Volume-4, Issue-1, Jan-2015 • ISSN No 2277 - 8160

Research Paper | Computer Science

AN OVERVIEW OF VEHICULAR AD HOC NETWORKS (VANET) AND ITS SECURITY ISSUES WITH POSSIBLE SOLUTIONS

V.Rajasekaran — Assistant Professor, Department of Computer Science, PSG College of Arts And Science, Coimbatore

J. Mohana Sundaram — Assistant Professor, Department of Computer Science, PSG College of Arts And Science, Coimbatore

ABSTRACT

The steady growth of automotive market and the rising demand for the safety of the passengers who in Vehicle, also driven by regulatory (governmental) domain, the potential of Vehicle-to-Vehicle connectivity is enormous. Emerging Vehicular Ad-Hoc Networks (VANET) has the potential to improve the safety and efficiency of future highways and state roads. While during with communication process security plays a vital role for VANET application. A vehicle in VANET is considered to be an intelligent mobile node which is able of communicating with its neighbors and other vehicles in the network. This paper analyzes the various security threats and the existing solutions to overcome these threat factors and show that there are active research efforts towards making VANETs a realism in the near future networking.

KEYWORDS : Security, Vehicular Ad Hoc Networks, Threats, Network Attacks.

***1.Introduction* :**

Vehicular networks represent a particularly new class of wireless ad hoc networks that enable vehicles to communicate with each other and/or with roadside infrastructure. VANET is a new standard that integrates Wi-Fi, Bluetooth, IRA, ZIGBEE and other mobile connectivity protocols. In recent years,With the sharp growth of vehicles on roads, driving becomes more challenging and dangerous .In a Record 1.2 million People worldwide are estimated to be killed each year on the roads . For this reason, nowadays the invest are heavily done in automobile industry to increase road safety and traffic efficiency, as well as to reduce the impact of transportation on the environment. VANETs have turned into an important research area over the last few years. VANETs are distinguished from MANET by their hybrid network architectures, node movement characteristics, and new application scenarios.

Characteristics

Drive behaviour, constraints on mobility, and high speeds create unique Characteristics in VANETs. These characteristics are as follows:

High mobility and Rapid changing topology: Vehicles move very fast and quick especially on highways. Thus, they stay in the communication range of each other just for several seconds, and links are recognized and broken fast. When the vehicle density is low or existing routes break before constructing new routes, it has higher probability that the vehicular networks are disconnected. So, the previous routing protocols in MANET are not suitable for VANETs.

Geographic position available: Vehicles can be operational with accurate positioning systems integrated by electronic maps. For example, GPS receivers are very popular in cars which help to provide location information for routing purposes

Mobility modelling and prediction: Vehicular nodes are usually embarrassed by prebuilt highways, roads and streets, so given the speed and the street map, the future position of the vehicle can be predicated. Vehicles move along pre- defined paths, this provides an opportunity to predict how long routes would last compared to arbitrary motion patterns like the random waypoint model .

Hard delay constraints: In VANETs applications, such as the collision warning or Pre-Crash Sensing, the network does not require high data rates but has hard delay constraints, and the maximum delay will be critical

No power constraint: Since nodes are cars instead of small handheld devices, power constraint can be neglected thanks to always recharging batteries.

VANET ROUTING Protocols

In VANET, the routing protocols are divided into five categories: Topology based routing protocol, Geo cast routing protocol, Position based routing protocol and Cluster based routing protocol, and Broadcast routing protocol. On the basis of application/area these protocols are characterized .

Topology Based Routing Protocols:

These routing protocols use links information For packet forwarding that exists in the network. They are classified into Proactive, Reactive & Hybrid Protocols.

i) Proactive routing protocols

This Routing Protocol income 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 destination route is stored in the background since there is no route discovery, but the disadvantage of this protocol is that it provides low latency for real time application. A table is built and maintained within a node. So that, each entry in the table shows the next hop node towards a certain destination. It also leads to the care of unused data paths, which causes the decrease in the available bandwidth. The various types of proactive routing protocols are: LSR, FSR.

ii) Reactive/Ad hoc based routing

This Protocol will perform only when it is necessary for a n ode to communicate with each other reactive routing opens the route. It preserves only the routes that are currently in use, as a outcome it reduces the burden in the network. Reactive routing involves of route discovery phase in which the query packets are submerged into the network for the path search and this phase confirms when route is found. The various types of reactive routing protocols are TORA, AODV, PGB, and DSR

Hybrid Protocols: To minimize the resistor overhead of proactive routing protocols and decrease the initial route discovery stick-up in reactive routing protocols, The hybrid protocols are introduced.

b) Position Based Routing Protocols This Routing protocol consists of class of routing algorithm. In order to select the next forwarding hops t hey share the property of using geographic positioning information. The packet is send without any map knowledge to the one hop neighbor, which is closest to destination. Position based routing is beneficial since no global route from source node to destination node need to be created and maintained.

c)Cluster Based Routing
Cluster based routing is favoured in clusters. A collection of nodes identifies themselves to be a part of cluster and a node is elected as cluster head will broadcast the packet to cluster. For the large networks good scalability can be provided but network delays and overhead are acquired when forming clusters in highly mobile VANET. In this Protocol virtual network infrastructure must be created through the clustering of nodes in order to provide scalability. The various Clusters based routing protocols are COIN and LORA_CBF

d) Broadcast Routing
This routing protocol is habitually used in VANET for sharing, traffic, weather and emergency, road conditions between vehicles and delivering advertisements and broadcasts. The various Broadcast routing protocols are BROADCOMM, UMB, V- TRADE, and DV-CAST.

e) Geo Cast Routing
Geocast routing is fundamentally a position based multicast routing. Its neutral is to distribute the packet from the source node to all other nodes within a specific geographical region (ZOR). To avoid unnecessary hasty reaction, these routing vehicles outside the ZOR are not alerted. A zone of forwarding (ZOF) is explained as the geographic area which vehicles in this area must deliver the packets to other ZOR vehicles.

3.Security Issues
Security is an issue that needs to be carefully assessed and addressed in the design of the vehicular

communication system. Several threats potentially exist, including fake messages causing disruption of traffic or even danger, compromising driver's private information, etc. Safety and traffic management need real time information and this carried information can affect life or death decisions.

Because VANET mobility is higher than MANET,
routing with capability of ensuring security in VANET is more problematic than Adhoc. Illegal collection of messages by eavesdropping and gathering of location information available through the transmission of broadcast messages. Location privacy and anonymity are important issues for vehicle users.

A secure system, besides the basic network nodes, will consist of a Vehicular Public Key infrastructure (PKI), a Secure Computing platform and various security mechanisms. Secure mechanisms comprise identity management using Electronic License Plates with certified public and private keys attached to the owner, Authentication and Integrity using Digital Signatures, Privacy using Pseudonyms, Pseudonym handling and Certification Revocation mechanisms.

4. SECURITY ATTACKS AND POSSIBLE SOLUTIONS IN (VANETS)
Vehicular ad hoc networks are also prone to several Security attacks. These Security can cause severe problems in the network and also poses some potential threats which can deteriorate their functioning and data privacy. The following section gives a general overview of Vehicular Communications Security attacks which are available in the VANET and it gives Solutions based on the existing solutions[2,4,7,8,9,10]. It gives the definition and the solution following it.

4.1 **Black Hole Attack** - Nodes refuse to participate in the network or when an established node drops out. All network traffics are redirected to a specific node, which does not exist at all that causes those data to be lost.

Soultion : Exploit the packet sequence number

included in any packet header. Find alternative route to the destination. This solution may impose overload to network. Finding additional node increases unwanted parameters such as delay or cost of service

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

Soultions: Privacy can be introduced by using Pseudonyms in the form of additional set of public/private keys which are given to the user which are used for a short period of time and changed frequently.

These keys do not contain identity related information but can be traced back to the owner in liability related cases with the help of central authorities.

The aim in using pseudonyms is to ensure that a vehicle cannot be tracked and a message cannot be attributed to its sender by other vehicles

4.3 **Selfish Driver :** Some drivers try to exploit their profit from the network by taking benefit of the network resources illegally. A Selfish Driver can tell other vehicles that there is cramming on the road

ahead. They must choose an alternate route. Thus the

road will be clear for him/her.

Solutions : All vehicles must be honest to follow

the protocols stated 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.

4.4 **Malicious Attacker -** This kind of attacker tries to aim damage via the applications available on the vehicular network. In many cases, these attackers will have definite targets, and they will have entrée to the resources of the network. For instance, a terrorist can issue a deceleration warning, to make the road congested before detonating a bomb.

Solutions : The vehicles transmitting should be an authenticated user registered to a Certificate Authority in order to uniquely identify the vehicle

4.5 **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.
- Drops 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):
Solution : If the private key shared between theAccess Point and car only, the attacker can never be able to exhaust the resource of the Access Point. Hence the delay in the request could also be prevented which usually occur in case of proxy-re encryption method of authentication

4.6 **Global Positioning System(GPS) Spoofing-** The

GPS satellite preserves a position table with the geographic location and identity of all vehicles on the network. An attacker can chump vehicles into thinking that they are in a different location by producing incorrect readings in the GPS positioning system devices. This is probable through the use of a GPS satellite simulator to generate signals that are tougher than those produced by the genuine satellite. It also affects routing in VANETs, especially geographical-based routing.

Solution: 1.) Global Navigation Satellite System

(GLONASS): This is a radio-based satellite navigation system. This is in process with global coverage and of the same accuracy as GPS, but the difficulties of GPS still hold good for GLONASS.

2.) **Map Matching (using Geographic information systems):** Where a vehicle's place is being recognized using some fixed point in map like "university library". One can then calculate the distance after a vehicle has passed the point. The main disadvantage is loss of accuracy.

3.) Distributed Relative Ad-hoc positioning: Here if any one of the vehicles has GPS, the others can comparative compute the distance using the GPS enable vehicle and pretend its place in global map. This requires no Infrastructure support. But it is extremely accurate.

4.7 **Pranksters-** People penetrating for faintness and hackers seeking to reach reputation via their damage. For instance, a prankster can persuade one vehicle to slow down, and tell the vehicle behind it to raise the speed.

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

4.8 **Sybil Attack** - Attacker generates huge number of pseudonymous, and rights or acts like it is more than a hundred vehicle Threats to Confidentiality less to express other vehicles that there is jam ahead, and force them to take alternate route.

Solution: A novel solution that uses on-board radar as the virtual 'eye' of a vehicle. Although the 'eyesight' is limited because a modest radar transmission range, a vehicle can see surrounding vehicles and receive reports of their GPS coordinates. By comparing what is seen to what has been heard, a vehicle can corroborate the real position of neighbors and isolate malicious vehicle

4.9 **Timing Attack -** Time is a crucial aspect in any

application so users need accurate information on right time without any delay. Time is also an important issue in ITS safety applications. In this attack attacker without manipulating the actual content add some time slot to create a delay in the message due to this user will receive the message after the required time. ITS safety applications are time critical application which requires data transmission on time otherwise major accidents can happen.

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

4.10 **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 incorrect information into the network, the information could be false or the transmitter could claim that it is somebody else.

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

4.11 **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. When the neighbors are attacked by the virus, they take the ID of the target node as well as the target's current location. Rental car companies are using this technique to track their cars

Soultion: The data being transmitted by the vehicles should be received by the registered vehicles only. Protocol should ensure that the vehicleID is never

revealed in the open.TPD ensures that the keys are not revealed to user

4.12 ***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.

Solution : Unauthorized manipulation must be detected and Message confidentiality should be implemented. .

4.13 ***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 may be introduced into the network when the cars' VANET units and roadside station receive software updates

Solution : To overcome this, all the services and software provided by the RSU should be Scanned and the Malware should removed.

4.14 **Brute force-**Brute force Safety connected information is critical in VANET. For secure VANET appropriate application of cryptographic algorithms and approaches are widely used to guard against the threat. The attacker can use brute force technique to break the cryptography key .

Solution: Brute force attack solution is proposed by Langley et al. . In this a secure authentication method which requires use of some unique identification for vehicles concatenated with some large random value and then hashed using some hash algorithm To deal with traffic analysis attack Cencioni et al. proposed VIPER: a vehicle-to infrastructure communication privacy enforce- ment protocol. It is resilient to traffic analysis attacks. In this vehicle will send their messages directly to RSU but to have vehicle acting as mix nodes.

***5. Conclusion*:**

This paper represents an overview of various Security issues in vehicular adhoc network. Various types of Threats in vehicular network has been identified and addressed. The above solutions for certain Attacks have to handle with a challenging environment including high mobility and hard delay constraints in thin and dense connected network. These solutions only cover a subset of all the Threats and are far from providing a comprehensive answer to the routing and security problems in VANETs.

REFERENCES

[1] VANETs: The Networking Platform for Future Vehicular Applications - Gayathri Chandrasekaran | [2] Security on Vehicular Ad Hoc Networks (VANET): A Review Paper Ankita Agrawal1, Aditi Garg2, Niharika Chaudhiri3, | Shivanshu Gupta4, Devesh Pandey5, Tumpa Roy6 | [3] Vehicular ad hoc networks (VANETS): status, results, and challenges - Sherali Zeadally • Ray Hunt • Yuh-Shyan Chen •Angela Irwin • Aamir Hassan | [4] Threat Analysis and Defence Mechanisms in VANET Maria Elsa Mathew and Arun Raj Kumar P. | [5] Vehicular Ad-Hoc Networks: An Information-Centric Perspective - Bo Yu Chengzhong Xu | [6] Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET) Ghassan Samara#1, Wafaa A.H. Al-Salihy*2, R. Sures#3 | [7] Overview of security issues in Vehicular Ad-hoc Networks José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda | [8] Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks - Surabhi Mahajan, Prof.Alka Jindal | [9] Security issues in VANET Rizwanul Karim Sakib | [10] VANET: Security attacks and its possible solutions – ajay rawat1, santosh sharma2, rama sushil3 | |