in the network. The impact of this attack is that after spoofing the identities or positions of other vehicles in vehicular network, this attack may lead to other types of attack. Figure 7 illustrates a Sybil attack in which a malicious vehicle creates a number of false identities of many vehicles & produces an illusion of extra number of vehicles on the road.[5]

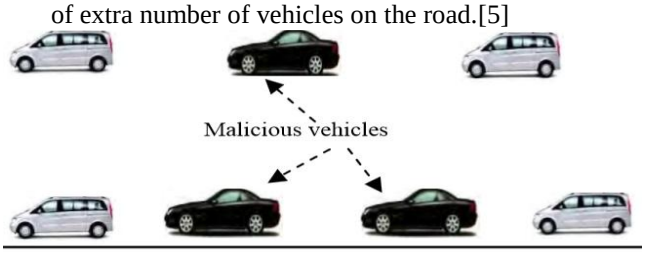


Fig.:7 Sybil Attack[5]

b. **Bogus Information**:- In this case, attackers are insiders, rational, and active. They can send wrong information in the network so that it can affect the behavior of other drivers. For example, an adversary can inject wrong information about a nonexistent traffic jam or an accident diverting vehicles to other routes and freeing a route for itself.[4]

c. **ID Disclosure**:- An attacker is insider, passive, and malicious. It can monitor trajectories of a target vehicle and can use this information for determining the ID of a vehicle.[4]

d. **Denial of Service (DoS) Attack** Denial of Service (DoS)[5] attack can be done by the network insiders & outsiders. An insider attacker may jam the channel after transmitting dummy messages & thus, stops the network connection. An outsider attacker can launch a DoS attack by repeatedly disseminating forged messages with invalid signatures to consume the bandwidth or other resources of a targeted vehicle. The impact of this attack is that, VANET losses its ability to provide services to the legitimate vehicles. Fig 2illustrates a Denial of Service (DoS) attack in which a malicious vehicle transmits a dummy message to an RSU & also to a legitimate vehicle behind it in order to create a jam in the network

.

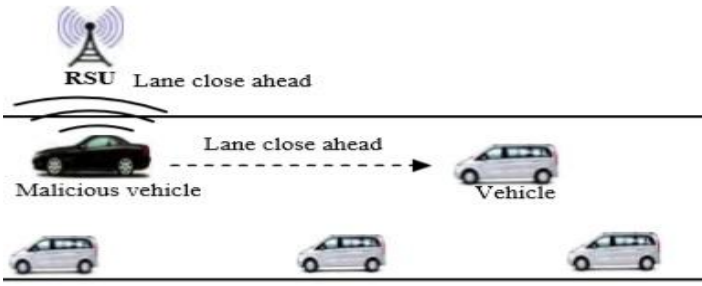


Figure 2: Denial of Service (DoS) Attack

Black Hole Attack :- In Black Hole attack [5], a malicious node pretends to have an optimum route for the destination node and indicates that packet should route through this node after transmitting the fake routing information. The impact of this attack is that the malicious node can either drop or misuse the intercepted packets without forwarding them. Figure 3 illustrates a Black Hole attack where a Black Hole region is created by a number of malicious vehicles & they refuse to broadcast the received messages from the legitimate vehicles to the other legitimate vehicles behind them. [5]

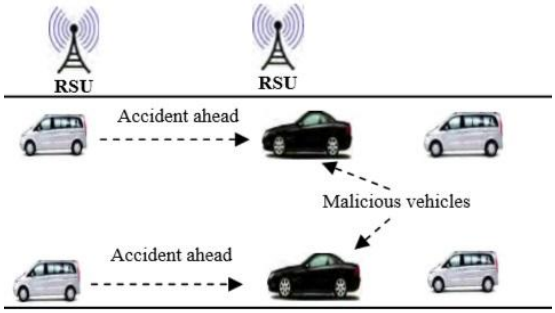


Figure 3: Black Hole Attack

a. **Sinkhole Attack** :- In Sinkhole attack a malicious vehicle broadcasts the fake routing information so that it can easily attract all the network traffic towards it. The impact of this attack is that it makes the network complicated & degrades the network performance either by modifying the data packets or by dropping them. Figure 5 illustrates a Sinkhole attack in which a malicious vehicle drops the data packets received from a legitimate vehicle & broadcasts fake routing information to the legitimate vehicles behind it.[5]

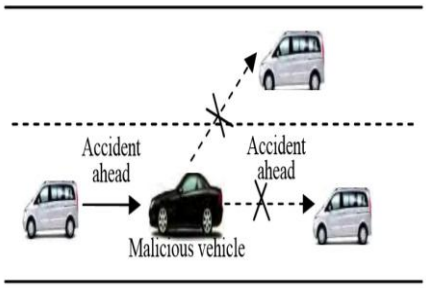


Fig.:5Sinkhole Attack[5]

C. **Intrusion Detection System** :- In general "Intrusion" means "action that compromise

integrity, confidentiality or availability of resource". "Intrusion Detection" means defensive strategy to protect the network systems against the Intrusion detected to minimize the damage or to launch counter blitzes.

An IDS is composed of three phases[6]: first is data collection then it is followed by analysis phase then finally phase that tries to counter the effect of intrusion.

IDS can be classified according to detection techniques used into three categories:

a. Signature based system [6]: Here, system cross verifies system behavior with the malicious behavior of node from the database –

b. Anomal**y detection system [6]:** Here, system monitors behavior of system from normal behavior and detects if behavior seems to be deviates from standard pre-established behavior of systemit triggers alarm**.**

c. **Specification based system [6]:** Set of protocols or condition of programs is pre-defined. Attack is alarmed ifprotocol or program condition is breached**.**

IDS architectures are classified into three categories:

a. **Stand-alone IDS :** Here in this architecture, every node individually collect data from other node and detects intrusion using local resources. Each node has no information of the potion of other nodes and no alerts cross the network. –

b. **Co-operative and distributed IDS :** Here, cooperation is established among the neighbors to detect intrusion. Neighboring nodes exchange alerts and regarding information. –

c. **Hierarchical IDS :** To overcome the lack of cooperation among different IDS approaches for ad hoc networks, this approached was proposed as here, network is divided into set of groups (clusters) contain leader in each cluster. Hierarchical IDS try to reduce cooperation among the nodes[6]

D. Existing Detection Mechanism For Attacks in Vanet[7]

In our existing work in the first time the user or the vehicle which should register with the near by Road Side Unit(RSU) by means of giving username and password. The user send the hello packet(username) to the RSU then the RSU prepares the users' interest like web pages, certain news, traffic information in certain areas etc. RSU assign new pseudonym to the user and also it contact the Trusted Authority(TA) and provide the key called as master key(Km). Those should be given in the form of ID packet to the user. The ID packet consists of username and pseudonym. Then the user send the identity packet which consist of username, password and secret key(Kc) to the RSU. Both the packets will beencrypted by using Km. RSUauthenticates the User and it should fetch the user credentials from the database by using Kc. RSU again contact the TA and provide the new key called session key(Ks). Then the RSU sent the packet key packet which have Ks. At last the acknowledgment is sent from the user to the RSU and also request for data is also sent then the reply is to be get back from the RSU to the Vehicle. In general, the vehicle should register with the near by road side unit in the first time of entering the range then if the vehicle want to get the data from the RSU at the time authentication will be performed. If the authentication is successful then the data has to be provided otherwise the the data or node is blocked**.** The main problems in our existing detection mechanism are

a. It uses heavy weight protocol.
b. The time consumption will be more.
c. If more users will be connect to single RSU overhead will be more.
d. It should not provide the security to insider attacks.[7]

E. Routing Protocols in Vanet [8]

In VANET, the routing protocols are classified into five categories**:.**

a. Topology Based Routing Protocols These routing protocols use links information that exists in the network to perform packet forwarding. They are further divided into Proactive, Reactive & Hybrid Protocols**.**

a.a Proactive routing protocols: The proactive routing means that the routing information, like next forwarding hop is maintained in the background irrespective of communication requests. The advantage of proactive routing protocol is that there is no route discovery since the destination route is stored in the background, but the disadvantage of this protocol is that it provides low latency for real time application. The various types of proactive routing protocols are: FSR, DSDV, OLSR, CGSR, WRP, and TBRPF.

a.bReactive/Ad hoc based routing: Reactive routing opens the route only when it is necessary for a node to communicate with each other. Reactive routing consists of route discovery phase in which the query packets are flooded into the network for the path search and this phase completes when route is found. The various types of reactive routing protocols are AODV, PGB, DSR, TORA, and JARR.

a.c Hybrid Protocols: The hybrid protocols are introduced to reduce the control overhead of proactive routing protocols and decrease the initial route discovery delay in reactive routing protocols. The various types of hybrid protocols are ZRP, HARP.

b. Position Based Routing Protocols Position based routing consists of class of routing algorithm. They share the property of using geographic positioning information in order to select the next forwarding hops. Position based routing is broadly divided in

two types: Position based greedy V2V protocols, Delay Tolerant Protocols

c. **Cluster Based Routing** Protocols Cluster based routing is preferred in clusters. A group of nodes identifies themselves to be a part of cluster and a node is designated as cluster head will broadcast the packet to cluster. Good scalability can be provided for large networks but network delays and overhead are incurred when forming clusters in highly mobile VANET. The various Clusters based routing protocols are COIN, LORA-CBF, TIBCRPH, and CBDRP.

d. **Geo Cast Routing Protocols** Geo cast routing is basically a location based multicast routing. Its objective is to deliver the packet from source node to all other nodes within a specified geographical region (Zone of Relevance ZOR). The various Geo cast routing protocols are IVG, DG-CASTOR and DRG. [8]

F. Authentication Scheme in Vanet

Before discussing Authentication Scheme we first discuss Security necessities in vanet

The security design of VANET should guarantee following:

1. Message Authentication, i.e. the message must be protected from any alteration.

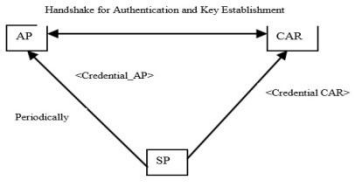
2. Data integrity does not necessarily imply identification of the sender.

3. Entity Authentication, so that the receiver is not only ensured that sender generated a message, in addition has evidence of the liveness of the sender.

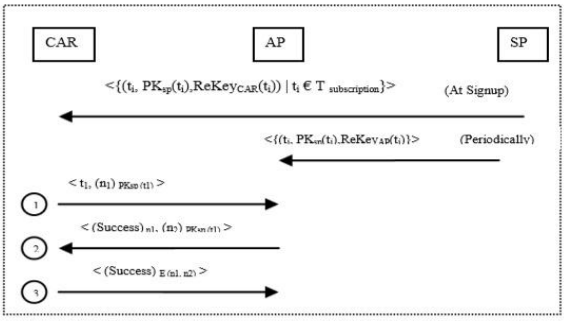
4. Conditional Privacy must be achieved in the sense that the user related information, including the driver's name, the license plate,

5., message alteration, and eavesdropping, [9]

Scheme :- The scenario for VANET communication we consider in this paper includes communicating entities of the service providers (SP), the cars, and the access points (AP) operated on behalf of service providers. The SPs and the APs can communicate with each other by some application-layer proprietary protocols via Internet. The APs are deployed along the roadside with reasonable wireless coverage to facilitate communication. A car typically belongs to one wireless network service provider, and communicates with the APs for accessing the internet along the road it travels through. When it travels, it also roams into wireless coverage that provide by other authorities.[9]



G. **Proxy Re-encryption Technique** :- For the first step, the car sends an authentication request to the AP detected in its range. The request message just contains the time of request t and a random number n1: <t1,n1 >. After the AP receives this message, it compares the time t1 provided by the car to its own clock. If the time is considered to be within normal deviation, the access point sends a message back to the car. The message constitutes a new random number n2 encrypted by the public key of the service provider of the time slot corresponding to t1: < (n2) PKSP (t1) >. After the car receives the reply, it uses the re-encryption key corresponding to t1 to re-encrypt the message. The outcome is thus available for it to decrypt using its own private key, and the n2 is revealed. It then takes n1 and n2, combines them by some cryptographic algorithm E known to both parties to generate E (n1, n2), and uses it as a symmetric key to encrypt a success tag as the authentication proof.



The encrypted message is sent back to the AP separately, or the car can also choose to immediately start sending data packets, with the authentication proof piggybacked to the first data packet. After the AP verifies the message by decrypting it using E (n1, n2), a secure and trusted connection is established. The session key E (n1, n2) is used to secure the following data transmission. For the AP to show itself as authorized, it needs to answer a challenge just as it posts to the car. For this purpose the AP needs to get time-related re-encryption keys along with the SP's public keys from the SP in a periodic fashion. When the car initiates authentication request, besides the timestamp, the nonce n1 is encrypted by the current public key of the SP as a challenge. After the AP receives the request, it can use re- encryption to resolve the challenge. In the response message, besides the challenge message to the car, it includes the proof of re-encryption capability by a success tag encrypted using n1 as a symmetric key. The car can then use n1 to reveal the success tag

II. CONCLUSION

In this paper we compared various research papers on vanet to analyse the current drawbacks and objectives in the vanet research. We laid out the several drawbacks including

security and performance and several efforts are being undertaken to make vanet a reality. In future we would like to propose an algorithm that would enhance the performance with the maintenances of security using a light weight mechanism.Vehicular Ad Hoc Networks is an emerging and promising technology, this technology is a fertile region for attackers, who will try to challenge the network with their malicious attacks. This paper gave a wide analysis for the current challenges and solutions, and critics for these solution, we also proposed a new solutions that will help to maintain a securer VANET network, in the future work we want to expand our idea about certificates of the safety messages, how to be created, discarded, and verified and test it by simulation

.

III. REFERENCE

[1]. Ankita Agrawal1, Aditi Garg2, Niharika Chaudhiri3, Shivanshu Gupta4, Devesh Pandey5, Tumpa Roy6 , "Security on Vehicular Ad Hoc Networks (VANET)". International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 3, Issue 1, January 2013)

[2]. Saurabh Kumar Gaur, S.K.Tyagi, Pushpender Singh "VANET" System for Vehicular Security Applications". International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013

[3]. Xiaodong Lin, Senior Member, IEEE, and Xu Li, "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks". IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 7, SEPTEMBER 2013.

[4]. Mina Rahbari 1 and Mohammad Ali Jabreil Jamali 2,"EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET". International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[5]. Priyanka Sirola ,Amit joshi, Kamlesh C. Purohit, "An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs)". International Journal of Computer Science Engineering (IJCSE)ISSN : 2319-7323 Vol. 3 No.04 Jul 2014

[6]. Mr. RaviPatel1, Ms. Khushbu Shah2, "GLANCEover VANET, ATTACKS over VANET and their IDS approaches". IJIRT | Volume 1 Issue 2 | ISSN: 2349-6002, 2014

[7]. TamilSelvan1, Komathy Subramanian2, Rajeswari Rajendiran3, "A Holistic Protocol for Secure Data Transmission in VANET", ISSN (Print) : 2319-5940 ISSN (Online) : 2278-1021 International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, December 2013

[8]. Mushtak Y. Gadkari1, Nitin B. Sambre2 , "VANET: Routing Protocols, Security Issues and Simulation Tools", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 28-38

[9]. Surabhi Mahajan Prof. Alka Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks"International Journal of Computer Applications (0975 – 8887) Volume 1– No.20, February 2010

Short Bio Data for the Authors

Namarpreet kaur She obtained her B.Tech (computer science & engineering) from Sai College of Engineering and Technology, Manawala, Amritsar,Punjab, India, pursuing M.Tech (computer science & engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. Her area of interest is Vanet and Security threat in Vanet

Aman Arora is working as an Head of Department in Department of Computer Science & Engineering, Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. He obtained his B.Tech (computer science engineering) from Guru Nanak Dev University, Punjab, India, M.Tech (computer science & engineering from Guru Nanak Dev University, Punjab, India.