REACT- Implementing Security in VANET and Increasing Stability using Greedy Forwarding Algorithm

Athira P
M.Tech. Student
Department of Electronics & Communication Engineering
AACET Thodupuzha, Kerala

Abstract— Privacy and security are major issues in vehicular ad hoc networks. Several works have been proposed with the same aim. However, as far as, some researches on VANET protocols have addressed the privacy issues and encryption key establishment. To do so, vehicles need to continuously send safety messages providing the position information to nearby vehicles. This frequent messaging may cause the tracking of vehicles, if it success to eavesdrop the wireless medium. The integrity of the messages exchanged between subscriber and RSUs and the privacy of VANET users who exchange these messages are a major concern. A web-based secure registration process allows a user to register in RSUs. At the registration session, users give all needed information that licenses them to have the advantage of secure connectivity throughout the communication. Moreover, the proposed cryptographic function that allows users and RSUs to provide the required security level of exchanged messages. For obtaining security against privacy hacking and eves dropping, it makes an RSU to make the next encryption key and the next pseudonym to use unique. Routing efficiency is improved using the highly stable greedy forwarding mechanism. Thus, the robustness of the user privacy and secure communication in service oriented vehicular networks and efficient routing is achieved under various communication attacks.

Key words: REACT, VANET

I. INTRODUCTION

The reliability of the messages exchanged between client and RSUs and the privacy of the position of the VANET users, when communicate with each other, are a major concern. Eventhough, they use AES, mainly the elliptic curve cryptography (ECC) standard. Prior to that, a symmetric scheme [Advanced Encryption Standard (AES)] is used. The safety of clients should be accounted throughout the communication. Hence, a web-based secure registration process is introduced, in which a user register with RSUs. At the registration session, users gives all needed information that license them to have the advantage of secure connectivity throughout the communication. Moreover, the proposed cryptographic function that allow users and RSUs to provide maximum security to exchanged messages. For obtaining security against privacy hacking and evesdropping, it makes an RSU to make the next encryption key and the next pseudonym to be unique. Also, a bunch of encryption keys are derived, which are used to encrypt the next data packet.

When a user gets connected to an RSU, they starts a new session. For securing users' location privacy, RSU sends a new pseudonym in each packet. A session gets started when the user sends a Hello packet that consists of their username to the adjacent RSU. The packet will hold a timestamp for preventing replay attacks. When the Hello packet reaches RSU, it assembles the user's data that do not need authentication with other systems, from their profile. The data's that require authentication will be delayed until the RSU gets the key Kc from the user. When the RSU prepares users' data, a pseudonym will be attached and it is routed to the users in an ID packet. The receiver acknowledges with an "Identify" packet that contains their username, password, and Kc. The packets would be encrypted using Km.

RSUs can well defend against software attacks. The RSUs don't store sensitive data, but every RSUs have a safe connection to a database server which keeps the RSUs' private datas. Each RSU will private database to avoid failures. Moreover, every RSUs will be observed by a TA, which will isolate it from the network, when detected with mallicious behaviour, by informing other RSUs and the vehicles which are connected to them. A secure protocol connects RSUs to one another. Individual user will be connected to a single RSU at a time. Users and RSUs exchange datas directly when they are within range and relies on the network-layer routing protocol when they are far. For this, an efficient routing protocol was designed that transfers messages between a users and an RSU through other vehicles in a reliable manner.

II. EXISTING SYSTEM

Each vehicle repeatedly sends messages over a single hop for every interval. The inter-message interval drops if the vehicles are very slow or stopped. Vehicles take decisions based on the received messages and may transmit new ones. Vehicle should only react to reliable messages that are sent by reliable senders. Therefore it is necessary to authenticate the senders of these messages. The reliability of messages also includes their consistency with similar ones, because the sender can be reliable while the message contains false data. Vehicles usually take decisions based on the received messages and may reply to that. Such that, if U receives an emergency message from another vehicle Q and, based on their positions, calculates that it is also in danger and it sends out its own warning messages. Symmetric authentication mechanisms usually prompt less expense per message than their asymmetric counter parts. The digital signatures are a good choice in the VANET setting, because safety messages should be sent to receivers as fast as possible. A preliminary authentication is not acceptable and actually creates more problems. Moreover, given the large amount of network members and the improper connectivity to authentication servers, a PKI (Public Key Infrastructure) is the most suitable way for providing integrity.

In the PKI system, vehicle will be provided with a public/private key. Before a vehicle sends the data, it signs it with its private key and the CA's certificate also included with the message. The recepient receives the message, they

will verify the public key of user using the certificate and then verify user's signature using its public key. For this, the receiver should have the public key of the sender.. If the message is sent in an emergency context, which means that it belongs to the liability-related class, this message should be stored including the signature and the certificate in the EDR for further potential investigations in the emergency. The use of secret information such as private keys incurs the need for a tamper-proof device in each vehicle. In addition to storing the secret information, this device will be also responsible for signing outgoing messages. To reduce the risk of its compromise by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station. The access to this device should be restricted to authorized people. For example, cryptographic keys can be renewed at the periodic technical checkup of the vehicle.

III. PROPOSED SYSTEM

Many services could be provided by using RSUs as agents to obtain data on the user's behalf. The services of the VANET includes many fields such as entertainment, download, emailing and chatting on social networks. A service-oriented vehicular security system allows VANET users to use RSUs in obtaining various types of data. In REACT, users register first with the RSUs online (through the Internet) before they start communicating to the RSUs from their vehicle. After registration, the RSUs obtains a master key (Km) from a trusted authority (TA) for the user. The users get their Km when they connect to an RSU from their vehicle. A novel algorithm uses the users' password from their account to securely transfer their Km to them. Km will be used to encrypt the initial packet key, which is assigned to the user at the beginning of each session. Then, each packet will be encrypted by a set of derived keys. With regard to the assumptions, presume that each vehicle is equipped with a positioning system (e.g., Global Positioning System) and a digital map and has an Electronic License Plate (ELP) installed.

Assume a hybrid RSU architecture in which some RSUs are directly wired to each other, others connect to the RSU network through the Internet (using gateways), whereas a third group is both wired to other RSUs and has an Internet connection. In all cases, however, each RSU has a way of connecting to any other RSU (possibly through other RSUs). In addition, several TAs are connected to the RSUs through secure wired links. TAs has powerful firewalls and other protections that prevent them from being compromised. In addition, the RSUs are supposedly equipped with trusted platform modules (TPMs), intrusion detection systems, and firewalls that enable them to resist software attacks. With respect to hardware attacks, RSUs can be monitored using hidden surveillance cameras such as digital video or analog CCTV cameras that report to a central station, in which observers can immediately notice a hardware attack and take the appropriate actions. The RSUs do not store sensitive data, but each RSU has a secure connection to a database server that stores the RSUs' private information.

Each RSU will have its own database to avoid the effect of failures. In addition, assume that each RSU will be monitored by a TA, which, upon detecting a malicious behavior from the RSU, will isolate it from the network by informing other RSUs, which inform vehicles that are connecting to them. A secure protocol (such as IP tunneling) is assumed to connect RSUs to one another. For VANET users, assume that each user will connect to a single RSU at a single time (to reduce overhead). Vehicles and RSUs exchange messages using unicast when they are within direct range and depend on the network-layer routing protocol when they are apart. For this purpose, design an efficient routing protocol that transfers messages between a vehicle and an RSU (and vice versa) through other vehicles in a reliable manner

IV. NS2

Simulation can be defined as reproduction of essential features of something as an aid to study or training. In simulation, we can construct a mathematical model to reproduce the characteristics of a phenomenon, system, or process often using a computer in order to information or solve problems. Nowadays, there are many network simulators that can simulate the MANET. In this section we will introduce the most commonly used simulators. We will compare their advantages and disadvantages and choose one to as platform to implement reactive/ proactive protocol and conduct simulations in this thesis.

Ns-2 is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. It consists of two simulation tools. The network simulator (NS) contains all commonly used IP protocols. The network animator (NAM) is use to visualize the simulations. Ns-2 fully simulates a layered network from the physical radio transmission channel to high- level applications.

Version 2 is the most recent version of ns. The simulator was originally developed by the University of California at Berkeley and VINT project the simulator was recently extended to provide simulation support for ad hoc network by Carnegie Mellon University. The ns-2 simulator has several features that make it suitable for our simulations.

- A network environment for adhoc networks,
- Wireless channel modules (e.g.802.11),
- Routing along multiple paths,
- Mobile hosts for wireless cellular networks.

Nam is an animation tool for viewing network simulation traces and real world packet trace data. NAM was designed to read simple animation event commands from a large trace file. In order to handle large animation datasets a minimum amount of information is kept in memory. Event commands are kept in the file and reread from the file whenever necessary.

The first step to use NAM is to produce the trace file. The trace file contains topology information, e.g., nodes, links, as well as packet traces. Usually, the trace file is generated by NS. During an NS simulation, user can produce topology configurations, layout information, and packet traces using tracing events in NS. However any application can generate a NAM trace file.

Simulator	Network Simulator 2
Number of nodes	38

Interface type	Phy/WirelessPhy
Mac type	802.11
Queue type	Droptail/Priority Queue
Queue length	50 Packets
Antenna type	Omni Antenna
Propagation type	TwoRayGround
Routing protocol	DSR
Transport agent	UDP
Application agent	CBR
Simulation time	100seconds

Table 1: Simulation model

V. MODULES

- Registration
- Master Key Exchange
- Session Initiation
- Handover Process
- Performance Evaluation

A. *Registration*

The users in the network, before starting communication, should register with RSU. During this registration process they provide name, address and phone number to the RSU. Each user will have a unique account in the RSU. The RSU with which the user connects first will be their default RSU, and this default RSU saves their account in its database. The users also provide a user name and password for the authentication purpose when they first register with RSU. In addition to this a secret key Kc also is provided by th user, which is used by the RSU to encrypt the authentication datas of the user and save them. The RSU will not save the sacret key, so tha it is only known to the user.

When the user connects to VANET from anywhere else. It sends a hello packet to the nearby RSU, it will communicate with the user's default RSU and obtain the details from the default RSU database regarding the user. These processes are much needed for the security of the data messages exchanged.

B. *Master Key Exchange*

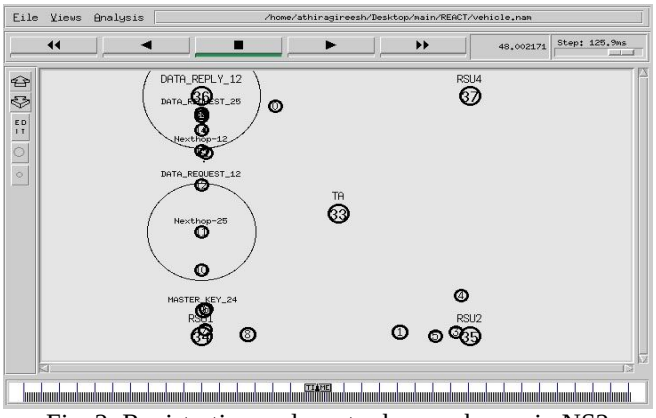

Fig. 2: Registration and master key exchange in NS2 simulator

When the user enter into the network, the first register with RSU. After this registration, before the transfer of the data messages, for security purpose an encryption key is required. This first encryption key will be provided by a Trusted Authority. The TA will send a master key to the RSU, which will then be given to the user. For the safe transfer of the master key certain measures are taken. The RSU will generate an Iteration count and send to the user. The user will use tis Iteration count and its password to generate some encryption keys for encrypting the master key. Thus the master key will be safely transferred to the user

C. *Session Initiation*

The user sends a hello packet to the RSU to atart a new session. The hello packet will include the user's user name and a timestamp. Timestamp is used for avoiding the reply attacks. When the RSU receives the hello packet, it will contact the user's default RSU and fetches its credentials. The RSU prepares the user's data and assign them a new pseudonym and send them in an ID packet. The pseudonym is used for the location privacy. Then the user will reply with an identify packet that contains its user name, password and Kc. The ID packet and the identify packet will be encrypted with the master key. The RSU will check the password of the user and authenticates it. Then the RSU will send the user credentials to the service provider for the user. The RSU obtains the packet keys for the encryption of each data packet from the trusted authority and sende it to the user. After these initiation processes the data exchange start.

D. *Handover Process*

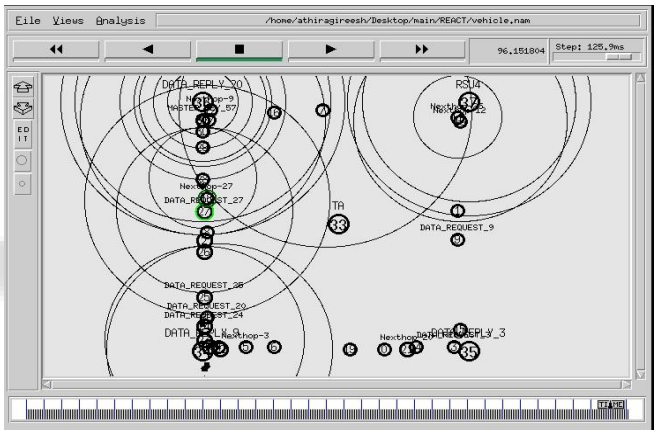

Fig. 3: Handover and data exchange in NS2 simulator

In the celluar networks, when the user gets away from the range of their base station, the handover process will be initiated. So that the service provided to the users will be uninterrupted. Likewise in VANET also the RSU initiates handover when the user gets away from its range. Unlike the cellular networks this process may be multihop in VANET. The control messages exchanged between the user and the RSU woud be small in size compared to the data messages. Suppose that a user is moving from RSU1 to RSU2. The handover process is initiated by the user sending a handover request to the RSU1. This handover request will contain the ID of RSU2. When the RSU1 receives this handover request it will send a handover packet to the RSU2 that contains the user's user name, next pseudonym(pn) and next packet key(Kn). The RSU1 will then send a handover confirm packet to the user that contains pn and Kn. The user will then send a hello packet to RSU2 that contains its username and pn which encrypted with Kn. The RSU2 will decrypt this and authenticate the user. Then it will send an ID packet that contains a new pseudonym to the user. Now the communication is between the user and RSU2. So the data messages pending in RSU1 should be transferred to RSU2.

For this, the RSU1 will wait a short period of time before sending the datas. This time period is for arriving the data replies from other sources for the user. Then RSU1 will send the data replies and the pending requesta to RSU2, which will then be send to the user. Thus the handover process is completed and the service provided to the user is uninterrupted.

E. Performance Evaluation

- Message Success Ratio (MSR): The percentage of messages that are received at their destinations successfully.
- Message Response Time (MRT): The total time required to send a request from a vehicle to an SP and to receive the answer
- Initialization Phase Time (IPT): The system security initialization time, i.e., the average time between the instance a vehicle starts a session to the instance it sends the first packet encrypted with a session key (or packet key)

Average Overhead Traffic (AOT): The extra traffic (mainly due to security packets and to the increase in the size of packets due to cryptographic operations) sent or received by a vehicle.

VI. HIGHLY STABLE GREEDY FORWARDING ALGORITHM

In Vehicular Ad-hoc Networks based on the proposed routing mechanism, if forwarding vehicles have high mobility, there is the chance for local topology inaccuracy. If the vehicle involved in the forwarding path vehicle moves frequently then there is the situation of link failure which leads to packet loss. Hence it is required to select the vehicles with low mobility which means selection of stable vehicle as forwarder based on its mobility. Mobility based forwarding vehicle selection scheme improves the routing performance.

Source vehicle predicts the distance of each neighbor from itself at particular time (t) using the current location of neighbor and speed of the neighbor. After certain time (t+T) it predicts the distance again using the current location of neighbor and speed of the neighbor. In both times if the vehicle comes under neighbor status then it is highly stable neighbor. To apply highly stable greedy forwarding distance between destination and highly stable neighbors are calculated. The neighbor which is having the minimum distance is selected as forwarder.

VII. CONCLUSION

The vehicular ad-hoc networks enable vehicles to communicate with each other. The service oriented VANETs provide internet access to the users in the vehicles. The users can access emails and other internet facilities when connected in VANET. Like other networks security is a major concern in VANET also. A number of solutions are proposed for this problem. An effective system is REACT. Here unique keys are used for the encryption of each data packet. The RSUs are exploited for the security purpose. In real life the vehicles are continuously moving, so stability of the system will be a problem. So inorder to provide stability higly stable greedy forwarding algorithm is introduced. Thus the stability of the system is increased. The Network Simulator 2(NS2) is used for the simulaton of the network and analysis. Using certain quality parameters the performance of the system is analysed and compared with other systems.

REFERENCES

[1] Khaleel Mershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 62, No. 2, February 2013
[2] Ram Shringar Raw, Manish Kumar, Nanhay Singh, "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET",International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013
[3] Sherali Zeadally, Ray Hun, Yuh-Shyan CheN, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", Springer Science+Business Media, LLC 2010
[4] YUN-WEI LIN, YUH-SHYAN CHEN AND SING-LING LEE, "Routing Protocols in Vehicular Ad Hoc Networks: A Survey And Future Perspectives," Journal of Information Science And Engineering 26, 913-932 (2010)
[5] Josiane Nzouonta, Neeraj Rajgure, Guiling (Grace) Wang, Member, IEEE, and Cristian Borcea, Member, IEEE, "VANET Routing on City Roads Using Real-Time Vehicular Traffic Information," Ieee Transactions On Vehicular Technology, Vol. 58, No. 7, September 2009
[6] Nathan Balon, "Introduction to Vehicular Ad Hoc Networks and the Broadcast Storm Problem"
[7] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges

