Delineating Security Threats and Solutions of Vehicular Ad-hoc Networks

Ramesh C. Poonia
Amity Institute of Information Technology
Amity University-Jaipur
Jaipur, India

Vaibhav Bhatnagar
Department of Computer Science
S.S. Jain Subodh P.G. (Autonomous) College
Jaipur, India

***Abstract*—Vehicular Ad-hoc Networks (VANETs) are the vital components of Intelligent Transport System. As far as Utility of VANET has concern, we can mainly classify into four groups like safety applications, commercial applications, convenience application and production applications. As all networks have some security threats, VANET also have some security threats of availability, authentication and driver's confidentiality. Black Hole Attack, Broadcast Tampering and Greedy Drivers etc. are the major issues of availability. Authentication has some serious issue of GPS spoofing and Sybil Attack. In this paper we are elaborating these threats and also their possible solutions. We are also evaluating the accuracy, robustness and efficiency of the already proposed solutions.**

Keywords-VANET; Black hole attack; DOS Attack;

I. INTRODUCTION *(HEADING 1)*

As we, all know rapid increment in the population leads to several hazards like Unemployment, Poorness and also rise in the heavy traffic. Vehicular Ad-hoc Network plays a vital road to control the traffic and the road safety. It is the main component of Intelligent Transport System and a subset of Mobile Ad-hoc Network, which is sufficient for communicating each other with or without fixed infrastructure. For implementing and learning various simulators are available like NS version-2 & 3, VanetMobiSim, MOVE, QualNet, NCTUns, TraNs, GlomoSim and etc. (1) (2) (3). We can implement VANETs in two ways:

- V2V (Vehicle to Vehicle Communication): In which two or more vehicles communicating each other without any backbone or a device. In the V2V communication, sensors are placed in the vehicles itself [3].
- V2I (Vehicle to Infrastructure Communication): In which vehicles are connected via backbone aliased as Road Side Units (RSU). In which sensors are placed in different locations like Red Light, Sign Boards and Bus Stops etc.

II. RELATED WORK

Association of Electronic Technology for Automobile Traffic and Driving (JSK) of Japan in 1980 was originated idea of the Inter Vehicular Communication System. In the year 1988, Josh Broch David et al. compare TORA, AODV, DSR and DSDV protocols on the basis of path optimization and packet delivery ratio and in 2009 QianFeng et al. with the help of NS-2 compared protocols AODV, DSR and OLSR and find that DSR is the most scalable routing protocol for VANETs. In 2007, Jerome Harri et al. explain the new simulator name as VanetMobiSim showed some new parameters are also essential for evaluation of performance (4)(5).

III. MAJOR SECURITY ATTACKS IN VANET

There are so many attacks on security implemented in VANETs. Some of them are following:

A. Denial of Service Attack:

On general concern Denial of Service attack is just sending to many fake requests on the server, so that server become hang or crash because of multiple and more frequent request just like in a class of 50 students everybody asking the doubt to available single faculty simultaneously as consequence faculty ran out of the class. Availability plays a huge role in VANETs because all vehicles depend and rely in the network only. The main target of the attacker in DOS Attack is the communication channel or media through which all the nodes are connected. Attacker jams this communication channel so that network is not available to the authenticate users [6]. In the figure1, we can see that Vehicle A jams the entire network of both V2V and V2I so that not all remaining nodes B, C, D can communicate among themselves.

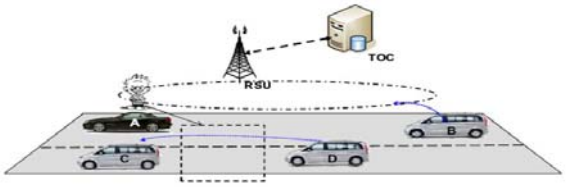

Figure 1. Overview of DOS Attack

Solution: Channel Switching is the methodology by which we can overcome DOS Attack. There are multiple channels provided by DSRC with range between 5.850 GZ to 5.925 GZ. Whole DSRC spectrum is clustered in seven segments or channels. These seven channels are categorized in two groups, one is safety related application and another one is non-safety

related application. CH 172, 178 and 184 are in safety related application and CH 174, 176, 180 and 182 are in non-safety application. If attacker jams or destroys one channel there is an option to switch to another channel so that the network is available to all nodes. Similar methodology of switching can be applied in technology. There are so many technologies for VANETs like Wi-Max, UMTS's Terrestrial Radio, Zig-Bee and Wi-Fi. They have a different Frequency Band, Data Rate and Range. According to the intensity of the attack, we can select our technology range higher or lower. Another solution can be having Multiple Radio Transceiver on OBU. With the concept Multiple Input Multiple Output OBU can have multiple Transceivers. If the DOS attack happens, OBU have option to switch into other Transceivers so the principle of availability can be maintained. Distributed DOS attack is enhanced but more dangerous attack compare to DOS attack. In DDOS attack there is more than one attacker that targets the single and common network in different time slots (7) (8).

B. *Blacke Hole Attack*

In General Black hole attack is a room or a place in the space in which force of gravity is so strong that even light is not able to pass through. In VANETs, Black Hole attack is created by a malicious node, which does not, passes the information or data to other nodes, sometimes-malicious node passes the fake or wrong information.

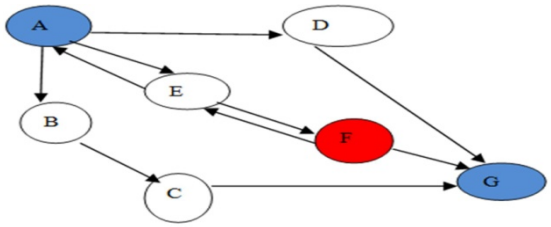

Figure 2. Overview of Black hole Attack

To understand in better way, we can take an example as per the above Figure 2. In the figure A is source node and G is destination node. As per the AODV routing first A will send RREQ message to its adjacent nodes B, E and D. Further they will also broadcast RREQ to their adjacent nodes. But in this scenario F is malicious nodes that does not pass RREQ message to G and in place pass RREP message acting as if it is the destination node. After the reply from F node A saves the route in its routing table for F instead of G. Whenever A need to send a message to G its message delivered only to F. F discards its Message which is sent for G or some time tamper the message hence a Black Hole attack is done (9).

Solution:

- By Generating Random Number: In order to verify the destination node, the source broadcast SRREQ message towards destination via different paths. It broadcast a random number X in all the networks. When destination receives the random number X, it immediately, reply another random number Y as SRREP. The sender will receive all SRREP packets & check the uniformity. If all the SRREP are uniform then the destination is verified otherwise node who sent different number will be consider as malicious (10).
- Packet Delivery Ratio: If there is a black hole in the networks then packet delivery ratio will be decreased because Black Hole node drops some of the packet coming from the source to authenticate destination. There also a high end to end delay of the node because malicious node will not check its route table and reply promptly (11).

C. *GPS SPOOFING*

In the GPS spoofing attack the attacker shows its false position. Attacker is on the other position and pretends to be on different position. He gets success to make all other vehicles fool with the help simulator of GPS satellite that spoofs its location to different location. This satellite simulator has more signal strength then original GPS satellite's signal (12).

Solution:

- Analyzing the Signal characteristics and Strength: GPS spoofing can be detected with deep analysis of signal strength. We can compare observed and expected strength of signals. Signal that are spoofed by GPS satellite simulator has relatively more magnitude then signals generated by legitimate GPS satellite for surface of the earth. Former perfection leads to confusion, if signal characteristics are too perfect that there is something wrong because in real scenario signal varies from satellite to satellite and changes time to time. Additional a very easy method by counting the number of satellite signals. A fake simulator transmits signal by multiple satellites near about 10 that is more than available real satellites.
- Analyzing time comparison: There is a constant time between simulator satellite and the receiver. But it is fluctuating if it is coming from real GPS satellite because satellite gets change after some period of times. Additionally trajectory cam also monitored by using separate Accelerometer of the receiver (13).

IV. Role of Cryptography for Preserving the Security in VANETs:

In VANET one message passes from one vehicle to another, important is this that message should be authenticated and should be visible or tampered by non-authenticate person. For this cryptography can be implemented. Cryptography is of two types i.e. Symmetric and Asymmetric. In symmetric, only one key is shared between sender and receiver to encode and decode the message.

Particulars	Asymmetric	Symmetric
Signature Generation	98	0.07

Signature Verification	2.9	0.035
Encryption	0	0.031
Decryption	0	0.165

TABLE I. COMPUTATIONAL TIME OF SYMMETRIC & ASYMMETRICCRYPTOGRAPHY

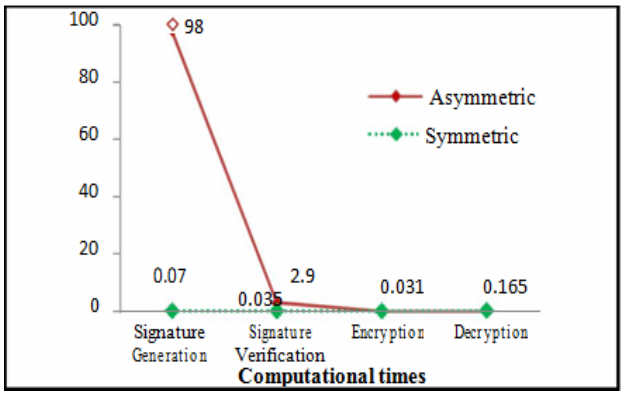

Figure 3. Computational time of Symmetric & Asymmetric Cryptography

Where in asymmetric key there are two public and private keys. Public key is used to encode the message and Private Key is used to decode the message. Digital Signature is best and most suitable for exchanging the message. An analogy based experiment performed for Asymmetric for Asymmetric and symmetric cryptography with following basis: 2400+ processor Athlon4, 768 MB RAM with algorithm of JRE. 1.5.0_06. The parameters on the basis are Signature Generation and Verification Encryption and Decryption. They are measured in time with ms unit. In the above table we have taken parameters of computational times namely Signature Generation, Signature Verification, Encryption and Decryption. Their Bandwidth Over Head is measured in percentage. From the analysis as shown in Figure 3, we can conclude that Asymmetric Cryptographic Algorithm has highest Signature Generation in terms of ms unit, contrast to this signature verification, signature generation, Encryption & Decryption are merely equal (14).

V. CONCLUSION AND FUTURE WORK

The idea behind VANET is road safety, but if we integrate with Mobile Application it could be a boon for humanity. There are several problems in our practical life that can be solved by implementing the concept of VANET like Blood Availability Donor, Car Pooling application, Garbage Collector Application. In this paper we have analyzed that VANET have so many threats but there are lot of solution proposed by different researchers. At the last we analyzed that Asymmetric PKI is best suitable for message passing, but since it is heavy to apply we can use Symmetric PKI.

REFERENCES

[1] Janech, Jan, Anton Lieskovsky, and Emil Krsak. "Comparation of strategies for data replication in VANET environment." *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*. IEEE, 2012.

[2] Lobiyal, D. K. "Performance evaluation of realistic vanet using traffic light scenario." *arXiv preprint arXiv:1203.2195* (2012).

[3] Shastri, A., R. Dadhich, and Ramesh C. Poonia. "Performance analysis of on-demand Routing protocols for vehicular ad-hoc Networks." *International Journal of Wireless & Mobile Networks (IJWMN) Vol* 3 (2011): 103-111.

[4] Broch, Josh, et al. "A performance comparison of multi-hop wireless ad hoc network routing protocols." *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, 1998.

[5] Feng, Qian, et al. "A performance comparison of the ad hoc network protocols." *Computer Science and Engineering, 2009. WCSE'09. Second International Workshop on*. Vol. 2. IEEE, 2009.

[6] Feng, Qian, et al. "A performance comparison of the ad hoc network protocols." *Computer Science and Engineering, 2009. WCSE'09. Second International Workshop on*. Vol. 2. IEEE, 2009.

[7] Hasbullah, Halabi, and Irshad Ahmed Soomro. "Denial of service (dos) attack and its possible solutions in VANET." World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering 4.5 (2010): 813-817.

[8] Pathan, Al-Sakib Khan, Hyung-Woo Lee, and Choong Seon Hong. "Security in wireless sensor networks: issues and challenges." *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*. Vol. 2. IEEE, 2006.

[9] Alem, Yibeltal Fantahun, and Zhao Cheng Xuan. "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection." *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*. Vol. 3. IEEE, 2010.

[10] Lu, Songbai, et al. "SAODV: A MANET routing protocol that can withstand black hole attack." *Computational Intelligence and Security, 2009. CIS'09. International Conference on*. Vol. 2. IEEE, 2009.

[11] Sharma, Sheenu, and Roopam Gupta. "Simulation study of blackhole attack in the mobile ad hoc networks." *Journal of Engineering Science and Technology* 4.2 (2009): 243-250.

[12] Zeadally, Sherali, et al. "Vehicular ad hoc networks (VANETS): status, results, and challenges." *Telecommunication Systems* 50.4 (2012): 217-241.

[13] Warner, Jon S., and Roger G. Johnston. "GPS spoofing countermeasures." *Homeland Security Journal* 25.2 (2003): 19-27.

[14] Plößl, Klaus, and Hannes Federrath. "A privacy aware and efficient security infrastructure for vehicular ad hoc networks." *Computer Standards & Interfaces* 30.6 (2008): 390-397.