Detection and Prevention of Security Attacks in VANET

Naveen R
1BM16CS055

N.S.V Chaitanya
1BM16CS053

Nikhil Srinivas M
1BM16CS058

Guide
Dr. Nandhini Vineeth
Assistant Professor

Department of Computer Science and Engineering, B.M.S. College of Engineering, Bangalore-560019

Introduction

In the current generation, road accidents and security problems increase dramatically worldwide in our day to day life. In order to overcome this, Vehicular Ad-hoc Network (VANETs) is considered as a key element of future Intelligent Transportation Systems (ITS). With the advancement in vehicular communications, the attacks have also increased, and such architecture is still exposed to many weaknesses which led to numerous security threats that must be addressed before VANET technology is practically and safely adopted. Distributed Denial of Service (DDoS) attack, replay attacks and Sybil attacks are the significant security threats that affect the communication and privacy in VANET. As simulators are being used in our work, we have discussed OMNET++ which is a new modernized latest mobility and network simulators as well as data network simulator. This is also integrated with the road traffic simulator SUMO with Veins, an open-source framework for VANET simulation. The objective of our work is to design an algorithm to detect and prevent various kinds of attacks using Java Security and Cryptography libraries. An analysis has also been done by applying four protocols on an existing scenario of real traffic simulator using OpenStreetMap and the best suitable protocol has been selected for further application.

Vehicular Ad-hoc Network (VANET) provides a smart transportation system owing to Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) message dissemination with an objective to provide safety on roads. Nearly 1.25 million people die each year and on an average 3,287 deaths, a day is observed according to the world health organization.

Proposed System

This paper proposes the methods for detecting and preventing security attacks for both V2V and V2I communication in VANETs. More specifically we are going to address security in VANET "**beaconing messages"**, i.e., messages sent from a vehicle to its neighbours with information of location, speed, braking and other sensorial data that aid safe decision making.
The main contribution of the paper has been given in the following points:

-
- Detecting some major security attacks which are highly probable and that exploit the both V2V and V2I communication by sending the false information to other vehicles and RSU in VANET communication as listed in the following.
  - Sybil Attack
  - Reply Attack
  - DDOS Attack
- Design of an Algorithm for detecting the Sybil nodes by considering the timestamp and velocity parameter of the beacon messages sent from the vehicle nodes which estimates the distance and predict the current position.
- Provided various measures to prevent the attackers in VANET communication.
- Implemented a system which detect the best routing protocol for the VANET communication by considering the realistic scenario generated from OSM and simulation has been done using SUMO and NS3.

High level design of the implemented system is shown in Fig. 1. which shows the detailed the transmission and authentications process of the beacons in the VANETs.

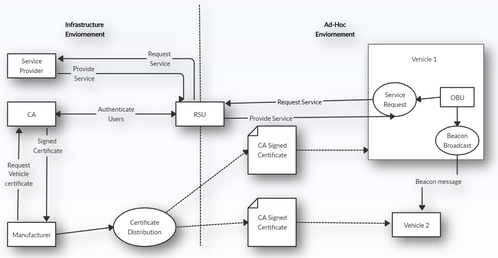

Fig. 1 High level diagram

Implementation of modules

- Firstly we addressed the **identification** requirement. To uniquely identify a vehicle we provided the **Vehicle Identification Number(VIN)** using CA authority which distributes unique key for each node.

- To solve the Problem of **authentication** and ensure **message integrity** and **non-repudiation** of the sender we implemented digital signature for each vehicle and the messages.

- Being a critical system we have also have to ensure **high availability** of the system. For that we intend to detect if a user is sending messages too frequently at the communication unit level, only passing them to the OBU after a minimum delta time between messages has passed. We can't ignore all future messages because they can be critical, but we drop the excess ones that won't affect road safety. How it all works shown in Fig. 2.

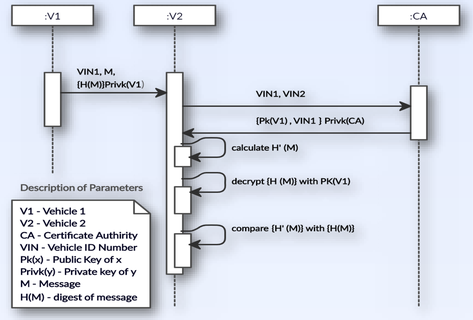

Fig. 2 Message Exchange between Nodes

- **Reply Attack:**

  - **Detection**: We have to guarantee that messages are fresh, making it impossible for an attacker to replay them later on. To accomplish this we decided to attach a timestamp to every messages from vehicle nodes. RSU stores the first 20 messages from each vehicle for certain period, within that time if same vehicle tries to re-send the same messages, we then calculate the time stamp of the messages, if the timestamp is above the given threshold, RSU will drop the messages sent by vehicle and detect it as Replay attack nodes.
  - **Prevention:** When RSU detects the vehicle as Replay Node attacker, it will not let any messages from attacker to vehicle nodes by checking in the cache memory and dropping messages with a timestamp above a certain threshold when compared to the current time.

- **Sybille Attack:**

  - **Detection:** Sybil attack is an identity spoofing attack that is based on creating a forged identity in a network and misusing it for his needs Proposed system first RSU checks if message sent from vehicle is authenticated and signed by CA, then estimates the speed of the node by predicting the timestamp of the last message sent from the node. The after RSU predicts the Position of the vehicle by considering estimated speed and last speed recorded in the RSU table. If the response comes below the certain threshold RSU detect it as a Sybille Node.
  - **Prevention:** After detecting the Sybille node, RSU sends request to CA to revoke the certificate and identity of the Sybille node. After getting response from CA, RSU stores the information of the Sybille node in RSU Cache to make verification easy next time. Finally, RSU informs the vehicle about the Sybille node and drops the messages.

Implementation of modules Cont'd…

- **DDOS Attack:**
  - **Detection: T**he attacker attacks the communication medium to create channel jam. The channel will not be available anymore to the nodes and they are not able to access it. Hence Proposed system, RSU calculate the frequency and velocity of the messages coming from vehicle, then RSU checks with upper and lower bound of the threshold, if the Result is Higher than the certain threshold, RSU detects those as the DDOS attackers nodes.
  - **Prevention:** After detecting the DDOS nodes, RSU sends request to CA to revoke the certificate and identity of the Sybille node. After getting response from CA, RSU stores the information of the Sybille node in RSU Cache to make verification easy next time. Finally, RSU informs the vehicle about the Sybille node and drops the messages

- **Best Routing Protocol:** the best reliable routing protocol is required for the transmission in the real-world scenario. To achieve that, we have implemented system which generates the real-world scenario by selecting the specified area from the OpenStreetMap Framework. where number of vehicles, Trucks, Traffic Signals and pedestrians were selected. Then, we analysed the generated scenario in Urban simulator called SUMO.

Simulation Result and Performance Analysis

We used the following Simulation tool in our implanted system

- SUMO – Simulation of urban mobility
- OSM – Open Street Map
- JVSN – Java VANET Simulation Network
- NS3 – Network Simulation

- Using SUMO a Mobilty.tcl file was generated to analyse the communication between the nodes by using the four different routing protocol such as (Ad hoc On-Demand Distance Vector) AODV, Dynamic Source Routing (DSR), Destination-Sequenced Distance-Vector DSDV, Optimized Link State Routing Protocol (OLSR) with the Network Simulator NS3. Finally, For the given simulation duration, the DSR protocol was giving the high throughput and less network over head in VANET communication system as shown in the Fig.3.

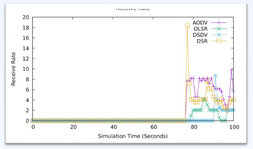

Fig. 3 DSR routing protocol gives the good throughput than other protocol

Algorithm	Signing Delay in ms	Verification Delay in ms
RSA 2048-bit	22.737	0.599
ECDSA 224 bit	0.800	3.000

Table 1. RSA and ECDSA Signing and Verification Delay

- The parameters used in these simulations are summarized in the table II. Each simulation was run 10 times and the presented results were averaged from these 10 executions. The Figure 4 and 5 show the right and false negative detection rates compared to the speed threshold and the number of attacker respectively.

- It can be noticed when the threshold is increased, the rate of false negative detection is higher. This could be explained by the fact that with a high speed threshold, we can miss a lot of attacks.

- In the figure 4, we fixed the speed threshold to 5 Km/h and we varied the number of attackers. With a low number of attackers, the detection is difficult since the difference between the estimated speed and the real one could not be very different, specially in the fluid zone, the speed remains the same even with more vehicles. The difference will be more significant in the congested area. This is shown by the figure 5.

Results Cont'd…

Number of Vehicles	Throughput of the Network	Packet Delivered Ratio	Packet Loss Ratio	Network LifeTime
5	250	58	300	41
8	300	59	190	39
10	350	62	152	38
12	360	68	130	37.5

Table 2. Performance Parameters in Simulation

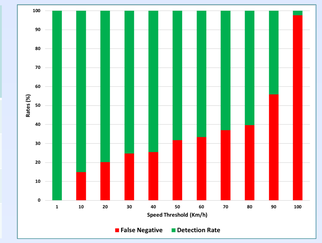

***Fig. 4* Attacks detection rate vs the speed threshold**

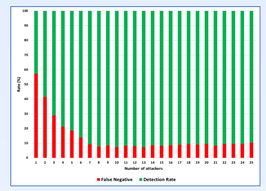

***Fig. 5* Attacks detection rate vs the number of attackers**

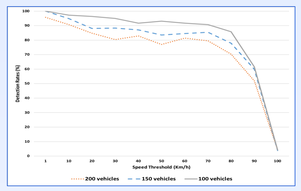

***Fig. 6* Attacks detection rate Vs. the speed threshold for different number of vehicles**

- Figure 6 shows that the detection rate is higher when the speed threshold is lower independently from the number of vehicles. This is due to the missing of attack detection when using high speed threshold.

- we will have almost the same detection rate, which is about 90% of right detection.

- The proposed algorithm for detection of DDOS attack is simulated using different number of nodes that is taking 5, 8, 10 and 12 number of nodes.

- The proposed technique is capable for detecting Sybil as well as DoS attacks if implementing on 12 nodes but all other techniques can only detect DoS attack..

- The throughput of the network is increased; packet delivery ratio is also increased. Although the network lifetime is decreased slightly but the packet loss ratio is decreased dramatically.

All the calculated parameters show that the proposed algorithm is far better than the existing one

Conclusion

This report highlights how the VANET environment can be improved by improving the driving experience, navigation services, road safety and other roadside services. Due to the characteristics of the VANET system and its architecture, VANET is vulnerable to many security attacks. There is a need to develop security solutions in the VANET environment. Many previous security efforts have applied the same old traditional security solutions without considering any special aspects of VANETs. We have studied the security challenges faced by VANETs and their architecture for our literature, which have helped us to come up with this solution the Replay attack, Sybil attack and DDOS attack and simulation has been done using the SUMO, NS3 and JVSN tools. We also implemented the system which shows the DSR routing protocol can be used for the communication in VANET Network in Urban area which.