ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 4, April 2016

Enhanced ID based Message Authentication and Secure Navigation in VANET

P.Savitha, A. John Clement Sunder, M.Balapriya

***Abstract*—Vehicular Ad-hoc Network is a new technology which takes an enormous attention in the recent years. In VANETs, authentication is one of the important security service for both inter-vehicle and vehicle roadside communications. Vehicles have to be protected from misuse of their private data and the attacks on their privacy, as well as investigated for accidents. In this paper, we introduce the public-key cryptography (PKC) to the pseudonym generation, for creating individual ID's for vehicles and also provides the navigation messages to the vehicles from the road side unit (RSU). The system also uses GPSR routing protocol to find the shortest path in case of congestion in the roads to reach the destination by using the navigation messages.**

***Index Terms*—** Authentication, GPSR, IBOOS, Navigation

I. INTRODUCTION

At the present time vehicles are used by many peoples. The biggest problems in increased use of private transport system leads to increase number of accidents on the roads. VANET provides a wireless communication among vehicles, using a dedicated short range communication (DSRC). DSRC is essentially IEEE802.11a amended for low overhead operation to 802.11p, the IEEE standardizes the communication stack by many families of standards referring to wireless access in vehicular environments (WAVE). VANET are divided into two types of communication, they are vehicle to vehicle communication (V2V) and vehicle to road side communication (V2R). These types of communications are used to share different kinds of information like, safety information for accident prevention and to avoid traffic jams. Other information like traveler related information which is considered as non-safety information. The sharing of this information is to provide a safety message to inform drivers about expected hazards which help to avoid the number of accidents. The GPSR routing protocol is commonly used to find the shortest path while transmitting the data packets.

In this paper, we mainly concentrate on the security of the network, for this purpose we propose an authentication framework by utilizing the IBOOS scheme for the V2R communication, and the V2V communication for better performance in network. In IBOOS, offline phase can be executed initially at RSUs and vehicles during the V2R communication, while the online phase is executed in vehicles during the V2V communication. We construct an efficient authentication framework with privacy preservation, by using the PKC-based pseudonyms and ID-based key management for the different kinds of communications in VANETs. If a malicious vehicle transmits a fraudulent authentication message, the trusted authority should be able to open the corresponding signature to trace the actual identity of the vehicle. In old days, there was no traffic signal and stop sign! So that many accidents occur because of drivers make mistakes easily. So, we have developed autonomous vehicle. It has the extraordinary capabilities.

Navigation is one of the important part in VANET which provides the correct and shortest path to reach the destination from the RSU. If any congestion happens in the road the RSU intimates the vehicle by navigation messages. In a VANET-based navigation system, a driver with the vehicle must be authenticated to ensure he is a valid subscriber of the system. So, communication messages in the system also authenticated to guard against the impersonation and message forgery attacks.

II. RELATED WORK

A. NETWORK STRUCTURE

A VANET consists of three network components road side units, vehicles and a regional trusted authority. The service of VANETs is divided into many different regions and each is served by one RTA which takes the control of the entire network. The wireless communication in VANETs takes place between the following two types, one is vehicle-to-roadside communication, and the other is vehicle-to-vehicle communication. Other communications are through secure wired channels, such as RSU-to-RTA and inter-RSU communication. By using these types of communication the information are shared between all vehicles without any loss in information. The network components and communication process in VANET are shown in fig.1 and the system shows the coverage area of RSU.

III. PRELIMINARIES

In this section, we introduce the public key cryptography (PKC) for pseudonym generation, the IBOOS for authentication between vehicles and RSUs. The conventional IBOOS schemes is not specifically designed for VANETs, we adapt the conventional scheme for VANETs. In this section, we provide the preliminary background of the PKC scheme, pairing for ID-based cryptography, as well as the IBOOS scheme, respectively for VANETs.

Manuscript received April, 2016.

***P.Savitha,** PG Student ,ECE Department, Bannari Amman Institute of Technology, Sathyamangalam, India.*

***A.John Clement Sunder,** Assistant Professor, ECE Department, Bannari Amman Institute of Technology, Sathyamangalam, India.*

***M.Balapriya,** PG Student ,ECE Department, Bnnari Amman Institute of Technology, Sathyamangalam, India.*

ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 4, April 2016

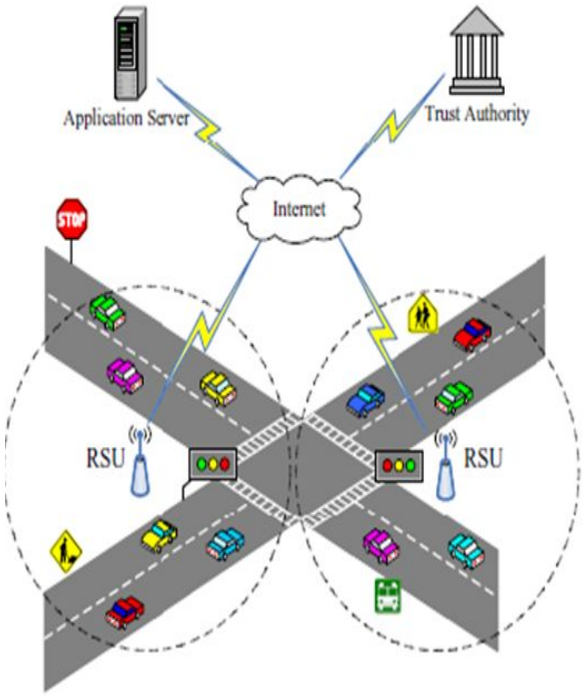

Fig.1 operations of proposed system

A. PUBLIC KEY CRYPTOGRAPHY

PKC is based on asymmetric key algorithms, in which different key are used to encrypt and decrypt a message. Many existing PKC schemes are available for pseudonym generation, such as RSA, HFE and NTRU. In the proposed method, each vehicle has a pair of cryptographic keys, i.e., a public encryption key (pkc) and a private decryption key (skc) shown in fig.2. The cryptographic key pairs are generated by the RTA periodically, and the public keys are transmitted to every RSU through secure channels. Each key (pkc) is broadcast to all vehicles by the RSU, while the corresponding private key (skc) is known only to the RTA. In this way, a vehicle can obtain a public key (pkc) and generate the PKC based pseudonym from the current public key, which can be decrypted only with the corresponding RTA's private key (skc).

B. IBOOS SCHEME FOR VANETS

An ID-based online/offline signature scheme in VANETs consists of five steps including setup, key extraction, offline signing, online signing and verification:

- Setup: The RTA computes a master key *s* and public parameter *param* for the private key generator (PKG), and gives *param* to all vehicles.
- Extraction: The RTA generates a private key *sek* associated with the ID using the master keys.
- Offline signing: Based on the *sek* and public parameters, the RTA/RSU generates an offline signature *SIGoffline* for each vehicle.
- Online signing: Based on the offline signature *SIGoffline* and a message M, the sending vehicle generates an online signature *SIGonline* of M.
- Verification: Based on the ID, M and *SIGonline*, the receiving vehicle outputs "accepts", only if the *SIGonline* is valid during verification and otherwise outputs "reject".

```
INITIALIZE THE LIST xListHead
Enter the option
1.New user
2.Enquiry
2
Enter the name
savi
Enter the key
1234
Enter the destination
1.Destination-1
2.Destination-2
3.Destination-3
1
Start of simulation...
```

Fig.2 Generation of keys

IV. MODULES DESCRIPTION

A. COMMUNICATION MODEL

Initially in VANET all the vehicles communicate together with a form of Vehicle to Vehicle communications or Vehicle to Road side (V2R) communication. Source node send RREQ to all the neighbors, when destination node receive the RREQ it will send RREP to source. Then it will update the routing table. It forwards the data in the same route. If any congestion happens in the road it sends the navigation messages to the vehicle as shown in the fig.3.

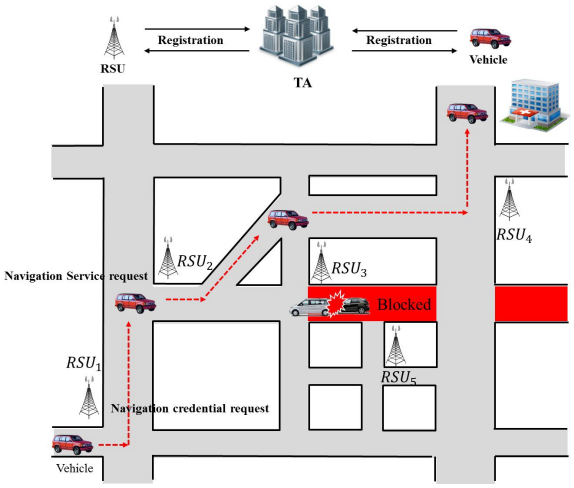

Fig.3 Road scenario

B. IBOOS SECURITY

ID-based online/offline signature scheme is suitable for the authentication scheme proposed. The scheme presents a method to convert any underlying signature scheme into an online/offline signature scheme. The offline signature scheme can be reused to sign more than one message. The security depends on Discrete Logarithm Problem. Unlike an IBOOS scheme presented in provides a direct online and offline signature scheme, does not require another underlying signature scheme. Verifying ECC signature is efficient for sensor nodes since we can set small verification exponents. This fact can be used in user authentication scheme, where sensor nodes verify only a signed user request. However, RSA signatures are large, resulting in a considerably

increased in message size. An ECC signatures are equally useful for signing and have short signature sizes. Therefore, ECC signatures are considered as more efficient than RSA signatures. To instantiate the authentication framework, the most efficient and secure ECC based signature schemes from the available IBOOS schemes are selected.

C. VEHICLE TRAFFIC CONTROL

VANET, all the vehicles have GPS for finding the location of the vehicle. Drivers can easily know exactly where he is. GPS with map is help to drive the vehicle. However, in many situationthe GPS receivers loss satellite signals and calculates the wrong positions because of signal blocking, reflection and interference. For example, the GPS report wrong information when they are in crowded area, where many tall buildings. The GPS receivers also loss satellite connections in places like tunnels or bridges, resulting in safety and convenience problem.

Registration process in the RSU

- All the users in VANET should register their details in RSU.
- After registration the RSU provides one initial packet key to the user.
- Using this packet key, all the user will get information about other nearby vehicles from the TA.

D. ROUTE DISCOVERY

If the source vehicle has no route to reach the destination vehicle, then source initiates the route discovery message in an on demand method. After generating RREQ packet, node looks up its own neighbor table to find it has any closer neighbor vehicle to reach the destination vehicle. If a closer vehicle is available, it forwards the RREQ packet to that vehicle. If no neighbor vehicle then the RREQ packet is flooded to all other neighbor vehicles. A destination vehicle replies to a received packet with a route reply (RREP) packet only in the following three cases:

- If the RREQ packet is the first to be received from the source vehicle
- If the RREQ packetscontains a higher sequence number than the RREQ packet previously respond to destination vehicle
- If the RREQ packet contains same source sequence number as that of RREQ packet previously respond to the destination vehicle, but new packet indicates a better quality route is available.

E. GPSR

In Greedy Perimeter Stateless Routing (GPSR) protocol, a node forwards a packet to an immediate next neighbor which is geographically very closer to the destination node. This type of forwarding of packet is termed greedy mode. If a packet reaches a local maximum, a recovery mode is used to forward a packet to a node which is closer to the destination than the nodes where the packet encountered the local maximum method. The packet resumes forwarding in greedy mode when it reaches a particular node whose distance to the destination is closer than the end node at the local maximum to destination.

GPSR uses two ways of forwarding the packets. One is greedy forwarding which is used to forward packets to the nodes which is closer to the destination and the another one is perimeter forwarding which forwards packet in the absence of greedy forwarding mode.

V. PERFORMANCE EVALUATION

A. SYSTEM SETUP

The nodes are placed according to the road transport system which are connected to the trusted authority shown in fig.4. The data is transmitted to all the nodes without any handoff in the network. It uses GPSR routing protocol to improve the performance of the vehicular networks and it also provides the navigation messages.

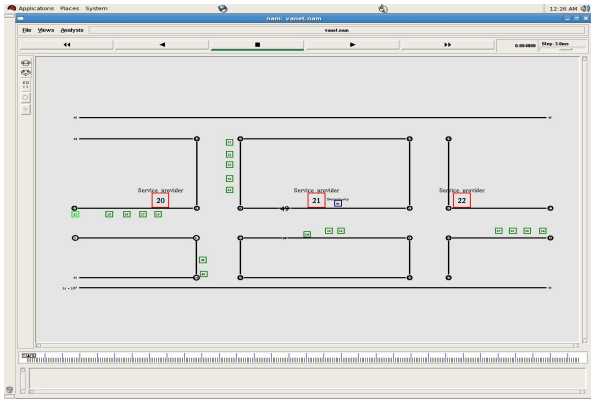

Fig.4 Node placement

B. OVERHEAD

The computation time indicates the computation overhead, which is the verification time used for the signature in online signature in IBOOS schemes shown in fig.5. The overhead increases due to increase in number of nodes in the network. The overhead of the vehicles increases when the vehicle movements are high then the capacity of the actual vehicle movement.

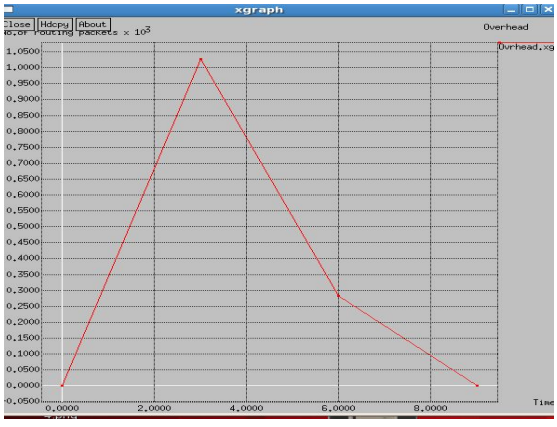

Fig.5 Overhead of packets

C. DELAY

The delay of a network defined as how long it takes for a bit of data that to travel across a network from one node or end point to another point. It is measured in multiples or fractions of seconds. Fig 6 shows the comparison of AODV

and GPSR routing protocol. Here the GPSR routing protocol delay is very less compare to the AODV routing protocol in the VANET system.

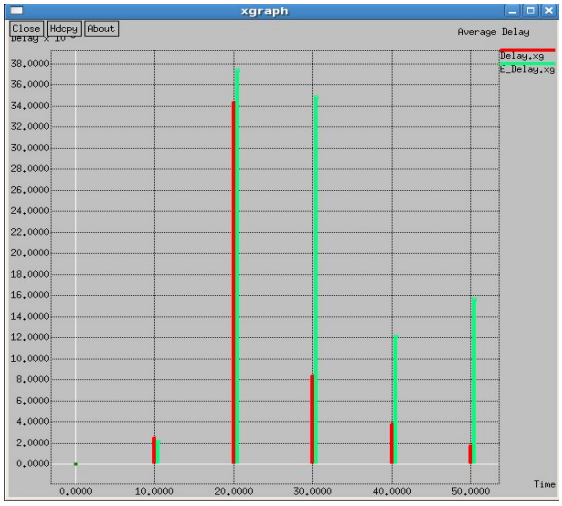

Fig.6 Delay

VI. CONCLUSION

In our proposed system, we are satisfying all the security and privacy requirements for VANETs along with the navigation messages, The vehicles which are registered can only participate in the information sharing in the network. By using this method the vehicle can complete the navigation querying process and receives immediate notification in a short time. The scheme preserves the privacy of the vehicle. The RSU is acts as a mediator for authentication in both the RSU and the vehicle. The vehicles use efficient routing protocol to improve the performance of the network.

REFERENCES

1. X. Lin, "TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving," IEEE Trans. Wireless Comm., vol. 7, no. 12, pp. 4987-4998, Dec. 2008.
2. N. V. Pardakhe et al., Detecting Shortest Path Using Vehicular Routing Protocol, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 9, September 2015
3. Miao Wang et al., Real-Time Path Planning Based on Hybrid-VANET-Enhanced Transportation System, IEEE Transactions on vehicular technology, vol. 64, no. 5, may 2015
4. T.W. Chim et al., VSPN: VANET-based Secure and Privacy-preserving Navigation, IEEE Transactions on computers 2014
5. R. Lu et al., "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," Proc. IEEE INFOCOM, pp. 1229-1237, 2008.
6. Y. Sun et al., "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010
7. J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.
8. F.R. Yu et al., "A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks," IEEE Trans. Network and Service Management, vol. 7, no. 4, pp. 258-267, Dec. 2010.
9. M. Gerlach and F. Guttler, "Privacy in VANETs Using Changing Pseudonyms—Ideal and Real," Proc. IEEE Vehicular Technology Conf. (VTC-Spring), pp. 2521-2525, 2007.
10. J. Sun, C. Zhang, and Y. Fang, "An ID-Based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks," Proc. IEEE Military Comm. Conf. (MILCOM), pp. 1-7, 2007.
11. S. Zeadally et al., "Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges," Telecomm. Systems, vol. 50, no. 4, pp. 217-241, 2012.
12. Sabahi, F., "The Security of Vehicular Adhoc Networks," Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on, vol., no., pp.338, 342, 26-28 July 2011.
13. Ebers, S.; Fischer, S., "Poster: Adapter framework for VANET simulators," Vehicular Networking Conference (VNC), 2014 IEEE , vol., no., pp.193,194, 3-5 Dec. 2014
14. Belmerhnia, L.; Djermoune, E.-H.; Brie, D., "Greedy methods for simultaneous sparse approximation," Signal Processing Conference (EUSIPCO), 2014 Proceedings of the 22nd European, vol., no., pp.1851, 1855, 1-5 Sept. 2014.
15. S. Bououden, M. Chadli, H.R. Karimi, An ant colony optimization based fuzzy predictive control approach for nonlinear processes, Information Sciences, Volume 299, 1 April 2015, Pages 143-158.
16. Qingzi Liu; Qiwu Wu; Li Yong, "A hierarchical security architecture of VANET," Cyberspace Technology (CCT 2013), International Conference, vol., no., pp.6, 10, 23-23 Nov. 2013.
17. Jie Li and Huang Lu "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs" vol. 26, no. 4, 2015
18. C. C. Lee and Y. M. Lai, "Toward a secure batch verification with group testing for VANET," Wireless Networks, vol. 19, no. 6, pp. 1441-1449, 2013.
19. C. Zhang, P. H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," Wireless Networks, vol. 17, no. 8, pp. 1851-1865, 2011.
20. Pras Vehical Mohapatra and S. Krishnamurthy."Ad Hoc Networks: Technologies and protocols‖." Springer Science and Business Media, Inc, Chapter 1, 2004.