Timing Attack in Vehicular Network

IRSHAD AHMED SUMRA¹, JAMALUL-LAIL AB MANAN², HALABI HASBULLAH¹,
¹Computer and Information Sciences Department
Universiti Teknologi PETRONAS,
Bandar Seri Iskandar, 31750,Tronoh, Perak,
MALAYSIA.
²Advanced Information Security Cluster, MIMOS Berhad,
Technology Park Malaysia Kuala Lumpur,
MALAYSIA.
isomro28@gmail.com, jamalul.lail@mimos.my, halabi@petronas.com.my

Abstract: - VANET safety and non safety applications have received more attention both by drivers and passengers on today’s highway. The main purpose of safety application is to provide safety road condition information to users and hence save human lives from accidents. Warning messages are the more critical part of the safety messages and if attackers alter its messages, it will not help in achieving the safety objectives. These messages may easily be altered due to the dynamic topology and high speed of running vehicles, which makes timing as the key factor for its success. In this paper we discuss some issues related to timing attack which can create delay in messages.

Key-Words: - Safety and non safety application, Attackers, Timing attacks, delay.

1 Introduction

VANET safety and non safety applications are taken more attention for driver and passengers for safety and comfortable on highway. Purpose of these applications to provides right information to users and safe the human levies from accidents. Warning messages are more critical part of the safety messages and if attackers alter such kind of messages then main objective of the VANET applications is not achieved. The main aim of VANET applications is to deliver right information to users at the right time. Due to dynamic topology and high speed of the vehicle, time is the key factor for sending and receiving messages. In this paper we are discuss timing attack which create delay in messages (safety or non safety) by adding some time interval. Trusted platform module (TPM) is hardware security module use to maintain the integrity of the data in vehicular network. Our proposed solutions are based on digital signature and TPM and explain in detail to overcome this new attack

There are two types of users’ requirements; firstly, the primary requirement is to ensure that the content of the message is secure and safe. Secondly, the secondary requirement is that safety message should reach destination on right time. From past experiences, we note that the behavior of attacker is not static, it is dynamic and any kind of attack could be launched from anywhere in network. For example, an attack may be a DOS attack or it could just be an alteration of the safety messages. For an attack on adding some delay in the safety message, bad consequences will happen if these messages are received at the wrong time. Due to its criticalness, users’ requirement includes timing security which must be well implemented. Nowadays many embedded sensors and security modules used in vehicular networks will need the enforcement of critical timing security.

TPM is one of the main security module and purpose of this module to maintain the integrity of message using the strong cryptographic functioning modules. Privacy Certification Authority (PCA) and Direct Anonymous Attestation (DAA) are two main protocols in conjunction with the TPM. It has been mentioned that DAA [3] is best solution in vehicular network; because it provides privacy of driver and security for applications.

This paper is divided into six sections; Section 2 describes the VANET safety applications and time requirements for these applications. Warning message need are more time critical applications and its importance is high as compared to non-safety applications. Section 3 explains the different types of delay in Vehicular Network. Section 4 explains timing attack and how it could affect communication in V2V and V2I and conclusion and future work is in last section 5.
2 VANET Applications and Time Requirements

Dedicated short range communication (DSRC) [4] is the communication medium which is used for safety and non safety applications in vehicular network. DSRC works on 5.9 GHz band and its communication range is up to 1000m. All safety application in VANET uses minimum frequency between 1 and 50 Hz with communication range between 100 and 1000m. Periodic and Event Driven messages [5] are used in vehicular network for sending safety messages. Periodic messages are generated to inform other vehicles in the network about the current status (speed, position, direction) of the nearby vehicle. The purpose of periodic message is to inform surrounding vehicles about current situation of the environment.

Event driven messages are sent to other vehicles during unsafe condition. It is only generated in emergency situation and priority of these messages is very high due to unsafe condition. Event driven message give information about the event time, location and event type to other vehicles of the network. The main challenge in this kind of the messages is to ensure that these messages are received correctly and quickly. Sender makes sure the messages are receive on time. This is time critical message and if attackers were to just generate some delay in these messages then user would not benefits from the safety application.

In safety message, time and contents of the message are both important. Right information must be received the users in right time, this is basic requirement of the safety applications. Figure 1 shows the VANET time critical warning applications. Safety applications [6] are most important applications, because it is directly related to users and its priority is critically high due to human life saving factor. Warning applications provide information about warning messages and these messages are time critical and its importance is also high for safety of human life. If an attacker creates delay in it then it could result in very serious tragedy on the road and many accidents may occur due to this.

Vehicles and links within VANET would not be able to perform their task in the presence of congested network. So main objective of the congestion control mechanism is that all entities in the network can still perform their task accurately in all conditions and user takes benefits from using network resources. Broadcast and geo-cast types of communications pose some challenges for communication between the network during sending and receiving messages. Congestion happens in hop to hop and hop to multihop in VANET and hence creates delay within the network. Cooperative and fully distributed congestion control approach, which are based on dynamic scheduling and transmission of priority-based messages as well as Utility-Based Packet Forwarding and Congestion Control (UBPFCC) are some of the proposed solutions for congestion control in different studies [8], [9], [10].

3.2 Routing Delay

There are many routing protocols that are used for sending messages from source to destination by using of different hops. Geographic Source Routing (GSR), Greedy Perimeter Coordinator Routing (GPCR), Anchor-based Street and Traffic Aware Routing (A-STAR), Mobility-Centric Data Dissemination Algorithm for Vehicular Networks (MDDV), Vehicle-Assisted Data Delivery (VADD), Directional Greedy Routing Protocol (DGRP), and Predictive Directional Greedy Routing (PDGR) are some of the routing protocols in VANET which have been mentioned in their studies [11], [12]. A-STAR, MDDV, VADD and DGRP are some of routing protocol has the drawback of generating maximum delay while sending packet from source to destination. Edge Node Based Greedy Routing Algorithm (EBGR) protocol has been proposed to mitigate this issue by reducing packet transmission delay in VANET. Different papers such as [13], [14], [15] have proposed many efficient routing
mechanisms and to reduce the routing delay in the network.

4 Possible Timing Attack in VANET

4.1 Vehicle-to-Vehicle (V2V) Timing Attack

Timing attacks may be of two levels. Basic level attack targets on peer to peer communication and threat level is low as compared to extended level timing attacks which targets on group communication. Consequently, more people are affected in extended level attack as compared to basic level attack. More detail of both levels of attacks is given below.

- **Basic Level Attack**

  **Peer to Peer (P2P) Network Communication:** This is a unicast type communication between one sender and one receiver. The threat level of timing attack on this communication is low because only one user is affected. Figure 2 explains the situation where vehicle B is an attacker vehicle and it launches timing attack between vehicle A and vehicle C. If vehicle C receives this message at right time, then C will have two options to move, either in direction A or B. For a serious case if vehicle C receiving right message which is delayed due to timing attack, vehicle C will go on a wrong highway where the accident actually happen. Figure 3 shows the location of vehicle C, wherein it turns to the wrong highway due to delay in message.

  - Messages Content: Warning: Accident a location Y.
  - Time: when attacker receive message: 2:30:35 pm
  - Add time slot: attacker add 15 second

In this example, a change of 15 seconds delay causes the vehicle C to change its direction to another way, where the accident actually happens.

- **Extended Level Attack**

  In extended level attack more than one user would be affected due to timing attack. Figure 4 shows how the attacker launches timing attack using a multicast technique in which attacker targets a specific group of vehicles. In this serious case, multiple users are seriously affected. Geo-cast and Broadcast are two more data dissemination technique that an attacker could use for this kind of attack.
4.2 Timing attack in Vehicle to infrastructure (V2I) Communication

Infrastructure is key part of vehicular network and user usually sends and receives messages to and from the infrastructure. Next, we discuss the timing attack on network infrastructure. There are two types of possible infrastructure attack cases in vehicular environment.

Case One: Timing Attack for Authentication

As we have mentioned in Figure 5 vehicle A sends request to RSU1 at time 8:45:30 for authentication. Vehicle X is attacker vehicle which joins the network to carry up an attack. Other vehicles within the network communicate in the usual way with other vehicles and the infrastructure. The attacker X then adds 20 sec delay to all communication messages within the nearby vehicles through the authentication request messages to RSU1. Due to the effect of attacker’s delay injection, the actual authentication request of vehicle A reaches RSU1 at time 8:45:50. Without realizing any attacker presence, RSU1 sends this request to TOC for authentication. In Figure 6 RSU1 is now looking for vehicle A, who sends its request for authentication. Due to high speed mobility of the vehicle and rapid changes of network topology, vehicle A has already reached the service area of the next RSU2. On 8:45:55 there is no more vehicle A in this specific region and hence cannot be “seen” by the RSU1.

Figure 5 Timing Attack for authentication

Figure 6 Reply from RSU for authentication

Case Two: Timing Attack for Taking Services

Safety and non safety are two potential VANET applications which aim to improve the traffic system and serve the users on road. An attacker may launch different types of attacks using different timing. Figure 7 explains how two possible cases of attacks that may happen.

First Case: Vehicle A wants to send accident information to RSU2 but attacker X creates trouble using timing attacks and the crucial information do not arrive on time to its authorized recipients. Using this type of attack, RSU2 is not able to guide the other vehicle users in that service area.

Second Case: Vehicle B which is staying in the area of RSU4 and taking services from it. Vehicle Y is an attacker vehicle and launches timing attacks between the RSU4 and vehicle B. The main objective of vehicular network and its applications to serve the users in the specific area is not fulfilled due to the timing attack.

Figure 7 Timing attack for taking services from different RSUs
4.3 Problem due to Timing Attack:

Data Redundancy

VANET provides different types of communication mechanism to users including point to point (P2P), point to multiple points (P2M), geocast and broadcast techniques. In timing attacks, the users receive multiple copies of same message in different time slots, which pose data redundancy issues. Cases of redundancy of data such as this are mainly due to timing attack. Figure 8 describes the data redundancy in the vehicular network due to timing attack. In this case, Vehicle A sends message about an accident at location Y to vehicle B and vehicle X. Vehicle B sends this message to nearby vehicle C at time t1. Vehicle X is in fact an attacker vehicle and taking advantage of this situation, it also sends this message again to vehicle C with time slot t2. Hence, the vehicle C receives the same message with different time slots from different vehicles. In this scenario the time slot is greater time slot t1 because the attacker adds some time slot in t2 and creates delay. The consequence of the affect of timing attack is also affecting the location of the vehicle. When vehicle C receives first message in t1 then the location of vehicle is L1 and second message receive on location L2. Location L2 may either be near the accident location or the ahead of the accident location.

\[ t2.L2 > t1.L1 \]  \hspace{1cm} (1)

In case of timing attacks the time slot (t2) and message receiving location is greater to time slot1 and location L1. Eq.(1) explain it.

![Figure 8 Data Redundancy in timing Attack](image)

5 Conclusion and Future Work

In this paper we have discussed some issues related to timing attack which can create delay in messages in Vehicular Networks. The issues discussed here can be considered as a newly highlighted problem and need attention by researchers working for solutions. In future work we are looking into possible solution based on trusted platform module (TPM) to secure integrity in vehicular network as a potential mechanism to resolve timing attacks.

Acknowledgment

This work is funded by Universiti Teknologi PETRONAS Postgraduate Assistantship Scheme and MIMOS Berhad.

References