International Journal of Multidisciplinary Research and Development

International Journal of Multidisciplinary Research and Development

Volume :2, Issue :5, 37-40
May 2015
www.allsubjectjournal.com
e-ISSN: 2349-4182
p-ISSN: 2349-5979
Impact Factor: 3.762

S. Radhika
M.Phil Research Scholar
Department of Computer Science Vivekanandha College for Women
Tiruchengode, Tamilnadu

S.Sindhu
M.Phil Research Scholar
Department of Computer Science Vivekanandha College for Women
Tiruchengode, Tamilnadu

Correspondence:
S. Radhika
M.Phil Research Scholar
Department of Computer Science Vivekanandha College for Women
Tiruchengode, Tamilnadu

A study on security challenges, issues and their solutions for vehicular ad-hoc network (VANET)

S. Radhika, S.Sindhu

Abstract
Vehicular Ad hoc Networks (VANETs) are the promising approach to provide safety and other applications to the drivers as well as passengers. It becomes a key component of the intelligent transport system. A lot of works have been done towards it but security in VANET got less attention. In this article, we have discussed about the VANET and its technical and security challenges. We have also discussed some major attacks and solutions that can be implemented against these attacks. We have compared the solution using different parameters. Lastly we have discussed the mechanisms that are used in the solutions.

Keywords: VANET, VANET architecture, ARAN, SEAD, SMT, NDM, ARIADNE

1. Introduction
Road traffic safety has been the challenging issue in traffic management. It can be achieved by exchanging the information of traffic environment among vehicles. All the vehicles are mobile in nature, hence a mobile network is needed which can be self organized and capable of operating without infrastructure support. VANET is an application of mobile ad hoc network. Wireless ad hoc network where vehicle to vehicle without any support of infrastructure.
Figure1.C2C-CC reference architecture
The ultimate goal of all works toward VANET is to provide road safety information among the nodes hence the frequent exchange of such type of data on the network clearly signifies the role of the security. Hence the security of the information in VANET is crucial. In this article we are going to discuss the security challenges and major attacks on VANET and also discuss the existing solution for these attacks.

2. Vanet Application and Characteristics:
The RSU can be treated as an access point or router or even a buffer point which can store data and provide data when needed. All data on the RSUs are uploaded or downloaded by vehicles. A classification of applications is also done by as Car to Car Traffic applications, Car to Infrastructure applications, Car to Home applications and Routing based applications.

2.1. Safety Related Application
These applications are used to increase the safety on the roads. These applications can be further categorized in following way.
1) Collision Avoidance: According to some studies, 60% accidents can be avoided if drivers were provided a warning half a second before collision. If a driver get a warning message on time collision can be avoided.
2) Cooperative Driving: Drivers can get signals for traffic related warnings like curve speed warning, Lane change warning etc.

2.2. User Based Application
A VANET can be utilized to provide following services for the user apart from safety:
1) Peer to peer application: These application are useful to provide services like sharing music, movies etc. among the vehicles in the network.
2) Internet Connectivity: People always want to connect with the Internet all the time. Hence VANET provides the constant connectivity of the Internet to the users.
3) Other services: VANET can be utilized in other user based application such as payment service to collect the tall taxes, to locate the fuel station, restaurant etc.

2.3 Commercial Applications
Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video.

1) Remote Vehicle Personalization/ Diagnostics: It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure.

2) Internet Access: Vehicles can access internet through RSU if RSU is working as a router.

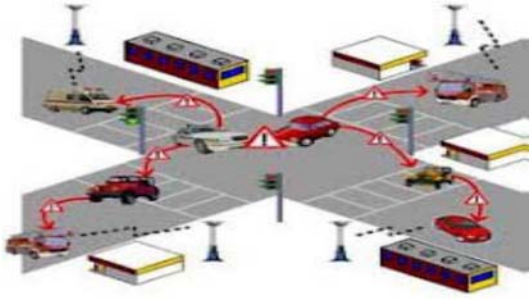

Fig 2: Emergency situation Notification.

3) Digital map downloading: Map of regions can be downloaded by the drivers as per the requirement before traveling to a new area for travel guidance.

3. Characteristics of Vanet
When equipped with WAVE (Wireless Access for Vehicular Environment, a novel type of wireless access dedicated to vehicle-to-vehicle and vehicle-to-roadside communications), in **it** forms a highly dynamic network. some characteristics of VANETs resembles with the characteristics of MANETs but there are specific features which can be categorized as follows:

1) High Mobility: The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy.

2) Unbounded network size: VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.

3) Frequent exchange of information: The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units.

4) Time Critical: The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

5) Sufficient Energy: The VANET nodes have no issue of energy and computation
resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power.

4. Challenging Issue in Vanet
Although the characteristics of VANET distinguishes it a different network but some characteristics imposes some challenges to deploy the VANET. These challenges can be categorized into following categories.

4.1. Technical Challenges
The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET. Some challenges are given below:

1) Network Management: Due to high mobility, the network topology and channel
Condition change rapidly. Due to this, we can't use structures like tree because these
Structures can't be set up and maintained as rapidly as the topology changed.

2) Security: As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied.

4.2. Social and Economic Challenges
Apart from the technical challenges to deploy the VANET, social and economical challenges should be considered. It is difficult to convince manufacturers to build a system that conveys the traffic signal violation because a consumer may reject such type of monitoring.

5. Security Issues in Vanet
VANET packet contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security

5.1. Security Challenges in VANET
The following list presents some security challenges:

1) Real time Constraint: VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used.

2) Data Consistency Liability: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency.

3) Low tolerance for error: Some protocols are designed on the basis of probability.
VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.

5.2. Security requirements in VANET
1) Authentication: Authentication ensures that the message is generated by the legitimate user. In VANET a vehicle reacts upon the information came from the other vehicle hence authentication must be satisfied.

2) Availability: Availability requires that the information must be available to the legitimate users. DoS Attacks can bring down the network and hence information cannot be shared.

3) Privacy: The privacy of a node against the unauthorised node should be guaranteed. Thisis required to eliminate the massage delay attacks.

5.3. Attackers on Vehicular Network

1) Insider and Outsider: Insiders are the authenticated members of network whereas
Outsiders are the intruders and hence limited capacity to attack.

2) Malicious and Rational: Malicious attackers have not any personal benefit to attack; they just harm the functionality of the network. Rational attackers have the personal profit hence they are predictable.

3) Active and Passive: Active attackers generate signals or packet whereas passive
attackers only sense the network.

5.4. Attacks in the VANET

To get better protection from attackers we must have the knowledge about the attacks in VANET against security requirements. Attacks on different security requirement are given below.

1) Impersonate: In impersonate attack attacker assumes the identity and privileges of an authorised node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the networkThey may be insider or outsiders. This attack can be performed in two ways:

i) False attribute possession:
ii) Sybil
2) Session hijacking: Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.

a) Eavesdropping is a most common attack on confidentiality. This attack is belongs to
Network layer attack and passive in nature. The main goal of this attack is to get access of confidential data.

b) Denial of Service: DoS attacks are most prominent attack in this category. In this attack the attacker prevents the legitimate user to use the service from the victim node.

2) Routing attack: Routing attacks re the attacks which exploits the vulnerability of
network layer routing protocols. In this type of attack the attacker either drops the packet
or disturbs the routing process of the network. Following are the most common routing attacks in the VANET:

a) Black Hole attack: In this type of attack, the attacker firstly attracts the nodes to
transmit the packet through itself. It can be done by continuous sending the malicious
route reply with fresh route and low hop count. After attracting the node, when the
packet is forwarded through this node, it silently drops the packet.

b) Worm Hole attack: In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the
Network from that point.This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries.

c) Gray Hole attack: This is the extension of black hole attack. In this type of attack
the malicious node behaves like the black node attack but it drops the packet selectively.

6. Solution of Previously Defined Attacks

There are many solutions provided to mitigate these attacks. We have taken five solutions that are most effective for above mentioned attack. Following are their descriptions:

6.1. ARAN (Authenticated Routing for Ad hoc network)

This is based on AODV but it prevents from attacks including spoofing. ARAN uses the public key cryptography and requires a certificate server whose public key is known to all nodes. A source node broadcasts the route discovery packet (RDP) to all its neighbours for route discovery.

6.2. SEAD (Secure and Efficient Ad hoc Distance Vector)

Distance Vector (DSDV) routing. SEAD supports the node which has limited CPUprocessing capability and protects from the DoS attack in which attackers attempts to consume excess network bandwidth. It uses destination-sequence number to avoid the long lived routing loop and also protects from replay attack as the destination-sequence number provide the freshness of the packet.

6.3. Ariadne

This approach is based on on-demand routing like DSR. It uses highly efficient symmetric cryptography. In this approach sender and receiver agrees on two keys say KSR and KRS for sender to receiver and receiver to sender respectively using MAC.

7. Conclusion

Security is the major issue to implement the VANET. Different types of attacks and their solutions are also discussed. Among all requirements authentication and privacy are the major issues in VANET. However confidentiality is not required in the VANET because generally packets on the network do not contain any confidential data.

References

1. S. Sesay, Z Yang and Jianhua He, "A survey on Mobile Ad Hoc Network", Information Technology Journal 3 (2), pp. 168-175, 2004
2. Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).
3. Yaseer Toor *et al*., "Vehicle Ad Hoc Networks: Applications and Related Technical issues", IEEE Communications surveys & Tutorials, 3rd quarter 2008, vol 10, No 3,pp. 74-88.
4. Y.- C. Hu and K. Laberteaux, "Strong Security on a Budget," Wksp. Embedded Security for Cars, Nov. 2006; http://www.crhc.uiuc.edu/~yihchun/

5. Maxim Raya e al., “The Security of Vehicular Ad Hoc Networks”, SASN’05, Nov 7 2005,
6. Alexandria, Verginia, USA, pp. 11-21
7. Hannes Hartenstein *et al*., “A tutorial survey on vehicular Ad Hoc Networks” , IEEE Communication Magazine, June 2008, pp. 164-171