Security and Privacy in Vehicular Ad Hoc Network (VANET): A Survey

Rizwana Kallooravi Thandil
Assistant Professor
Sullamussalam Science College,
Areacode

ABSTRACT

Vehicular Ad-Hoc Network (VANET) which is an application of mobile area network(MANET) are one of the main areas of research since they are expected to greatly influence and improve safe driving and traffic conditions. Apart from the great benefits it offers, these networks are highly vulnerable to attacks. Due to this reason much attention is given to the security and privacy issues in VANETs. Security issues in Vehicular Ad-Hoc Networks (VANETs) are important because of its diverse implications in safety related and congestion avoidance applications. A lot of research works have been undergone to improve performance and security of this network. In this paper I review recent advances in some of the security proposals proposed by researchers in this area.

General Terms

Security, Privacy, Performance.

Keywords

VANET, security, privacy, communication, broadcast.

1. INTRODUCTION

The rapid advancement in wireless communication networks has made it possible for Inter-Vehicular Communications (IVC) and Road-Vehicle Communication (RVC) in Mobile Ad Hoc Networks (MANET).This led to the evolution of new type of MANET known as Vehicular Ad Hoc Network to improve road safety, better traffic conditions, efficient driving and infotainment.

Since VANET is an application of MANET every node can move freely within the available network and be in connection. Each node can communicate with other nodes and the node could be a vehicle or a Road Side Unit (RSU).

Now that the number of vehicles increased exponentially the death rate is estimated about 1.2 million people yearly worldwide, and millions of people get injured, moreover traffic congestion makes a huge wastage of time and fuel.

2. ARCHITECTURE OF VANET

The basic components of vehicular ad hoc network architecture are: On Board Unit (OBU), Road side Unit (RSU), Trusted Authority (TA) and Application Unit (AU).Each components are explained below.

2.1 On Board Unit (OBU)

An OBU is usually mounted on a vehicle used for exchanging information with Road Side Units or with other vehicles. It consists of a resource command processor (RCP).The resources may include a read/write memory, a user interface(UI), a specialized interface to connect to other OBUs and a network device for short range wireless communication based on IEEE 802.11p radio technology[1]. OBU may also include a network device for non-safety applications. The OBU connects to other nodes in the network through a wireless link based on the IEEE 802.11p radio frequency channel. OBUs are in charge of communicating with other nodes (OBU or RSU). It enables communication services to the Application Unit (AU) and redirects data from other OBUs on the network. The functions of OBU include wireless radio access, geographical routing, mechanisms to control network congestion, reliable message transfer, data security etc.

2.2 Road Side Unit (RSU)

These are gateways that allow vehicles to establish connection with internet. This is the stationary part of the network. The RSU is equipped with one network device for a dedicated short range communication based on IEEE 802.11.The main functions of RSU are as follows:

•Extending the network coverage of the Ad Hoc network and thereby enabling exchange of information between communicating OBUs and RSUs.

•RSU acts as a source of information.

•RSU helps the OBUs to get connected to internet.

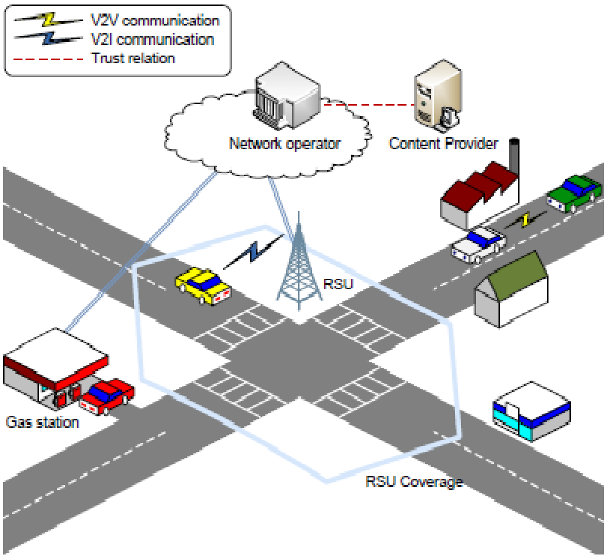

Figure: 1 Structure of VANET[17]

2.3 Trusted Authority (TA)

TA is the component which enables security in the network. For two vehicles in VANET to communicate securely, each must possess a copy of the other’s credentials in the form of a certificate. A universally-trusted Certificate Authority (CA), which provides vehicles with signed certificates, must revoke the certificates that it previously signed [14]. Typically, the CA adds the identification of the revoked certificate to a

Certificate Revocation List (CRL).2 The CA then publishes the updated CRL to all nodes, instructing them not to trust the revoked certificate. RSUs are used to broadcast this CRL to all mobile nodes as they pass. The main functions are as follows.

•Generate keys for encrypting the messages and sending the keys over a secure channel.

•Managing list of participating vehicles.

•Tracing the source of messages that creates problems in the network.

•Identifies attacks if any.

2.4 Application Unit (AU)

Application Unit is a device mounted inside the vehicle in the network. The device can contain applications for enhancing safety and to enable the OBU to connect to the network/internet.

3. COMMUNICATIONS IN VANET

Communication in VANET is over a wireless medium and is implemented with Dedicated Short Range Communications (DSRC) data link technology [3].VANET communication is categorized as follows:

•**Vehicle-to-Vehicle Communication (V2V):** In this type of communication vehicles within the network can exchange information regarding the traffic conditions, occurrence of accidents ahead if any, climate conditions etc.

•**Vehicle–to-Road Side Unit Communication:** Here vehicles communicate with fixed equipments installed along the roadside called Roadside Units to communicate with internet.

•**In Vehicle Communication:** The communication involves an OBU and multiple application units. The connection can be either wired or wireless. A communication link is established between an OBU and application unit for executing various applications provided by the application provider.

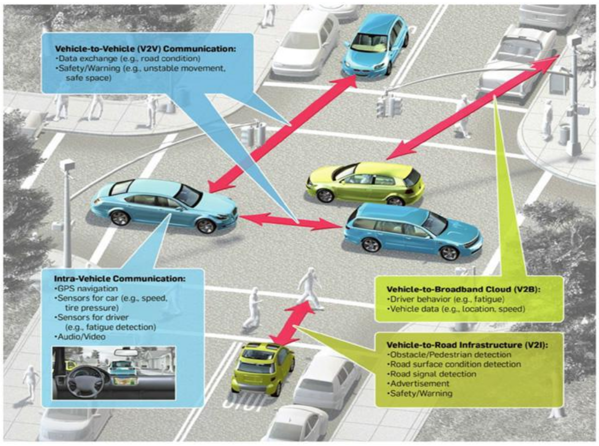
Vehicle-to-Vehicle (V2V) Communication:
•Data exchange (e.g., road condition)
•Safety/Warning (e.g., unstable movement, safe space)
Intra-Vehicle Communication:
•GPS navigation
•Sensors for car (e.g., speed, tire pressure)
•Sensors for driver (e.g., fatigue detection)
•Audio/Video
Vehicle-to-Broadband Cloud (V2B):
•Driver behavior (e.g., fatigue)
•Vehicle data (e.g., location, speed)
Vehicle-to-Road Infrastructure (V2I):
•Obstacle/Pedestrian detection
•Road surface condition detection
•Road signal detection
•Advertisement
•Safety/Warning

Figure: 2 Types of Communication in VANET [2]

4. APPLICATIONS OF VANET

Plenty of applications can be developed using VANET and it can provide a wide range of information to drivers and passengers. Applications of VANET can be classified into safety applications, on safety applications and commercial applications.

4.1 Safety Application

These applications deal with all safety related issues like road conditions, weather conditions, monitor other vehicles in the network etc. This application informs other vehicles in the network about these situations. The broadcasting feature of VANET will be used by the application for the purpose. Some of the safety applications are discussed below.

4.1.1 Slow /Stop Vehicle Advisor

A slow or a halted vehicle can send warning signals/messages to the surrounding vehicles in the network [1].

4.1.2 Post Crash Notifications

Vehicles met with accidents can broadcast messages about its position to neighboring vehicles. It can sent messages to the high way patrol for seeking further help[1].

4.1.3 Collision Avoidance

Improving collision avoidance application reduces road accidents to a great extent. By mounting sensors at the RSU information can be collected, processed and warning messages can be forwarded to the vehicles to avoid collision. Various strategies can be followed to avoid collision like warn vehicles about violating traffic signals, low bridge warning, wrong side driving alert etc.

4.1.4 Emergency Electronic Brake Light (EEBL)

This application is very crucial in crash prevention. First two cars involved in accident may benefit from EEBL but rest of the cars in the network can avoid the crash.

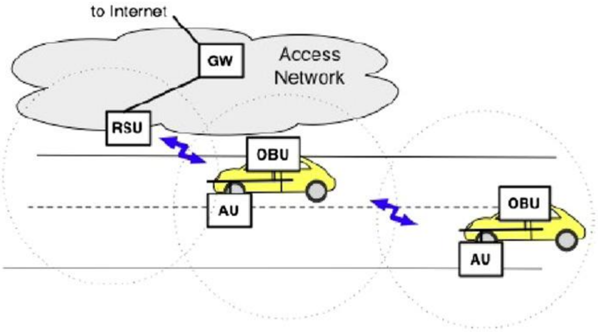

Figure: 3 RSU interfacing OBUs and internet connectivity [2]

4.1.5 Road Hazard Control Notification

This application informs the vehicles about the geographical features of the road such as having a sharp curve ahead or occurrence of a landslide etc. Sensors can be mounted on RSU to capture information about wild animals in the roads running through forests. There may be cases when dangerous animals cross the road or halt on road the information can be broadcast to the surrounding vehicles so that the vehicles can be prevented from moving ahead.

4.1.6 Cooperate Collision Warning

These applications warn vehicles heading towards collision.

4.2 Non Safety Applications

These applications are aimed to improve the comfort level of passengers and drivers. These applications help the travelers to locate the closest petrol pumps, hotels, theatres and search for the cost/price of each area. The passengers can even play online games and book rooms in hotels or book tickets for a movie. These applications help to collect toll on the go and gives information to locate free parking area. Travelers can obtain information regarding the availability of parking space with the help of these applications. The entire parking area in each city is split into a large number of circular zones. An RSU is placed at the center of each zone.

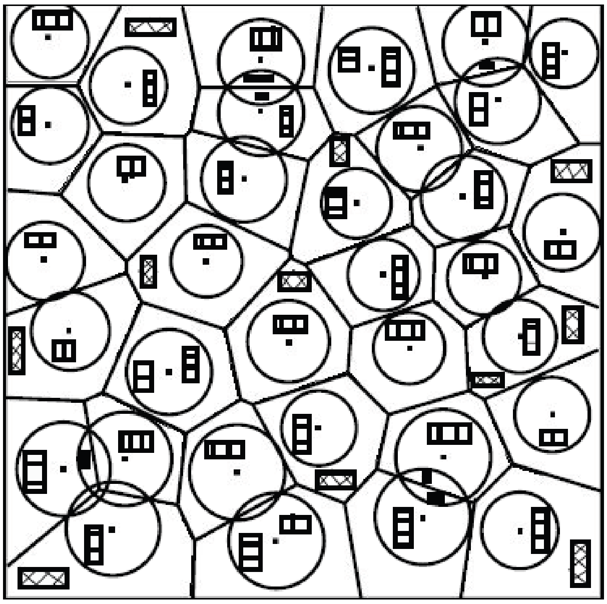

Figure: 4 illustration of the splitting the entire area into zones and Voronoi regions for each RSU [12].

4.3 Business Applications

These applications help the travelers to purchase goods and commodities online. These applications provide the facilities for online bank transactions and travelers can purchase anything online. A passenger can download a movie on the go or he can download the personalized vehicle settings and upload vehicle diagnostics to and from the infrastructure [1]

5. SECURITY ISSUES IN VANET

As any other network VANET is also susceptible to attacks. Some f the attacks are discussed below.

5.1 Denial of Service Attack

An intruder/attacker takes control of the network and block entire communication within the network. No nodes will be capable of executing any VANET applications.

5.2 DoS Resilience

Attacker can overwhelm the RSUs by exploiting the computational and communication resources by flooding with request messages.RSU wastes computational time by verifying certificates of false messages [12].

5.3 Message Suppression Attack

The attacker drops selected packets from the network which hold crucial information [3] thereby blocking these messages from reaching the receiver. The attackers aim at dropping the messages which holds information like registration, insurance and prevent the authorities from learning about collisions and thus avoids delivering collision reports to Roadside Units.

5.4 Message Injection

An intruder may try to modify the real data by injecting some additional data thereby altering the message. The attack of this category includes delay in transmission, resending the already sent data and as a result the attacker may give false information to the nodes. If the road is too busy and if there is a heavy traffic the message from RSU to nodes to take diversion will be altered by the attacker and may give information like the road is clear and there is no traffic congestion.

6. SURVEY ON SECURITY AND PRIVACY PROPOSALS FOR VANETs

Lot of attempts has been made by researchers in the security and privacy issues of VANET worldwide.

According to Bharathi Mishra [1] the concept of vehicular network was first proposed by a team of engineers from Delphi Delco Electronics Systems and IBM corporation in 1998.

Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux and Antonio Lioy [3] in 2007 proposed solutions to issues like *reducing* security overhead without weakening security, effect of the security and the pseudonym-based mechanismson safety applications and reducing the cost of providing vehicles with large numbers of pseudonyms meet the security and privacy requirements.

Tony K. Mak, Kenneth P. Laberteaux, Raja Sengupta [4]in 2005 formulated a protocol design for Multi Channel VANET Providing Concurrent Safety and Commercial Services. They proposed safety requirements while supporting non-safety communications with an 802.11-like radio.

Yi Yang, Rajive Bagrodia ,[5] Mobile Systems Lab, Computer Science Department ,University of California, Los Angeles in the year 2009 proposed Evaluation of VANET-based Advanced Intelligent Transportation Systems. The proposed method involved distributed simulation platform that integrates transportation simulation and wireless network, providing a user level simulation environment to evaluate the feasibility and performance limitations of VANETs. The proposed simulation platform facilitates the dynamic interaction between the two simulation domains, allowing runtime control of vehicles' behavior in the transportation simulation as they react in real time to information exchange in the simulated communication network. Case studies are conducted within the proposed simulation platform to evaluate the performance of Dynamic Route Planning when deployed in VANETs, using metrics collected at the transportation system level such as travel and delay time.

Nattiya Khaitiyakun and Teerapat Sanguankotchakorn [6] of Asian Institute of Technology Pathumthani, Thailand in the year 2014 proposed an analysis of data dissemination on VANET by using Content Delivery Network (CDN) technique. They proposed a method to apply the CDN technique for data dissemination from a single source node to multiple destinations in VANET environment.

Tracy Ann Kosa, Stephen Marsh and Khalil El-Khatib [7] published a paper on privacy representation in VANET in the year 2013.They proposed a framework for privacy representation. The framework allowed automated computation of privacy in VANET.

Tiffany Hyun-Jin Kim, Ahren Studer et.al [8] proposed a model in 2010 to distinguish spurious messages from legitimate ones. The proposed method will explore the information available in a VANET environment and assist vehicles to filter out malicious messages which are transmitted by a minority of misbehaving vehicles.

Jyoti Grover, Manoj Singh Gaur , Rakesh Kumar Tiwari and Vijay Laxmi [9] proposed a method in the year 2012 for detecting incorrect position information using speed and time span verification in VANET. They proposed a distributed solution to detect malicious nodes propagating incorrect position information within the network.

Christian Lochert, Björn Scheuermann, Christian Wewetzer, Andreas Luebke and Martin Mauve [10] proposed a method in the year 2008 for domain specific aggregation scheme to minimize the required overall bandwidth. They also proposed a genetic algorithm to identify good positions for static roadside units.

Lobna Nassar, Mohamed Kamel, Fakhri Karray Electrical & Computer Engineering [11], University of Waterloo proposed a method in the year 2014 for evaluating VANET information retrieval context aware systems using the average distance measure (ADM)

Ramu Panayappan and Jayini Mukul Trivedi[12] proposed VANET based method for parking facility. The security and privacy issues are also discussed in the paper.

Syed A. Khayam and Hayder Radha[13] Department of Electrical & Computer Engineering, Michigan State University, East Lansing, MI 48824, USA in the year 2004 presented a paper on Analyzing the Spread of Active Worms over VANET. They investigate the parameters which govern the spread of active worms over VANET. They analysed two cases of worm spread: 1) preemptive patching, where the number of patched VANET nodes remains constant; 2) interactive patching, where patching is performed during a worm outbreak.

Kenneth P. Laberteaux, Toyota Technical Center, Ann Arbor, MI, U.S.A REFERENCES and Jason J. Haas and Yih-Chun Hu, Dept. of Electrical and Computer Engineering, University of Illinois[14] — Urbana-Champaign, Urbana, IL, U.S.A. in the year 2008 proposed a method for node-to-node epidemic distribution of certificate revocation lists.

Jason J. Haas, Yih-Chun Hu and Kenneth P. Laberteaux proposed a lightweight mechanism for revoking security certificates appropriate for the limited bandwidth and hardware cost constraints of VANET in the year 2009 [15].The proposal includes a certificate organization method where certificates for a single vehicle are related by a single, secret revocation key. It also includes a mechanism for passing Certificate Revocation Lists (CRL) updates, rather than the entire CRL, in order to reduce the network.

Fatma Hrizi, Jérôme Härri and Christian Bonnet EURECOM, Mobile Communications Department Sophia-Antipolis, France in the year 2012 proposed a prediction model that can adapt to sudden traffic changes known as the Glow-worm swarm filter (GSF)[16].They developed a bio-inspired prediction model capable of detecting sudden traffic changes typically found in traffic safety contexts.

Ki-Eun Shin, Hyoung-Kee Choi and Jongmin Jeong proposed in the year 2009 a secure multimedia resource trading system in VANET, using a short-time self-certificate signature scheme which reduces certificate verification overheads [17].

Gongjun Yan, Gyanesh Choudhary, Michele C. Weigle, Stephan Olariu,[18] Department of Computer Science, Old Dominion University, Norfolk, VA 23529-0162, USA in the year 2007 proposed a method to enhance position security in VANET by using the on-board radar to detect neighboring vehicles.

Adetundji Adigun, Boucif Amar Bensaber and Ismail Biskri in the year 2012 proposed a protocol based on periodically communication’s pseudonym exchange in VANET[19].

7. CONCLUSION

Vehicular Ad Hoc Network will be reality in the near future. Apart from the services it offers it is highly vulnerable to attacks as I have cited earlier. Active researches should be done in securing VANET for completely enjoying the technology. This paper reviewed lot of papers and came to a conclusion that VANET has a lot of challenges when coming to reality. In my future work I will propose new solutions in securing the network.

8. REFERENCES

[1] Security in Vehicular Ad Hoc Networks:A Survey,Bharathi Mishra et al.

[2] A comprehensive survey on vehicular AdHoc network Saif Al-Sultan n, et.al,Journal of Network and Computer Applications

[3] Efficient and Robust Pseudonymous Authentication in VANET, Giorgio Calandriello et.al, Laboratory for Computer Communications and Applications ,EPFL, Switzerland.

[4] A MultiChannel VANET Providing Concurrent Safety

and Commercial Services, Tony K. Mak, Kenneth,et.al. University of California.

[5] Evaluation of VANET-based Advanced Intelligent Transportation Systems ,Yi Yang, Rajive Bagrodia ,[5] Mobile Systems Lab, Computer Science Department ,University of California, Los Angeles

[6] An Analysis of Data Dissemination on VANET by using Content Delivery Network (CDN) technique. Nattiya Khaitiyakun and Teerapat Sanguankotchakorn of Asian Institute of Technology Pathumthani, Thailand.

[7] Privacy Representation in VANET, Tracy Ann Kosa, Stephen Marsh and Khalil El-Khatib.

[8] VANET Alert Endorsement Using Multi-Source Filters, Tiffany Hyun-Jin Kim, Ahren Studer et.al.

[9] Detecting Incorrect Position Information using Speed and Time Span Verification in VANET, Jyoti Grover, Manoj Singh Gaur , Rakesh Kumar Tiwari and Vijay Laxmi, Malaviya National Institute of Technology,Jaipur

[10] Data Aggregation and Roadside Unit Placement for a VANET Traffic Information System, Christian Lochert, Björn Scheuermann, Christian Wewetzer, Andreas Luebke and Martin Mauve, Computer Networks Research Group Heinrich Heine University ,Düsseldorf, Germany.

[11] Evaluating VANET Information Retrieval Context Aware Systems using the Average Distance Measure ADM, Lobna Nassar, Mohamed Kamel, Fakhri Karray Electrical & Computer Engineering, University of Waterloo.

[12] VANET-Based Approach for Parking Space Availability, Ramu Panayappan and Jayini Mukul Trivedi, CyLab / Carnegie Mellon University.

[13] Analyzing the Spread of Active Worms over VANET, Syed A. Khayam and Hayder Radha, Department of

Electrical & Computer Engineering, Michigan State University, East Lansing, MI 48824, USA.

[14] Security Certificate Revocation List Distribution for VANET, Kenneth P. Laberteaux, Toyota Technical Center, Ann Arbor, MI, U.S.A REFERENCES and Jason J. Haas and Yih-Chun Hu, Dept. of Electrical and Computer Engineering, University of Illinois[14] — Urbana-Champaign, Urbana, IL, U.S.A.

[15] Revocation Mechanism for VANET Design and Analysis of a Lightweight Certificate, Jason J. Haas, University of Illinois at Urbana-Champaign Urbana Illinois, U.S.A. Yih-Chun Hu, University of Illinois at Urbana-Champaign Urbana Illinois, U.S.A. and Kenneth P. Laberteaux, Toyota Research Institute Ann Arbor, Michigan, U.S.A.

[16] Can Mobility Prediction be Compatible with Cooperative Active Safety for VANET?, Fatma Hrizi, Jérôme Härri and Christian Bonnet EURECOM, Mobile Communications Department Sophia-Antipolis, France.

[17] A Practical Security Framework for a VANET-based Entertainment Service, Ki-Eun Shin, Hyoung-Kee Choi and Jongmin Jeong, Sungkyunkwan University, Suwon, South Korea.

[18] Providing VANET Security Through Active Position Detection, Gongjun Yan, Gyanesh Choudhary, Michele C. Weigle, Stephan Olariu, Department of Computer Science, Old Dominion University, Norfolk, VA 23529-0162, USA, Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks.

[19] Proof of Concept of a Security Based on Lifetime of Communication's Pseudonyms for the VANETs, Adetundji Adigun, Boucif Amar Bensaber and Ismail Biskri, Proceedings of the second ACM international symposium on Design and analysis of intelligent vehicular networks and applications.