Implementation of Temporal Attacks in Vehicular Ad Hoc Networks

Nitesh Kr. Prajapati Jyoti Grover M.S.Gaur

Malaviya National Institute of Technology, Jaipur- India

ABSTRACT

Vehicular Ad Hoc Network (VANET) is vulnerable to temporal attacks in which a malicious node either impedes or delays the forwarding of critical safety messages received from neighboring nodes. It can also perform replay attack by sending the information of events occurred earlier. VANET applications are based on periodic exchange of safety packets. It is very important that all the safety packets are sent on time so that proper action should be taken. It is the responsibility of each node in VANET to forward the received safety packet to its neighboring nodes. Attacker node exploits VANET vulnerabilities and performs these attacks. We discuss these attacks in brief and analyze their impact on VANET performance through NCTUns-6.0 simulations. We also propose counter measures for these attacks.

Keywords- VANET, Packet Replay, Packet Delay, Packet Suppression, attack, simulation.

1. INTRODUCTION

Vehicular Ad Hoc Network (VANET) is an emerging technology where Vehicle to Vehicle (V2V) and Vehicle to Road side unit (V2R) communication is based on Dedicated Short Range Communication (DSRC) band [1]. VANET is needed for automated and Intelligent Transportation Systems (ITS). VANET communication is used to improve vehicle passenger's safety by means of inter-vehicle com- munication. In the case of an accident, inter vehicle communication can be used to warn other vehicles approaching the site.

VANET consists of two types of wireless communication devices – (a) On-Board Unit (OBU) and (b) Road Side Unit (RSU). OBUs are located inside the vehicles and RSUs form the infrastructure of the network. Due to ad hoc nature of VANET owing to moving vehicles, there are not any centralized servers. Vehicles are required to manage network themselves. A conceptual architecture of VANET is shown in Figure 1.

VANET is a mobile ad hoc network (MANET) but there are certain differences. Unlike MANET, movement pattern is restricted to certain routes as vehicles can move along the road only. As average vehicle speed is more in VANET, network partition is more frequent. VANET does not have energy constraints since they are connected to the vehicles electrical system. Although there is no centralized control, RSUs provide an infrastructure framework.

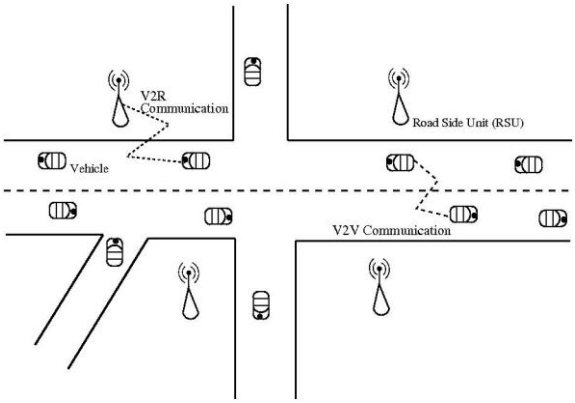

Figure 1. Architecture of Vehicular Ad Hoc Network

Due to the inherent wireless characteristics, VANET is open for malicious nodes that exploit its vulnerabilities. VANET vulnerabilities originate from its wireless nature and unencrypted exchange of information. Each node is free to access the communication channel. It is not protected against any physical disturbance. Safety messages are meant for all the nodes in VANET and sent in plain text form. It is ensured that everyone can understand the safety message broadcast in VANET. Likewise, everyone is free to send messages with any type of content.

Information security is an essential requirement for the effectiveness of inter-vehicle communication. VANETs are vulnerable to many security threats and attacks. Various types of attacks in VANET are presented in [2] [3]. An adversary may eavesdrop on the channel easily or insert wrong information in the network. Vehicles are assumed to be cooperative and relay packets to others, but malicious nodes may not comply with this protocol.

Sender–ID	Timestamp	Position	Speed	Warning

Figure 2. Safety Message format

All vehicles periodically broadcast beacon packets containing their status (e.g. position, speed, direction) along with the safety messages about dangers. A safety message is shown in Figure 2. The difference between the beacon packets and safety packets is that the former does not have warning field and safety packets are sent only on the occurrence of specific event.

Owing to movement of vehicles and changing traffic

conditions on roads in VANET environment, it is challenging to determine if the node spreading traffic safety information is malicious or not. Two critical elements in VANET safety message are location and time. Information that is more recent in time and location of an event are more relevant. Malicious node exploits this through modification of time and position information in forwarded packets. Selfish vehicles may attempt to clear up the path ahead with false traffic reports, criminals being chased may disseminate bogus notifications to other vehicles in order to block police cars, terrorists may produce serious traffic collisions with contradictory traffic announcements.

It is a usual norm in VANET to forward each received packet to neighboring nodes. Malicious nodes can adversely impact this process either by delaying, replaying or suppressing the safety packets.

In this paper, we focus on the attacks related to **time** information in safety packet only. Specifically, the contribution of our paper is:

- Modeling and simulation of packet delay, suppression and replay attacks in VANET.
- Consequences of these attacks on VANET performance
- Proposal for countermeasures against these attacks.

The rest of this paper is organized as follows. Section II discusses related work of several attacks and their detection approaches in inter-vehicle communication system. Section III describes VANET model and attacker model. In Section IV, experimental setup to implement these attacks and its consequences on VANET performance is discussed. A brief outline of proposed methodology is introduced in Section V. Concluding remarks with future work are covered in Section VI

2. RELATED WORK

Various types of attacks on an inter-vehicle communication system are presented by Aijaz *et al* in [2]. They analyze how an attacker can manipulate the input of an OBU and sensor readings. The authors propose plausibility checks using constant system examinations, but no detailed discussion on implementation of plausibility check is presented.

M. Raya and J.P. Hubaux [4] describe how adversaries use safety applications to create various attacks and security problems. Ghosh *et al* [5] present misbehavior detection scheme (MDS) for post crash notification (PCN) applications. Golle *et al* [6] propose an approach to detect and correct malicious data in VANET. They assume that vehicular node is maintaining all the information that nodes have about the network. It is not feasible to design a model based on global knowledge of the network.

Raya *et al* [8] have formulated a misbehavior detection system to exclude malicious vehicles from the communication system through clustering. Nai-Wei *et al* [3] presented Illusion attack in VANET. In this attack, a malicious node creates a particular traffic situation and sends fraud traffic warning messages to other nodes for convincing them that a traffic event has occurred. To detect and defend against the illusion network, plausibility validation network model is introduced in this paper.

Yan *et al* have proposed a position verification approach for detection of position related misbehaviors in [7]. Schmidt *et al* [9] construct reputation model for normal VANET behavior. Any deviation from the normal behavior is marked as suspicious. Raya *et al* [11] present their work on "data centric trust" in VANET. They confirm the occurrence of an event based upon the messages received from multiple vehicles.

3. SYSTEM AND ATTACKER MODEL

In this section, we present a description of the VANET model and Attacker model.

A.VANET model

Each node in VANET has an EDR (Event Data Recorder), GPS (Global Positioning System) receiver, computing platform and a radar. It is assumed that a unique vehicle ID is assigned to each vehicle. At the data link layer, dedicated short range communication (DSRC) protocol [1], currently being standardized as IEEE 802.11p is used. It provides transmission range of 250 to 1000m, with data rates in the 6-27Mbps range. Beyond DSRC, vehicular networks can also leverage other wireless communication technologies such as Cellular, Satellite and WiMAX. In VANET, all information is publicly available as safety messages are meant for each vehicle. No public key infrastructure (PKI) or other cryptographic framework is assumed.

B. Attacker Model

A malicious node can introduce some delay while forwarding the received safety packet from originator or suppress the received packets, i.e. block the forwarding process in VANET. An attacker can also replay the received packets apart from acting as a normal node (forwards all the received packets). It is assumed that attacker has sufficient capacity for storing messages. In all these cases, receivers will not be able to take proper action on time. We have considered three attack models in VANET.

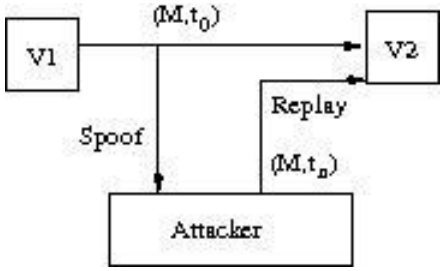

Figure 3. A typical Packet Replay attack in VANET scenario

1. **Packet Replay Attack:** Replay attack is a form of attack in which a normal data transmission is fraudulently repeated or delayed. This operation is carried out by a malicious node who intercepts the safety packet and retransmits it. Replay attack is usually performed by an unauthorized user to impersonate a legitimate vehicle or RSU. A typical replay attack scenario in VANET is shown in Figure 3.

2. **Packet Delay Attack**: This attack is a subset of packet replay attack. In this attack, a vehicle delays the packet being forwarded by certain time duration in the network. An example of packet delay attack is shown in Figure 4. It is more harmful than replay attack as vehicles may not get enough time to respond to particular emergency situation. In Figure 4, a vehicle V1 broadcasts *TRAFFIC JAM* safety packet at time-stamp $t0$ to its neighboring nodes after observing the traffic. All the legitimate vehicles (V2, V3) forward this packet to others at time-stamp t_1 but a malicious vehicle ***Attacker*** introduces a delay of $(t_n - t_1)$ time duration. The road becomes jam free at

time-stamp t_n and ***Attacker*** sends the TRAFFIC *JAM* packet (received at t_1) time-stamp. As a result of the falsification of information, other cars may change their route to nearby roads that may lead to real congestion on this route.

3. **Packet Suppression Attack**: In this attack, whenever a vehicle receives safety packet from the neighboring node, it does not forward this packet at all. An example of packet suppression attack is shown in Figure 5.

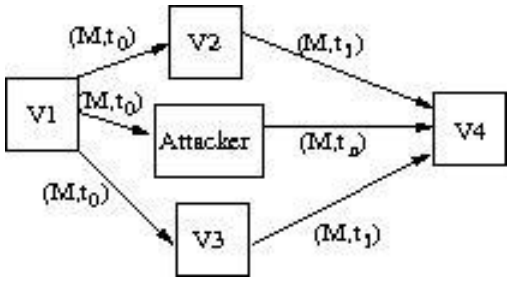

Figure 4. An example of Packet Delay attack in VANET Scenario

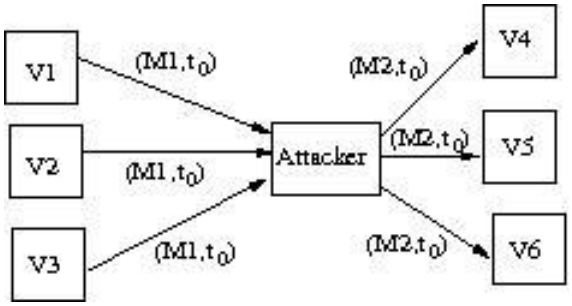

Figure 5. Packet Suppression attack in VANET scenario

4. EXPERIMENTAL SETUP AND RESULT ANALYSIS

We used NCTUns-6.0 simulator [10] for our experimental setup. This simulator provides support of simulation parameters including topology (road network), communication and network protocol, vehicular traffic etc. We applied a widely used radio propagation model – 'shadowing model' to consider the multi–path propagation effects of the real world communication system. Different forms of attacker node as discussed in previous Section are implemented. We modified safety packet distribution module in NCTUns-6.0. In Packet Replay attack, an attacker node forwards received critical event information (in the form of safety packet) from the originator, it normally forwards this packet to further approaching vehicles. Additionally, an attacker keeps a copy of this packet and forwards this packet again in the network at later time interval. An attacker vehicle supplements significant delay while forwarding the packet in Packet Delay attack. In Packet Suppression Attack, an attacker vehicle captures the received packet and does not forward it. We disable the packet propagation module associated with attacker node to implement this form of attack.

In our experiments, we simulated a two–direction 6 km highway with multi lanes in each direction. The average speed range is set between 8–50 m/s, traffic arrival rate is 500 vehicles/hour and transmission range is 250 meters. Each simulation case has varied number of attackers.

We used varying number of above defined attackers in our experiments. Each experiment was run 5-7 times with a different seed value. Figure 6. shows the impact of these attacks on percentage of packets delivered to destined nodes. Destined nodes are the nodes located within the area of critical situation. These results are evaluated using 10% malicious nodes in VANET scenario. All the attackers start their operation at 30 seconds and end at 55 seconds. This graph shows that the percentage of packet delivered is reduced in the case of Delay Attack with respect to normal scenario. During the Suppression attack, attacker nodes are not distributing the received packets. Therefore their delivery percentage is reduced to minimum. In the normal case, the percentage of packet delivered is nearby 90 (10 percentage packets are lost due to other reasons like collision). In replay attack, number of packet drop increases due to more number of collisions in the network.

5. PROPOSED DETECTION APPROACH

We propose a general model to detect delay, replay and suppression attacks in VANET. In order to implement this approach, we consider following assumptions:

- Each vehicle is equipped with Geographical Positioning System (GPS).
- Vehicles communicate using DSRC communication technology.
- Majority of vehicles are honest. Malicious vehicles are small fraction of VANET population.
- Number of RSUs is uniformly deployed by trusted authorities and vehicles trust message generated by RSU.

Our model is based upon multiple sources of information to differentiate the legitimate packets from delayed or replayed packets. Attacker performing packet suppression operation is also detected if received packet is not able to justify information derived by other sources of information. Figure 7 shows complementary sources of information to validate the messages received from packet delay, replay, suppression attackers or normal nodes. Each vehicle tests the received message based on the information from several sources and combines their outputs. When the combined output implies that a received packet is relevant and legitimate, only then it is accepted by receiver.

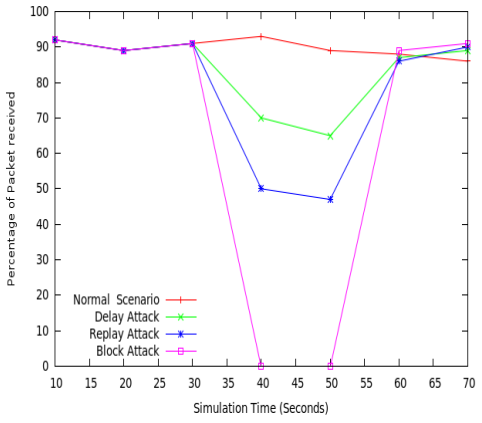

Figure 6. Impact of Temporal attacks on percentage of packets delivered to destined nodes in VANET scenario

1. **Direct Observation**: Vehicles and RSUs are manufactured with various sensors. Each node may use data from these sensors for verification purposes. Nodes can manipulate the current situations based on the type of information received from attacker node and its behavior. For example, in the case of replay or delay attack, if an attacker is broadcasting Road Accident message on particular road segment and moving towards the direction of accident. This situation is directly observed by message receiving nodes.

2. **Response from other vehicles**: When a node broadcasts a safety message of latest occurred event, all the receiving nodes behave similarly. Whereas, in case of delayed or replayed packets, there is difference in behavior of neighboring nodes of victim. For example, a vehicle can detect that the message about the existence of an accident is feigned if other vehicles near the accident location do not slow down, but rather drive through the accident site.

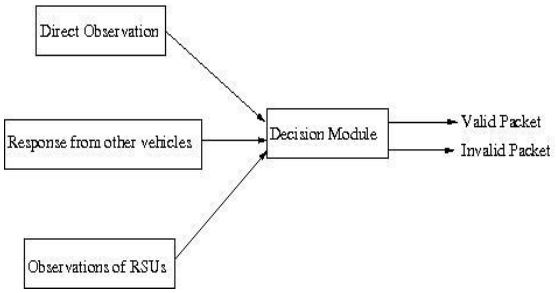

Figure 7. A complete Data Flow of Proposed Detection Approach

3. **Observations of RSU**: Uniform deployment of RSUs along the road can help in determining the road conditions. For example, a vehicle receives message of congestion on road while RSUs do not indicate congestion in that area. Receivers verify each message before reacting according to the message.

6. CONCLUSIONS AND FUTURE WORK

Malicious nodes are harmful for proper functioning of VANET applications. If correct traffic information is not delivered to the drivers before the vehicle approaches the location of occurred event, critical problems can significantly alleviate. In this paper, we implement various attacks based on the time-stamp information broadcast in the safety packets. We analyze the consequences of these attacks on VANET applications. We propose a detection model for these attacks using different sources of information. As a part of future work, we would like to implement this detection approach.

7. REFERENCES

[1] D. Jiang and L. Delgrossi. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular En- vironments. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2036–2040, 2008.

[2] Amer Aijaz, Bernd Bochow, Florian Dtzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, and Tim Leinmller. Attacks on Inter Vehicle Communication Systems - an Analysis. In *In Proc. WIT*, pages 189–194, 2006.

[3] Nai-Wei Lo and Hsiao-Chien Tsai. Illusion Attack on VANET Applications - A Message Plausibility Problem. In *Globecom Workshops, 2007 IEEE*, pages 1–8, 2007.

[4] M. Raya and J.P. Hubaux. Securing Vehicular Ad Hoc Networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[5] Mainak Ghosh, Anitha Varghese, Arobinda Gupta, Arzad A.Kherani, and Skanda N. Muthaiah. Detecting Misbehaviors in VANET with Integrated Root-cause Analysis. *Ad Hoc Netw.* 8:778–790, September 2010.

[6] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and Correcting Malicious Data in VANETs. In V*ANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37, New York, NY, USA, 2004. ACM.

[7] Gongjun Yan, Stephan Olariu, and Michele C. Weigle. Pro- viding VANET Security Through Active Position Detection. *Comput. Commun.*, 31(12):2883–2897, 2008.

[8] Maxim Raya, Panagiotis Papadimitratos, Virgil D. Gligor, and Jean-pierre Hubaux. On data centric trust establishment in ephemeral ad hoc networks. In *IEEE INFOCOM*, 2008.

[9] R. K Schmidt, T. Leinmuller, E. Schoch, A. Held, and G. Schafer. Vehicle Behavior Analysis to Enhance Security in VANETs. In *Vehicle to Vehicle Communication, V2VCOM*, 2008.

[10] Nctuns 6.0, Network Simulator and Emulator. http://NSL. csie.nctu.edu.tw/nctuns.html.

[11] Maxim Raya, Panagiotis Papadimitratos, Virgil D. Gligor, and Jean-pierre Hubaux. On data centric trust establishment in ephemeral ad hoc networks. In *IEEE INFOCOM*, 2008.