A Novel Mechanism for Secure and Efficient VANET Communication

V.Vijayalakshmi, S.Saranya, M.Sathya, C.Selvaroopini

(Assistant professor, Department of CSE, Christ College of Engineering and Technology, Pondicherry, India)
(Student, Department of CSE, Christ College of Engineering and Technology, Pondicherry, India)
(Student, Department of CSE, Christ College of Engineering and Technology, Pondicherry, India)
(Student, Department of CSE, Christ College of Engineering and Technology, Pondicherry, India)

ABSTRACT*- A Vehicular Ad hoc NETwork (VANET) is a type of mobile Peer-To-Peer wireless network that allows providing communication among nearby vehicles and between vehicles and nearby fixed roadside equipment. The lack of centralized infrastructure, high node mobility and increasing number of vehicles in VANETs result in several problems discussed in this paper, such as interrupting connections, difficult routing, security of communications and scalability. Existing system for VANET communication is proved to have several drawbacks. We have proposed a mechanism in order to provide secure and efficient communication in VANET environment. We overcome the drawbacks of the existing system by using Malicious Vehicular Analyzer algorithm and Elliptic Curve Cryptography (ECC). Using these algorithms, malicious messages are identified. It also detects the accident and other problems in the path of the vehicles. Elliptic Curve Cryptography (ECC) algorithm is used for stronger security during communication.*

Keywords*: ECC, emergency messages, VANET security, vehicular analyzer, warning messages, etc.*

I. INTRODUCTION

Thousands of people around the world die every year in road accidents and many more are severely injured. Implementations of safety information such as speed limits and road conditions are used in many parts of the world but still more work is required. Vehicular Ad Hoc Networks (VANET) is used to collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger before they actually face it [1]. VANET comprise of entities such as sensors and On Board Units (OBU) installed in the car as well as Road Side Units (RSU). The data collected from the sensors on the vehicles can be displayed to the driver, sent to the RSU or even broadcasted to other vehicles depending on its nature and importance. The RSU distributes this data, along with data from road sensors, weather centers, traffic control centers, etc. to the vehicles and also provides commercial services such as parking space booking, Internet access and gas payment. The network makes extensive use of wireless communications to achieve its goals but although wireless communications reached a level of maturity, a lot more is required to implement such a complex system.

VANET makes each of the participating vehicles to a wireless node or router, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. Each and every vehicle in the network is expected to send message about its speed, location and direction for every 300 msec.

When the cars go out of its network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created. It is believed that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Ad hoc networks have been studied for some time but VANET will form the biggest ad hoc network ever implemented, therefore issues of stability, reliability and scalability are of concern. The general architecture of VANET communication along with Road Side Unit (RSU) is show in Fig. 1.

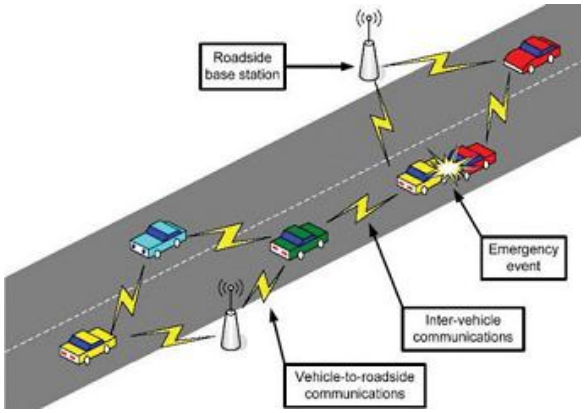

Fig.1 General VANET architecture

II. LITERATURE SURVEY

As a prime target of the quality of privacy in vehicular ad hoc networks (VANETs), location privacy is imperative for VANETs to fully flourish. Although frequent pseudonym changing provides a promising solution for location privacy in VANETs, if the pseudonyms are changed in an improper time or location, such a solution may become invalid. [6] It presents an effective pseudonym changing at social spots (PCS) strategy to achieve the provable location privacy. In particular, we first introduce the social spots where several vehicles may gather, e.g., a road intersection when the traffic light turns red or a free parking lot near a shopping mall. By taking the anonymity set size as the location privacy metric, we then develop two anonymity set analytic models to quantitatively investigate the location privacy that is achieved by the PCS strategy. In addition, we use game-theoretic techniques to prove the feasibility of the PCS strategy in practice.

Extensive performance evaluations are conducted to demonstrate that better location privacy can be achieved when a vehicle changes its pseudonyms at some highly social spots and that the proposed PCS strategy can assist vehicles to intelligently change their pseudonyms at the right moment and place. Vehicular Ad Hoc Networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists(CRLs) to reliably secure the network. In any PKI system, the authentication of a received message is performed by checking that the certificate of the sender is not included in the current CRL and verifying the authenticity of the certificate and signature of the sender. A Message Authentication Acceleration (MAAC) protocol for VANETs[7], which replaces the time-consuming CRL checking process by an efficient revocation check process. The revocation check process uses a keyed Hash Message Authentication Code (HMAC), where the key used in calculating the HMAC is shared only between non-revoked On- Board Units (OBUs). In addition, the MAAC protocol uses a novel probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key. By conducting security analysis and performance evaluation, the MAAC protocol is demonstrated to be secure and efficient.

III. EXISTING SYSTEM

VANETs adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. In any PKI system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. An Expedite Message Authentication Protocol (EMAP) for VANETs [2], which replaces the time-consuming CRL checking process by an efficient revocation checking process.

The revocation check process in EMAP uses a keyed Hash Message Authentication Code HMAC, where the key used in calculating the HMAC is shared only between non revoked On Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables non revoked OBUs to securely share and update a secret key. EMAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods employing CRL. By conducting security analysis and performance evaluation, EMAP is demonstrated to be secure and efficient but still it shows the following difficulties.

Drawbacks in existing system

- Many attacks can be done in this malicious message.

- The authentication delay using the linear CRL checking process.
- Delay in the checking process of the certificates.
- The end-to-end delay also increases with the number of revoked certificates.
- The message loss ratio increases.
- High communication cost.

IV. PROPOSED SYSTEM

Our proposed system is expected to overcome the drawbacks of the existing system. Each vehicle in VANET is assigned with a unique IP number along with its ordinary vehicle registration number. Thus a new vehicle is authenticated and authorized before it is registered with the main server. Vehicle's IP number and registration number is used in order to register it with the system. RSU authenticates each and every vehicle and its corresponding certificates before registering the vehicle with the system. The RSU receives messages from vehicles on the road. If there is any traffic jam or road damage or accident or any other undesirable situations occurring in the road, the nearby vehicle informs the RSU [3][4].

The RSU broadcast this alert message to other vehicles in the network. So that other vehicles may take an alternative route or take some other decision regarding the issue. By using malicious vehicular analyzer algorithm malicious vehicles can be detected. Each vehicle in traffic jam sends message to the RSU about the situation. RSU authenticates the user and the message, and then broadcast it to other vehicles in the network. This algorithm use countdown timer in order to identify the original warning message from malicious messages. When there is not enough messages within the specified time, the first message is considered fake and malicious hence that message is removed from the system and the vehicle trust limit is reduced.

Data stored and retrieved will be strongly encrypted using Elliptic Curve Cryptography algorithm [5]. Thus only encrypted data will be stored and retrieved from the storage system. Elliptic Curve Cryptography (ECC) will be used for secure transactions for message communication which might ensure its security for changes.

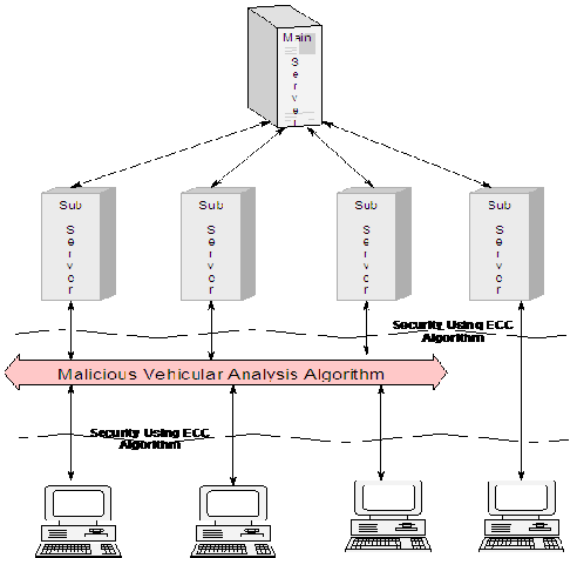

Fig. 2 System Architecture

Advantage of proposed system

- Monitors and handles all the suspected system involved in malicious activities.
- Elliptic Curve Cryptography is used for secure message transfer.
- Reduces message overhead.
- Traffic congestion control in the system.
- Economical than other existing mechanisms.

V. MODULES AND DESCRIPTION

- Registering new vehicles
- Receive emergency and warning messages from vehicles
- Securing using ECC
- Malicious Vehicular Analysis Algorithm

A. Registering New Vehicles

Each vehicle in VANET is assigned with a unique IP number along with its ordinary vehicle registration number. Thus a new vehicle is authenticated and authorized before it is registered with the main server. Vehicle's IP number and registration number is used in order to register it with

the system. Server authenticates each and every vehicle and its corresponding certificates before registering the vehicle with the system.

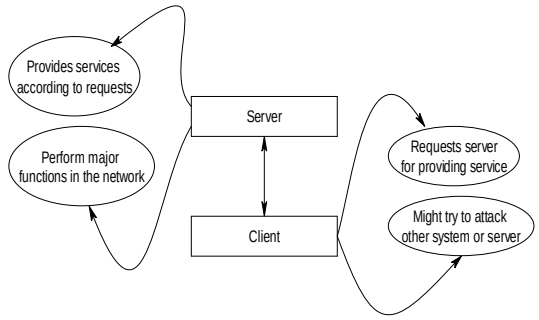

Fig. 3 Client and Server Connection

B. Receive Emergency and Warning Messages from Vehicles

The RSU receives messages from vehicles on the road. If there is any traffic jam or road damage or accident or any other undesirable situations occurring in the road, the nearby vehicle informs the RSU. The RSU broadcast this alert message to other vehicles in the network. So that other vehicles may take an alternative route or take some other decision regarding the issue.

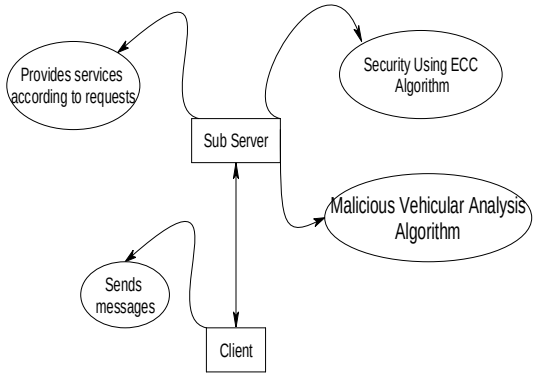

Fig. 4 Sub server Creation

C. Securing using ECC

Data stored and retrieved will be strongly encrypted using elliptic curve cryptography algorithm[5]. Thus only encrypted data will be stored and retrieved from the storage system. Elliptic Curve Cryptography (ECC) will be used for secure transactions for message communication which might ensure its security for changes.

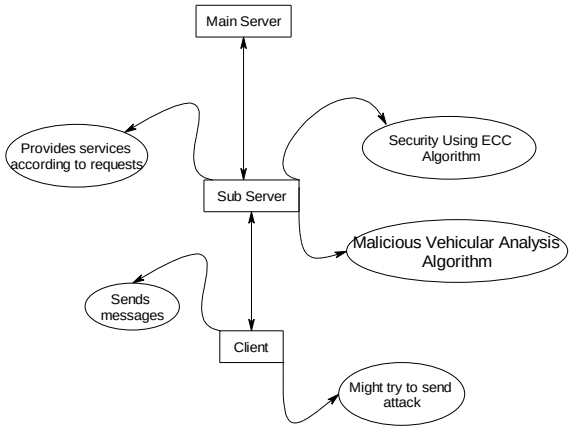

Fig. 5 Using ECC algorithm

D. Malicious Vehicular Analysis Algorithm

This algorithm is used to detect the malicious vehicles in the network. It considers 2 facts such as,

1. On board unit in each vehicle identifies traffic condition and sends message to RSU.
2. Traffic jam results due to the jamming of at-least more than 10 vehicles.

So each vehicle in traffic jam sends message to the RSU about the situation. RSU authenticates the user and the message, and then broadcast it to other vehicles in the network. This algorithm use countdown timer in order to identify the original warning message from malicious messages. When there is not enough messages within the specified time, the first message is considered fake and malicious hence that message is removed from the system and the vehicle trust limit is reduced.

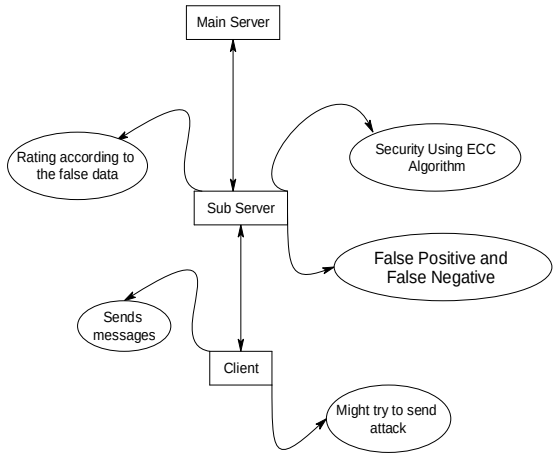

Fig. 6 Malicious Vehicular Analysis

VI. CONCLUSION

In the existing system we have problems like message attacks, authentication delay using the liner CRL checking process and delay in the checking process of the certificates. In addition to these disadvantages there are drawbacks like end-to-end delay increases with the number of revoked certificates, message loss ratio increases and high communication rate. We conclude that our proposed system will overcome all the drawbacks that are mentioned in the existing system.

REFERENCES

[1] G.M.T. Abdalla, M. A. Abu-Rgheff, and S. M. Senouci. "Current Trends in Vehicular Ad Hoc Networks," IEEE Global Information Infrastructure Symposium, Morocco July 2007.

[2] Albert Wasef,Xuemin Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks" published in Mobile Computing, IEEE Transactions on (Volume:12 , Issue: 1).

[3] Andreas Buchenscheit, Florian Schaub, Frank Kargl, and Michael Weber ,"A VANET-based Emergency Vehicle Warning System", published in Vehicular Networking Conference (VNC), 2009 IEEE.

[4] Chiasserini,C.F., Fasolo,E., Furiato, R., Gaeta,R., et al.(2005) "Smart Broadcast of Warning Messages in Vehicular Ad Hoc Networks" in Proceedings of the workshop Interno Progetto NEWCOM. Turin, Italy.

[5] Don Johnson, Alfred Menezes and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). Published in International Journal of Information Security, Vol. 1 (2001) pp. 36-63.

[6] "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs" by Rongxing Lu, Xiaodong Li, Luan, et al. Published in Vehicular Technology, IEEE Transactions on (Volume:61 , Issue: 1) .

[7] MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks by Wasef, A, Xuemin Shen Published in Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE.