Survey On Security Requirements In Vehicular Ad-Hoc Networks

Ravneet Kaur, Dr. Jyoteesh Malhotra.

Department Of ECE, Guru Nanak Dev University, RC-Jalandhar, Punjab,
Email:neetarora58@gmail.com

ABSTRACT: This paper presents a literature survey on security issues in Vehicle Ad-hoc Networks (VANETs). Many researchers have done work on Mobile Ad-Hoc Networks (MANETs) where VANETs routing protocol has been taken as a new protocol. In VANET cars are allowed to talk to each other where a wireless device sends information to nearby vehicles. In this research we will discuss the security issues such as confidentiality, authenticity, availability and non-repudiation aimed to secure communication between V2V and V2I. Tabulated statistics on the relationship between security services versus the technique to encounter the possible attacks is shown. Five security services with security attacks and techniques have been presented. The new technique for VANETs can be build taking this paper as reference.

Keywords: Vehicle ad-hoc networks (VANETs), Smart city through VANET, ITS, Security.

1. Introduction

A Vehicular Ad-Hoc Network or VANETis a technology that has mobile nodes in a network for creating a network. VANET turns every vehicle into a wireless node, allowing vehicles to connect to each other which are 100-300 metres apart and a wide range of network is created. When a vehicle fall out from a signal range and drop out of the present network, other cars can join in to connect other vehicles so a mobile Internet can be created. An assumption is made that the first systems in which it is integrated are police and fire vehicles communicating with one another to provide safety. Mobile networks are very fast emerging for developing new and traditional applications. It has been characterized by rapidly changing topology, high mobility and one-time interactions.

A) VANET overview

A VANET is a type of MANET which provide communications between vehicles, among nearby vehicles, and road side unit. The goal of VANET is to provide security while communicating, and also safety to drivers and other road users. The special electronic device is connected to each vehicle which provides Ad- Hoc Network connectivity to the passengers. Each vehicle is equipped with this electronic device, which will be a node in the Ad-Hoc network and can receive and relay others messages though the network. Road sign alarms, warningbefore collision and traffic view will give the driver safety to reach the destination. Other services like multimedia and Internet connectivity facilities will be provided within the wireless coverage area of each vehicle. Some of the examples of VANET are automatic parking and toll collection. MANET differs from VANET as it can contain many nodes that have un-controlled movingpatterns. But since VANET is formed mainly by vehicles so movement of node isrestricted by factors like a road structure, traffic jams and traffic regulationsand rules. Because of this it can be said that VANET willbe supported by any fixed infrastructure known as road side units that provide various services and access tostationary networks. Vehicles in VANET tendto move in an organized way. Mainly controlling traffic, at road junctions, is a challenging task formetropolitan city planners. This situation can become hazardous if robots at robotcontrolled intersections got malfunction and at same time police are notavailable to control the traffic flow. Once in a while the robots got malfunction and the traffic police are not available to give hand signals to thehooting, yelling and cursing road users. The situation gets even worse if there is an accident along one way or a big truck has hada breakdown at the narrower intersection point. Long queuesof moving vehicle pileup and the situation can be very frustrating for one to usecertain notorious ways. Driving through a citywhere there are very narrow roads andinadequate parking area during peak hours is a disaster for time-savers and theimpatient. Intelligent Transportation System applies advanced technologies to surface transportation systems and is viewed widely as the solution to the traffic control problems that the 21st Century societies will face.

B) Intelligent transportation System (ITS)

VANET uses ITS for vehicular communication where each node acts as sender, receiver, and the router to broadcast information to the network.

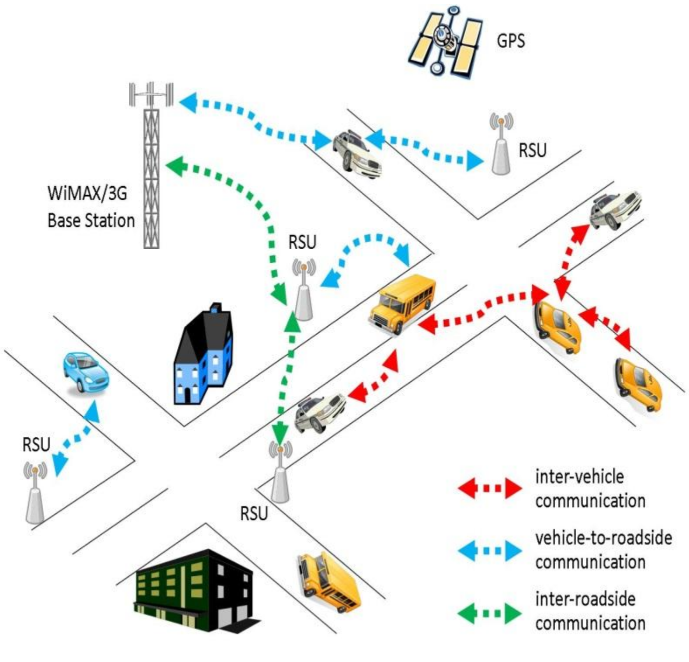

GPS
WiMAX/3G Base Station
RSU
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Figure 1: *VANET architecture*

An ITS as shown in figure 1 mainly consists of mobile nodes (e.g. Vehicles), fixed nodes (e.g. Roadside units) and certification authorities (CAs).Roadside units (RSUs) and CAs

Copyright © 2015 IJTEEE.

are fixed units and vehicles are mobile units. RSUs are static and connected to the backbone network for communication. The frequency and distribution of RSUs depend upon the communication protocol used which is divided into two types.

- Dense RSUs based where regions of RSUs are overlapped with each other.
- Sparse RSUs region where the ranges of RSUs do not overlap with each other.

Our proposed protocol uses sparse RSUs region. Nodes (vehicles) are equipped with On Board Unit, Trusted Platform Module, sensors, Global Position System device etc.On Board Unit helps in communication like vehicle to vehicle, vehicle to infrastructure, and routing based communication. Various sensors are used to measure status like fuel consumption and environmental condition like slippery road, safety distances.GPS is used to provide information about the vehicles current position and TPM provides secure communication. Road side units which are static acts as an intermediate between vehicles and CA and also transfer information about road conditions and traffic information to the vehicles(nodes) of its region.

C) VANET Applications

VANET play major role in two broad categories.

Safety Related Application-These applications are used to increase the safety on the roads. These applications can be categorised in following way.

i. Collision Avoidance: If drivers were aware half a second before collision, 60% accidents can be avoided.
ii. Traffic optimisation: signals like traffic jams, road accidents etc. can be send to the vehicles so that they can choose their alternate path and can save time.
iii. Cooperative Driving: Signals for traffic related warnings like speed warning on the curves, or while changing Lane etc. Such signals can co-operate the driver for the safe driving.

User Based Application- VANET can also provide following services to the user apart from safety:

i. Peer to peer application: Services like sharing music, vedios etc. among the vehicles in the network can be provided through these applications.
ii. Internet Connectivity: People always want to be on Internet all the time. Hence VANET can be used to provide the constant connectivity of the Internet to the users.
iii. Supplementary services: VANET can also provide other user based application such as payment service to collect the tall taxes, to locate the fuel station, parking slots, restaurant etc.

D) Characteristics of VANET

In addition to the similarities to ad hoc networks such as MANET, VANETs possess unique network characteristics that distinguish it from other ad hoc networks and influence research in this area.

i. High Mobility:The vehicles in VANETs usually are moving at high speed. This makes harder to predict its position and making protection vehicles privacy.
ii. Rapidly changing network topology: Network topology in VANETs tends to change frequently because due to random speed of vehicles, the position of the vehicle changes frequently.
iii. Unbounded network size:Network size in VANET is geographically unbounded because it can be implemented for single city, several cities or for countries.
iv. Frequent exchange of information:The vehicular ad-hoc networks motivate the nodes to gather information from the other nodes and road side units. Hence the information exchange among vehicles becomes frequent.
v. Wireless Communication: Vehicles are connected and exchange their information via wireless environment.
vi. Time Critical:The information in VANET which is transferred wirelessly must be delivered to the vehicles with in time limit so that a decision can be made without delay and perform action accordingly.
vii. Sufficient Energy:In VANET vehicles have no issue of energy and computation resources.

2. MOTIVATION

This paper has discussed the security issues such asconfidentiality, authenticity, availability and non-repudiation aim to secure communication between V2V and V2I. Privacy in vehicular networks has to deal with various kinds of threats that try to correlate received identifiers, or to correlate them to real-world identity, or to have position-identifier pairs. This paper discusses and analyse the possible of security attacks from various researchers that address security and privacy concern in VANETs. Thisstudy presents the relationship between securities services versus the technique proposed to encounter the possible attacks.

3. BACKGROUND

POSSIBLE ATTACKS IN VANETS

There are a numbers of possible attacks in VANETs which are listed below. The purpose of these attacks is to create problem on network for users to access the system or phishing some information.

A. Sybil Attacks

Sybil attack is the creation of multiple fake nodes broadcasting false information. In this, On Board Unit(OBU) installed in vehicle sends multiple copies of messages to other nodes and each message contains a different fabricated identity. The problem arises when attacker is able to pretend as multiple vehicles and reinforce false data. One of the interesting method proposed to encounter Sybil attack are based on statistical andprobability algorithm integrated with signal strength as an input data. Calculation is based on the difference between received signal strength and estimate signal strength is claimed by positioner. A framework to detect Sybil attacks in vehicles has been proposed using Certificate Authority (CA). The process involves two main steps, system initialization and attacks detection, in which public key and private key are used during system initialization to sign in the message.

B. Node Impersonation

It is an attempt by an attacker to sendmodified version of message and claims that the message comes from original node for the unknown purpose. A technique using greedy

Copyright © 2015 IJTEEE.

algorithms is used to detect and isolate node impersonation that is Detection of Malicious Vehicle (DMV). This scheme uses RSU to detect and observe an abnormal behaviour of nodes.If distrust value is higher than threshold value then the identity(ID) of the vehicle will be reported to the relevant Certificate Authority (CA) as malicious.

C. Masquerade attack:

A subscriber which is unauthorised may overhear the authentication messages on the air and try to have it authenticated to the access point by replaying them. The attacker can replay the car's authentication request by getting the car's public key and certificate.

D. ID Disclosure

Attackers sometimes disclose the identity of nodes in the network and track the location of the target nodes. Then it monitors the target nodes and sends a virus to the neighbours of the target nodes.When the virus attacks the neighbours of the attacker, then they take the ID of the target nodes as well as current location of target node. Various techniques have been proposed to deal with privacy one of them is identity disclosure which is used to prevent vehicle from being tracked by identifying keys that are used. The other is pseudonyms which use the Public Key Infrastructure to sign the message and this makes it difficult to track.

E. DoS and DDoS Attack

Attackers can initiate excessive authentication requests in order to exhaust the resources. One of the solutions would be to limit the number of authentication requests which can be processed in a unit of time period. This can guarantee that the server is not overwhelmed by Denial of service attack. But with this request could be delayed. Some trade-offs have to considered in order to implement such schemes.

SECURITY SERVICES

Security is an important issue for ad hoc networks,especially for security applications. To increase the security of an ad-hoc network, we need to consider the following attributes as criteria to measure security which includes availability, confidentiality, authentication and non-repudiation.

A. Availability

It deals mainly with network services for all nodes comprises of bandwidth and connectivity. Technique using group signature scheme has been introduced to encounter the availability issues, prevention and detection. This scheme focuses on availability of exchanging the messages between vehicles and road side units. The proposed technique still survives even when the attack causes network unavailability due to interconnection using public and private keys between RSUs and vehicles.

B. Confidentiality

Confidentiality ensures that unidentified entitiescan never have the access to the classified information in the network .Confidential information such as name, plate number and location can also be prevented from unauthorized access.Pseudonyms, is the most popular technique, which is used to preserved privacy in vehicular networks. Multiple key pairs with encryption will be given to each vehicle. Different pseudos' are used to encrypt messages and only relevant authority has access to it none of the vehicle node has been linked to it.When any earlier pseudo expires, vehicles needto obtain new pseudo from RSUs.

C. Authentication

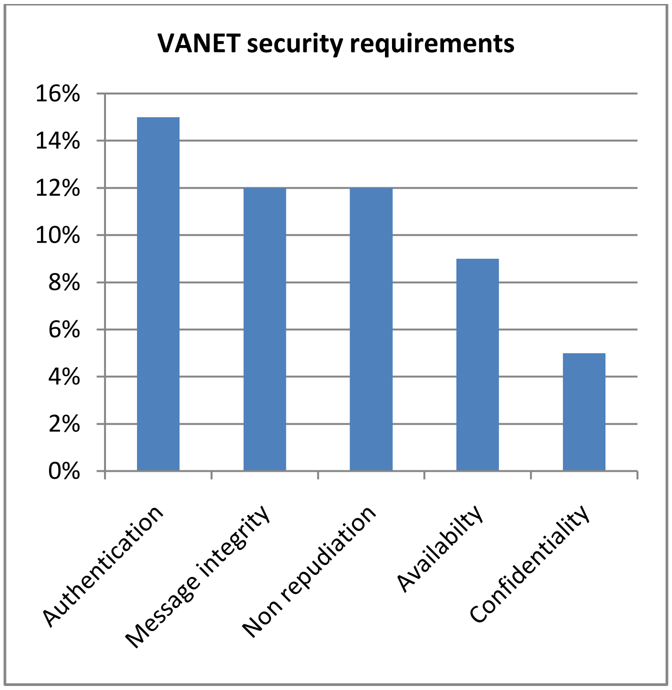
To verify the identity between vehicles and RSUs Authentication is required and also for the validation of integrity of the information exchange. It alsoensures that all the nodes are the authenticated vehicles to communicate within network. To establish connection between vehicles, RSUs and AS, public or private keys with certificate authority are proposed. On the other hand, as an authentication method, password is used to access to the RSUs and AS.

D. Integrity

Data integrity is very essential because it assures that the data received by nodes, RSUs and AS is similarto the data which has been generated during the exchanges of the message. Digital signature which is integrated with password access is used to protect the integrity of the message.

E. Non-Repudiation

Itensures the sender and receiver so that later on it cannot deny ever sending and receiving the message such as accident messages. Non-repudiation is also called audit ability in certain areas.



4. CONCLUSION

In this paper we have discussed various aspect of VANET like its architecture, application, and attacks. Also various characteristics of VANET have been listed which distinguished it from other networks like MANET. In this paper various attacks in VANET have been classified. Clear observation has been made that the classification helps to deal with different types of attack in VANET. Security challenge and security requirements have also been discussed. After survey we have found that attacks in multilayer like denial of services (DOS) and DDOS can prove hazardous for security system as well as authentication and Privacy are very big challenges.

Copyright © 2015 IJTEEE.

RREFERENCES

[1] B. Xiao, B. Yu, and C. Gao, “Detection and localization of sybil node in VANETs,” B. Proceedings of the 2006 Workshop on Dependability Issues in Wireless ad Hoc Networks and Sensor Networks, 2006, pp. 1-8.

[2] Y.Qian, N.Moayeri,”Design of Secure and Application Oriented Vanets”Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE,11-14 May 2008, Singapore.

[3] J. Jakubiak, Y. Koucheryavy,”State of the Art and Research Challenges for VANETs” Consumer Communications and Networking Conference, 2008, 5th IEEE, date: 10-12 Jan. 2008, pp: 912-916.

[4] M. Raya, J. Pierre, Hubaux,”Securing vehicular ad hoc Networks” Journal of Computer Security,vol.15, january 2007, pp: 39-68

[5] A.Weimerskirch, J.JHaas, Y.C.Hu, K.P.Laberteaux,”Data security in vehicular communication networks”, chapter no.09, pp309-310. Z. Tong, R. R. Choudhury, N. Peng, and K. Chakrabarty, “P2DAPsybil attacks detection in vehicular ad hoc networks,” IEEE Journal onSelected Areas in Communications, vol. 22, no. 3, 2011, pp. 582 - 594.

[6] S. Park, B. Aslam, D. Turgut, and C. C. Zou, “Defense against Sybil attack in vehicular ad-hoc network - based on roadside units support,”in Proceedings of the IEEE Military Communications Conference(MILCOM'09), Boston, MA, vol. 18, no. 21, October, 2009.

[7] W. W. Neng, M. H. Wueh, and M. C. We, “Anovelsecure communication schemein vehicular ad hocnetworks,” ComputerCommunications Archive, vol. 31, no. 12, pp 2827-2837, July 2008.

[8] D. Ameneh and P. R. A. Ghaffar, “Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks,” accepted for publication in Springer Multimedia Tools and Applications, SpecialIssue on Secure Multimedia Communications in VANET.

[9] L. Wenjia and J. Anupam, “Outlier detection in ad hoc networks using dempster-shafer theory,” 10th International Conference on Mobile Data Management'2009, pp. 112- 121, 2009.

[10] J. Guo, J. P. Baugh, and S. Wang, “A group signature based secure and privacy-preserving vehicular communication framework,”Proceedings of the Mobile Networking for Vehicular Environments(MOVE) workshop in conjunction with IEEE INFOCOM, Anchorage,Alaska, May 2007.

[11] F. A. Hawi, C. Y. Yeun, and M. A. Qutayti, The 4th International Conference on Information Tecnology, ICIT 2009, pp. 3-5 October, 2009.

[12] M. Ghosh, A. Varghese, A. Kherani, and A. Gupta, “Distributed misbehavior detection in VANETs,” WCNC 2009, IEEE WirelessCommunication and Networking Conference, Budapest, Hungary,IEEE Press, April 2009.

Copyright © 2015 IJTEEE.