International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 3, Issue 7

Security Threats and its Solution for Vehicular Ad hoc Network: A Review

Mr. Trambak Pawar **Prof. AmitKumar Manekar**

***Abstract* — In Vehicular Ad hoc Networks (VANETs), integrity of data is important security concern for the inter-vehicle and vehicle to roadside communications. Vehicles and the information have to be protected from the attacks on their privacy and from the misuse of their private data which is shared over communication. Safety information exchange enables life-critical applications, like lane merging and the alerting functionality during intersection traversing. So security plays an important role in VANET applications. In a VANET, vehicles are rely totally on the integrity of received data as it is helpful for deciding when to send the alerts to drivers. The communication is done through wireless communication. That is why security is an important issue for vehicular network applications. In this paper, we address the security issues of networks and the threats which create overhead and decreases and slow down the performance of VANET also the solution for the attacks and threats .**

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. A VANET uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node,allowing cars around 50 to 250 meters of each other to connect and, in turn, create a network with a wide range. As car fall out of the signal range and drop out of the ad hoc network, other cars also join in then connect the other vehicles to one another so that the wireless ad hoc network is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. The world largest automotive companies promote this VANET technology like BMW, AUDI, Mercedes, FORD. Vehicular Ad Hoc Networks (VANETs) are important wireless communication paradigms. The System and infrastructure less nature of VANETs makes them suitable for collecting emergency data in disastrous areas. A critical issue in VANETs is how to reduce energy consumption and maintain a longer life time for nodes in VANET. Several energy-efficient schemes are proposed to resolve this issue. Recent studies demonstrate that network coding can achieves a lower energy consumption in VANETs. The energy saving comes from fact that less transmissions are required when in-network nodes are enabled to encode packets. Besides basic transmissions, energy consumption can also come from encryption and decryption operations at each node, as most VANETs need some level of protection on their content. For example, in a battle field, the data communicated between soldiers with mobile devices can be very sensitive, and should be kept confidential during transmissions. In fact, the information mixing feature of network coding provides an intrinsic security, based on which a more efficient cryptographic scheme can be designed. Vile la et al propose such a scheme, in which the source performs random linear coding on the messages to be sent and locks/encrypts the coding vectors using the symmetric key shared between it and all sinks, network coding can be performed directly on the encrypted coding vectors, without impacting the standard network coding operations.

II. VANET ARCHITECTURE

The VANET communication may be of 3 types-

1. Inter-vehicle communication

In this Inter vehicle communication system the communication is take place in between the vehicle to vehicle by creating the network. This is a temporary network which is having small range from 50 to 250 meters. The On Board Device is placed on the vehicle to connect the vehicles in the network.

2. Vehicle to roadside communication

This type of network the communication is established between Road Side unit (RSU) and vehicles for sharing of data. This type of network having one to many vehicles connected to RSU. The common example is the police station and the other small police vehicle.

3. Inter-Road Side Units communication

In this type of communication is take place between roadside unit and the base station. The roadside units i.e. RSU can work as router to the share the information to each other.

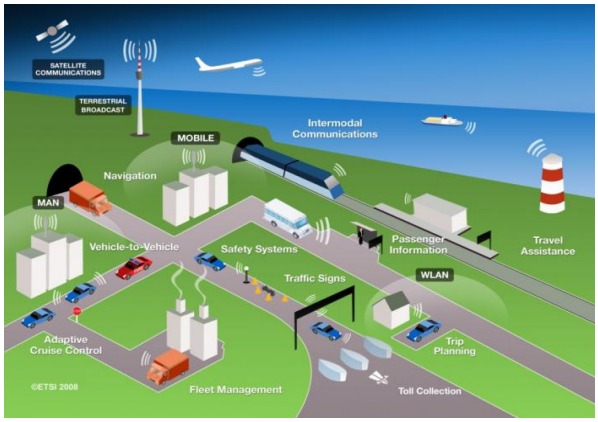

Fig.1 VANET example

III. SECURITY REQUIREMENTS

As the development in VANET technology there are various security and privacy challenges are also introduced as below.

a. Vehicle Identification and Authentication:

Vehicle Identification is that each participating node in network must have a different and unique identity. Though, identification itself does not imply that the entity proves that it is its actual identity this requirement is called entity authentication. In V2V warning propagation it needs identification to perform message routing and forwarding identifiers are essential to build

routing tables and sender authentication is needed for liability purposes.

b. Privacy Preservation:

Privacy preservation is critical for vehicles. Privacy is achieved when two requirements are satisfied intracability and invincibility. First Property states that vehicle's actions should not be traced (i.e. different actions of the same vehicle should not be related). On the other hand, second property imposes that it should be impossible for an unauthorized entity to link a vehicle´s identity with that of its driver/owner.

However, this privacy protection should be removed when required by traffic authorities. These requirements are present in all V2V communications in case of liability but not applied to I2V warnings, as the sender (i.e. the infrastructure) does not have privacy needs.

c. Non-repudiation:

Non-repudiation requirement assures that it will be impossible for an entity to deny having sent or received messages in the network. It is needed for the sender in V2V warnings. In this way, if a vehicle sends some data which is malicious, there is a proof for the liability purposes.

In case of the I2V and V2I warnings, the origin of the non-repudiation is needed, so fake warnings can be undoubtedly link with the sending node. Currently the receipt of Non-repudiation is not needed.

d. Confidentiality:

Confidentiality is assures that messages are read by authorized parties only. This is required only in the group communications, in which all the group members allowed to read such information. The other VANET settings transmit public information.

e. Availability:

Availability imposes that every node is capable of sending any information at any time. As most interchanged messages affect road traffic safety, the availability is most critical factor in this type of environment. To fulfill this requirements we can implement the communication protocols and mechanisms that can save as much as bandwidth and computational power also. In all communication patterns the availability can affects not only V2V communications, but also I2V communication.

f. Data Trust:

Data trust is globally related to the assurance of information, data integrity and accuracy. Data at stake must not be altered or modified and, more importantly, it should be truthful i.e. original messages send by sender. In the network potential crashes, bottlenecks and other traffic safety problems are caused by false and updated data. Data trust should be provided on all VANET communications as it is required for data sharing.

IV. THREATS TO VANET

Following are the threats to security in VANET. This includes various types attacks which tries to get access to VANET.

1. Black Hole Attack –

Nodes refuse to participate in the network or when an established node drops out. All network traffics is redirected to a specific node, which is not exist at all it will causes those data to be lost.

2. Malware –

Malware attacks, such as viruses in VANETs, have the potential to cause serious disruption to its normal operation. Malware attacks are more likely to be carried out by a malicious insider rather than an outsider. Malware attacks into the network when the cars VANET units and roadside station receive software updates.

3. Spamming –

The presence of spam messages on VANETs elevates the risk of increased transmission latency. The lack of centralized administration causes serious problems in VANET.

4. Selfish Driver –

Some drivers try to maximize their profit from the network by taking advantage of the network resources illegally. A Selfish Driver can tell other vehicles that there is congestion on the road ahead. They must choose an alternate route. Thus the road will be clear for him/her.

5. Malicious Attacker –

This kind of attacker tries to cause damage via the applications available on the vehicular network. In this, the attackers have a specific target, and they tries to access to the resources of the network. For instance, a terrorist can issue a deceleration warning, to make the road congested before detonating a bomb.

6. Denial of Services (DoS) –

In DoS attack the main objective is to prevent the legitimate user from accessing the services and from the resources. The attack occurs by jamming the network or channeling the system so that no vehicle can access it and aggressive injection of dummy messages. This avoids communication completely in the network which is devastating in real time applications.

Three different ways in which the attacker can achieve this are: In basic level, the attacker overwhelms the node resource so that the node becomes continuously busy and will not be able to process further. In extended level, the attacker jams the channel by generating high frequency in the channel. Thus the vehicle will not be able to communicate in the network and they drop down the packets.

The goal of is to overwhelm the node resources such that the nodes cannot perform other important and necessary tasks. It leads to Jamming the Channel and Distributed Denial of Services (DDoS).

7. Masquerading –

The attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives. Message fabrication, alteration, and replay can also be used towards masquerading. For example, assume an attacker tries to act as an emergency vehicle to defraud other vehicles to slow down and yield.

8. Global Positioning System (GPS) Spoofing –

The GPS satellite maintains a location table with the geographic location and identity of all vehicles on the network. An attacker fools vehicles into thinking that they are in a different location by producing false readings in the GPS positioning system devices. This is possible by the use of a GPS satellite simulator that generates signals that are stronger than those generated by the genuine satellite. This also affects routing in VANETs, especially geographical-based routing.

9. Pranksters –

People probing for vulnerabilities and hackers seeking to reach fame via their damage. For instance, a prankster can convince one vehicle to slow down the speed, and then tell the vehicle behind it to increase the speed.

10. Sybil Attack –

Attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicle Threats to Confidentiality les to tell other vehicles that there is jam ahead, and force them to take alternate route.

11. Timing Attack –

Time is a crucial aspect in any application so users need accurate information on right time without delay. In ITS safety applications time is also an important factor. In this attack without modifying the actual content of messages the attacker can add some time slots to create a delay in the message due to this user will not receive the message on the required time. ITS safety applications are time critical application which requires data transmission on time otherwise major accidents can happen.

12. Message Tampering –

Any node acting as a relay can disrupt communications of other nodes. It can drop or corrupt messages, or meaningfully modify messages. In this way, the reception of valuable or even critical traffic notifications or safety messages can be manipulated. An attacker can make this attack by transmitting false information into the network, the information may false or the sender can claim that it is somebody else.

13. ID Disclosure –

This attack discloses the identity of other nodes in the network and tracks the current location of the target node. A global observer monitors the target node and sends a 'virus' to the neighbors of the target node. As the neighbors are attacked, they take not only the specific information of the target node but also the target's current location. To track the cars this techniques use by travel companies or Rental car companies.

V. REVIEW WORK

In this section we analyze the many research papers to understand the existing solutions for the security problems in the VANET. Here are the some security solutions which avoid the attack to VANET.

Black hole attack:-

Exploit the sequence number of packet which is included in any packet header as well as find out the alternative route to reach at the destination node. This may create overload on network. Finding additional node increases unwanted parameters such as delay or cost of service.

Spamming:-

Privacy can be introduced by using Pseudonyms in the form of additional set of public/private keys which are given to the user which is changed frequently. These keys used for short period of time and do not contain any identity related information but it may be traced in liability related cases by using central authorities. The aim of using these pseudonyms is only to ensure that a vehicle cannot be tracked and a message cannot be attributed to its sender by other vehicles.

Selfish Driver:-

All vehicles must be trusted to follow the protocols specified by the application. One proposed solution to mitigate this attack is to verify the received data in correlation with the data received from other sources.

Malicious Attacker:-

The vehicles transmitting the messages must be an authenticated user registered to a Certificate Authority in order to uniquely identify the vehicle.

Denial of Services (DoS):-

If the private key shared between the Access Point and car only, the attacker cannot be able to exhaust the resource of the Access Points. Hence the delay in the request could also be prevented which usually occur in case of proxy-re encryption method of authentication.

Global Positioning System Spoofing:-

Global Navigation Satellite System (GLONASS): This is a radio-based satellite navigation system. This is the process with the global coverage and of the same precision as GPS.

Map Matching (using Geographic information systems): Where a vehicle's position is being identified using some fixed point in map. One can then calculate the distance after a vehicle has passed the point. The main disadvantage this system is the loss of accuracy.

Distributed Relative Ad-hoc positioning : In this system if any vehicle in the network has GPS, the other vehicles can easily calculate the distance using the GPS enable vehicle and simulate its position in global map. This is highly accurate and not required the infrastructure support.

Pranksters:-

To overcome this, the services provided by the RSU should be available to the vehicles whenever it is required.

Sybil Attack:-

A novel solution is that use on-board radar as the virtual eye of a vehicle. Although the 'eyesight' is limited because of the transmission range of radar, a vehicle can see surrounding vehicles as well as receive reports of their GPS coordinates. A vehicle can easily identify the accurate position of other vehicles and isolate malicious node.

Timing Attack:-

Using a globally synchronized time for all nodes and other is using nonce (Timestamp).

Message Tampering:-

Unauthorized manipulation must be detected, so that the content of the messages sent between the vehicles should not be changed.

ID Disclosure:-

The data being transmitted by the vehicles should be received by the registered vehicles only. Protocol should ensure that the vehicle ID is never revealed in the open. TPD ensures that the keys are not revealed to user.

CONCLUSION

In this paper we review various research papers on VANET to study the current drawbacks and objectives in the VANET security techniques. With the wireless technology becoming pervasive and cheap, VANET is going to turn out to be the networking platform that would support the future vehicular applications. We analyze the several different threats including security and performance and several efforts are being undertaken to make VANET a reality. We also provide the basic security solution for threats in VANET.

REFERENCES

[1] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin Shen, "Security in vehicular ad hoc networks,' Communications Magazine, IEEE , vol.46, no.4, pp.88-95, April 2008.

[2] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks", IEEE Trans. on Vehicular Technology, vol. 63, pp. 907-919, 2014.

[3] S. Dietzel, J. Petit, G. Heijenk, and F. Kargl, "Graph-based metrics for insider attack detection in VANET multihop data dissemination protocols", IEEE Trans. on Vehicular Technology, vol. 62, pp. 1505- 1518, 2013.

[4] Y. Peng and J. Chang, "A novel mobility management scheme for integration of vehicular ad hoc networks and fixed IP networks," *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 112–125, Feb. 2010.

[5] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," *IEEE Trans. Veh. Technol.*, vol. 58, no. 3, pp. 1454–1466, Mar. 2009.

[6] J. P. Hubaux, *et al.*, "The security and privacy of smart vehicles," *Security & Privacy, IEEE,* vol. 2, pp. 49-55, 2004.

[7] Security issues in VANET Rizwanul Karim Sakib

[8] VANET: Security attacks and its possible solutions – ajay rawat1, santosh sharma2, rama sushil3

[9] Security on Vehicular Ad Hoc Networks (VANET): A Review Paper Aditi Garg1, Ankita Agrawal 2, Niharika Chaudhiri3, Tumpa Roy4, Devesh Pandey5, Shivanshu Gupta 6

[10] Vehicular ad hoc networks (VANETS): status, results, and challenges - Sherali Zeadally · Ray Hunt · Yuh-Shyan Chen Angela Irwin · Aamir Hassan

[11] Threat Analysis and Defence Mechanisms in VANET Maria Elsa Mathew and Arun Raj Kumar.

[12] Vehicular Ad-Hoc Networks: An Information-Centric Perspective - Bo Yu Chengzhong Xu

[13] Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET) Ghassan Samara#1, Wafaa A.H. Al-Salihy*2, R. Sures#3

[14] Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks - Surabhi Mahajan, Prof. Alka Jindal

[15] Intelligent Transport Systems (ITS); Vehicular Communications; Geonetworking; Part 4: Geographical Addressing and Forwarding for Point to-Point and Point-to-Multipoint Communications, ETSI TS 102 637-4, 2011.

[16] E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, "Communication patterns in VANETs," IEEE Commun. Mag., vol. 46, no. 11, pp. 119–125, Nov. 2008.

[17] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in VANETs," in Proc. 3rd ACM Conf. Wireless Netw. Security, 2010, pp. 111–116.

[18] S. Yousefi, M. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): Challenges and perspectives," in Proc. 6th Int. Conf. ITS Telecommun., 2006, pp. 761–766.

[19] N. Banerjee, M. D. Corner, D. Towsley, and B. N. Levine, "Relays, base stations, and meshes: Enhancing mobile networks with infrastructure," in Proc. 14th ACM Int. Conf. Mobile Comput. Netw., 2008, pp. 81–91.

[20] K. L. Thng, B.-S. Yeo, and Y. Chew, "Performance study on the effects of cell-breathing in WCDMA," in Proc. 2nd Int. Symp. Wireless Commun. Syst., 2005, pp. 44–49.

[21] K. Doppler, M. Rinne, C. Wijting, C. Ribeiro, and K. Hugl, "Device-todevice communication as an underlay to LTE-advanced networks," IEEE Commun. Mag., vol. 47, no. 12, pp. 42–49, Dec. 2009.

[22] H. Hartenstein and K. Laberteaux, VANET: Vehicular Applications and Inter-Networking Technologies. Hoboken, NJ, USA: Wiley, 2010, ser. Intelligent Transport Systems.

[23] C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, and M. Mauve, "Data aggregation and roadside unit placement for a VANET traffic information system," in Proc. 5th ACMInt.Workshop VANET, 2008, pp. 58–65.

[24] T. Nadeem, S. Dashtinezhad, C. Liao, and L. Iftode, "TrafficView: A scalable traffic monitoring system," in Proc. IEEE Int. Conf. Mobile Data Manage., 2004, pp. 13–26.

AUTHOR'S PROFILE

Author's Name : Trambak Pawar
is a P.G. student of Computer Engineering at SITRC College of Engineering , Nasik under Savitribai Phule Pune University . He has completed his undergraduate Course of engineering from Savitribai Phule Pune University. His areas of interest include Network Security..