ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2014

Privacy Protection against Man-In-The-Middle Attacks in Vehicular Ad hoc Networks

R.Jebima Ravi[1]

PG Student [CS], Dept. of ECE, Dhanalakshmi Srinivasan College of Engineering, Coimbatore, Tamilnadu, India [1]

ABSTRACT: In vehicular Ad hoc Networks, the privacy protection is one of the major requirements. Since there are huge number of vehicles on our highways and city roads there must be possibility of attacks. To protect the privacy of vehicles, one solution is to hide the vehicle's identity with the use of pseudonym keys (i.e, temporary identities). Each vehicle uses its pseudonym key to communicate with other vehicles and road side units. The main effort of this work is to provide a solution towards privacy protection in vehicular Ad hoc Networks. Initially, we view vehicular ad hoc networks having non-overlapping sub networks referred to be a cell. Each cell with small geographic area having a pseudonym server which generates a list of pseudonyms using capacity planning algorithm. The Diffie Hellman Key Exchange scheme is also used to increase privacy protection. Our another effort is to reduce the routing overhead by using Hybrid Location based Ad hoc Routing (HLAR) protocol for routing pseudonyms and further communication. The accurate results are obtained and the performance is compared with reactive by detailed simulations.

KEYWORDS: Vehicular Ad hoc Networks, Hybrid Location based Ad hoc Routing, Diffie Hellman Key Exchange, privacy.

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) are highly mobile wireless network technology that is implemented to help traffic monitoring, vehicular safety, and other commercial applications. A vehicular ad hoc network uses moving vehicles as nodes in a network in order to create a mobile network. An accurate position of vehicles can be estimated by using global positioning systems or on-board sensors. VANETs are used for short range, high-speed communication among nearby vehicles, and between vehicles and roadside infrastructures.

Within VANETs, there are huge number of vehicles on our highways and city streets, leads to possibilility of severe attacks and routing overhead [6]. So the scalable and robust privacy protection must be needed. In this paper, the Diffie Hellman Key Exchange technique is used in order to improve privacy protection especially solves man-in-the-middle-attacks. Then the routing overhead is also reduced by using hybrid location based Ad hoc routing.

II. RELATED WORKS

II.A. A CERTIFICATE AUTHORITY AND REACTIVE ROUTING BASED PRIVACY

There are many challenges for the protection of privacy in vehicular ad hoc networks due to large mobility, to the characteristics of traffic flow, to the correlation among each vehicle and its driver, and to the high population of vehicles. The scalability and robustness are promoted by employing a combination of two strategies. First, the vehicular networks are viewed as non-overlapping sub networks and each local to a geographic area referred to as a cell. Depending on the topology and the nature of the area, these cells may be as large as few city blocks or, indeed, may comprise the entire downtown area of a smaller town. Each cell has a server that maintains a list of pseudonyms that are valid for use in the cell. Each pseudonym consists of the cell's ID and of a random host ID. The public and private keys of each vehicle and infrastructure are assigned and maintained by a Certificate Authority (CA) [1].

Also, instead of issuing pseudonyms to vehicles proactively, as virtually all existing schemes do, the pseudonyms are issued to those vehicles that need them, and also request them. Prior to communicating with either the infrastructure or with other vehicles in the cell, vehicles need to request pseudonyms from the cell server. The pseudonyms are intended to hide the real identity of vehicles, either their host name, or IP address.

II.B. A SCALABLE ROBUST AUTHENTICATION PROTOCOL BASED PRIVACY

A decentralized authentication protocol uses RSUs to maintain a group within their communication range, which is normally much longer than the V2V communication range, is used. Vehicles can anonymously broadcast V2V messages that can be verified by other vehicles in the group and neighboring groups. In this system, vehicles only request a new secret member key when they pass by an RSU for the first time or when their existing secret member keys expire. Since each vehicle only verifies messages from vehicles that have moved into the range of the same RSU and its neighbors, it can easily check whether the anonymous sender was revoked with the help of those RSUs and does not need to retrieve the revocation list from a remote centralized authority. This greatly reduces the certificate management overhead [4].

Although each party in this system needs a secret member key, the system's master key is only known and stored by a centralized authority, rather than being stored in each tamper proof device that is embedded in vehicles.

II.C. SYMMETRIC RANDOM KEYSET BASED PRIVACY

A group based privacy preserving authentication protocol for vehicular networks is used. A symmetric random key set is used for anonymously privacy-preserving authentications in vehicular networks. The random keyset based authentication protocol that preserves user privacy under the zero-trust policy, in which no central authority is trusted with the user privacy is used. In the zero-trust policy, vehicles trust neither public nor private servers nor networks [2].

The privacy-preserving authentication protocol can efficiently authenticate users without compromising their privacy using malicious user identification and key revocation. This system also takes the advantage of the shared keys between different random sets to achieve anonymity. The anonymity is further enhanced by using independent keys for authentications at neighboring RSUs.

III. SYSTEM DESIGN AND IMPLEMENTATION

III.A. DESIGN CRITERIA

The Network Simulator version 2.32 is chosen to simulate VANET and evaluate the protocols. It is an object oriented, discrete event driven, open source network simulator. It has notable advantages when compared to other simulators. In VANETs, the number of nodes can exceed several thousands and it has more efficient routing tables, which can be easily simulated. It is easy to debug errors. It is a binded model between c++ and OTCL. Wireless network performance mainly depends upon end to end throughput and average delay. It is cost effective of network deployment as wiring is not possible.

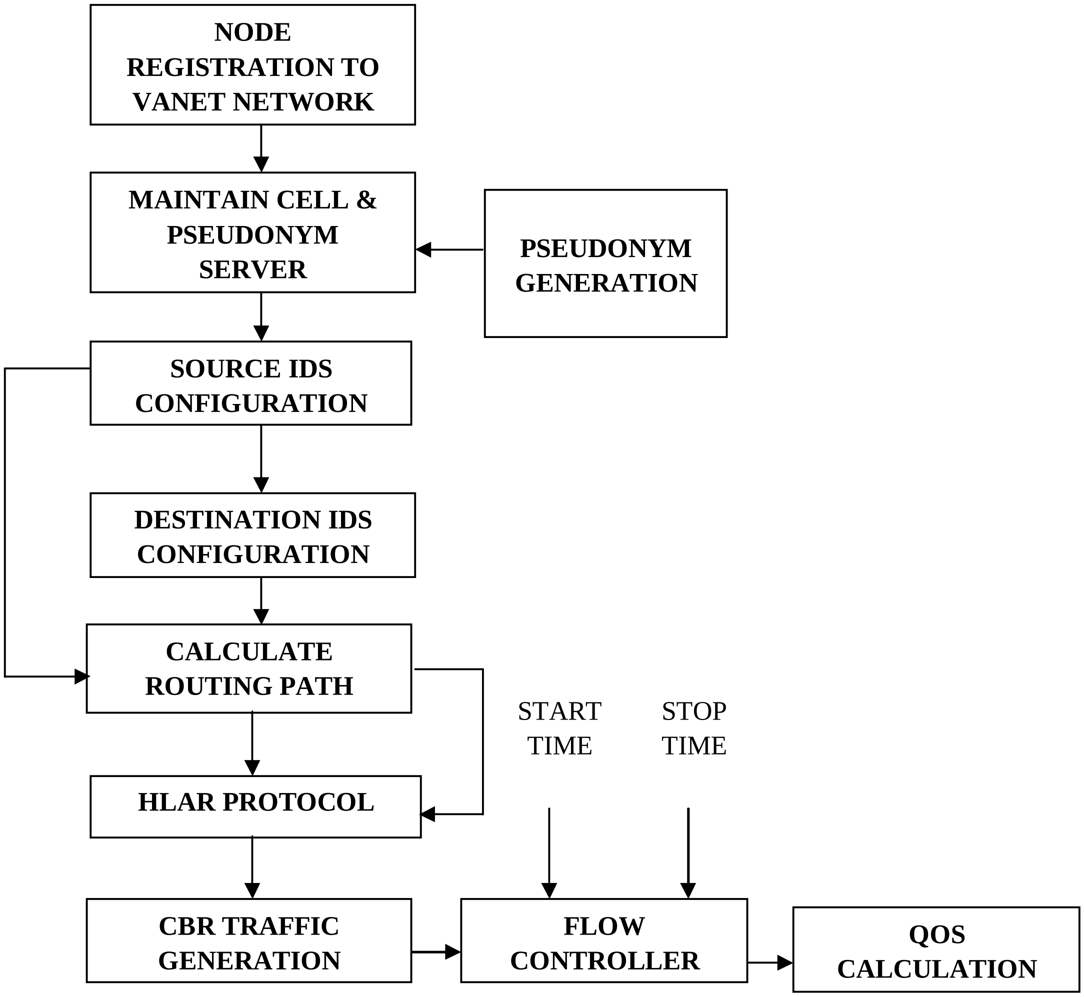


Fig.1 Process Flow

The Fig.1 shows the process flow which includes node registration, maintenance of pseudonym server, pseudonym generation, source and destination configuration, routing path calculation, constant bit rate data generation.

Initially the nodes are designed and registered to the Vehicular Ad hoc Networks. In Vehicular Ad-hoc Network there is no fixed topology. The topology is changeable. The nodes move with variety of velocity in various directions. Vehicular Adhoc networks are clustered into non-overlapping sub networks, each local to a geographic area referred to as a cell. Each cell has a server that maintains a list of pseudonyms valid for use in the cell. A capacity planning scheme which allows server to predict, by taking into account the time-varying attributes of the traffic, the probability that a given number of pseudonyms will be required at a certain time as well as the expected number of pseudonyms in use in a cell at a certain time. Then the source node and destination node are configured and identify whether the destination node is within the coverage area of source node by sending request packets to the destination node. If the destination node is not within in the coverage area, the source nodes transmit packets through the intermediate nodes. The routing path is calculated based on the Hybrid Location based Ad hoc Routing (HLAR) mechanism.

III.B. PROTOCOLS AND ALGORITHMS CHOSEN

III.B.i. HLAR PROTOCOL

A hybrid location-based ad hoc routing (HLAR) protocol combines a modified AODV protocol with a greedy-forwarding geographic routing protocol. HLAR protocol has the features of reactive routing with location-based geographic routing. It efficiently make use of all the location information available, to minimize the routing overhead, and to gracefully exit to reactive routing as the location information degrades [3]. Each node will have two separate tables, which were locally constructed from the beacon packets: 1) a neighbor table, which will be used to perform geographic routing, and 2) an “ETX” table, which will be used to construct the AODV route (the AODV routing table) upon request to obtain optimal scalability performance.

III.B.ii. DIFFIE HELLMAN KEY EXCHANGE

The Diffie Hellman Key Exchange Scheme establishes shared secret key among unknown vehicles over an insecure communication medium [4]. It improves privacy protection in wireless networks especially the passive attacks.

III.B.iii. CAPACITY PLANNING SCHEME

A capacity planning scheme allows system servers to predict, by taking into account the time-varying attributes of the traffic, the probability that a given number of pseudonyms will be required at a certain time as well as the expected number of pseudonyms in use in a cell at a certain time [1]. Based on the prediction, the pseudonym server generates pseudonyms for a cell at a time.

IV. SIMULATION AND RESULTS

The simulation is done by using a Network Simulator version 2.32 software. Initially the nodes are designed as per the requirement. In this simulation we have designed 19 nodes. The nodes are the vehicles that take part in communication. They transmit packet among themselves. The coverage area of each node is 100m. Then the nodes are register to the Vehicular Ad hoc Networks. In Vehicular Adhoc Network there is no fixed topology. The topology is changeable. The nodes move with variety of velocity in various directions.

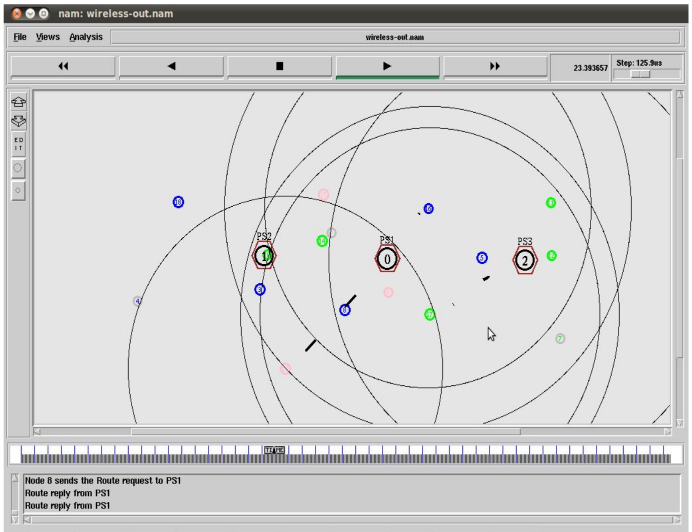
Vehicular Adhoc networks are clustered into non-overlapping sub networks, each local to a geographic area referred to as a cell. Each cell has a server that maintains a list of pseudonyms valid for use in the cell. The source node and destination node are configured and identify whether the destination node is within the coverage area of source node by sending request packets to the destination node. If the destination node is not within in the coverage area, the source nodes transmit packets through the intermediate nodes. The routing path is calculated based on the Hybrid Location based Adhoc (HLAR) routing mechanism. It efficiently make use of all the location information available, to minimize the routing overhead, and to gracefully exit to reactive routing as the location information degrades.

TABLE 1

SIMULATION PARAMETER

Channel	Wireless Channel
Propagation	Two Ray Ground
Mac	802_11
Queue	Drop Tail, Priority
Antenna	Omni Antenna
Queue Length	50
Number of nodes	19
Routing Protocol	HLAR

The Table 1 shows the simulation parameters such as channel, propagation, queue, antenna, queue length, number of nodes, and routing protocol.



```
Node 8 sends the Route request to PS1
Route reply from PS1
Route reply from PS1
```

Fig.2 Network Topology

Fig.2 represents the network topology using Network Simulator 2.32. Here 19 nodes are assigned. The circle represents the coverage area of nodes. Here the coverage area of each node is 100m. The black bars represents the data transmission. The nodes 0, 1, and 2 are pseudonym servers and remaining nodes are moving vehicles. There is data transmission between vehicles and pseudonym servers.

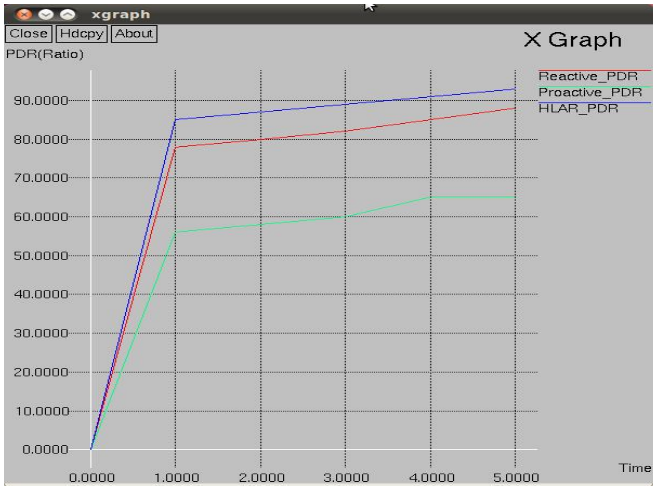


Fig.3 Delivery Ratio

In Fig.3, the packet delivery ratio of the vehicular network increases with time. Here the packet delivery ratio of HLAR protocol is better compared to the Pro active and Re active protocols. The packet delivery ratio of HLAR protocol is high because of low packet loss.If the destination node is not within in the coverage area, the source nodes transmit packets through the intermediate nodes. The routing path is calculated based on the Hybrid Location based Adhoc (HLAR) routing mechanism. It efficiently make use of all the location information available, to minimize the routing overhead, and to gracefully exit to reactive routing as the location information degrades.

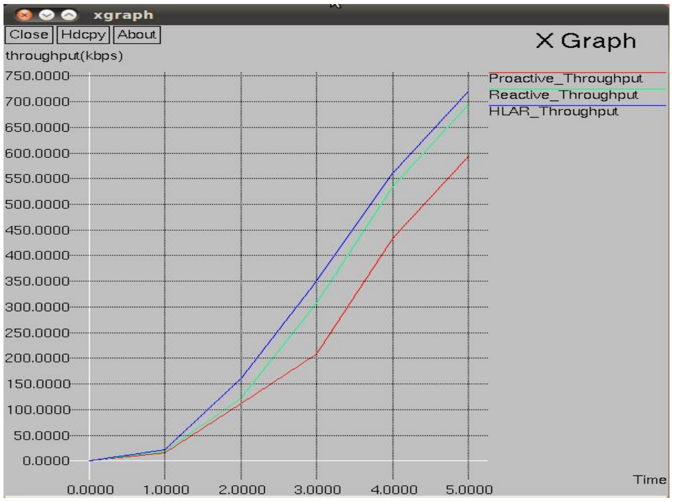


Fig.4 Throughput

In Vehicular Ad hoc Network using HLAR algorithm and Diffie Hellman Key Exchange, the routing overhead get decreased and the privacy gets improved. Since there is no need to route packets to all vehicles, the packet delivery rate is very high. So the throughput gets increases. In Fig.4, the throughput of the vehicular network increases with time. The throughput of HLAR protocol is better when compared to Pro active and reactive protocol Since the packet loss and packet delay are low.

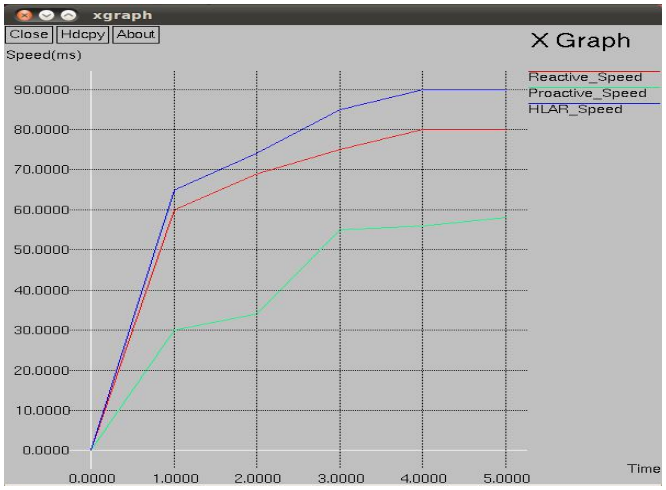


Fig.5 Speed

In Vehicular Ad hoc Network using HLAR algorithm and Diffie Hellman Key Exchange, the routing overhead get decreased and the privacy gets improved. Since there is no need to route packets to all vehicles, the packet delivery rate is very high. So the throughput gets increases. In Fig.5, the Speed of data transmission decreases when time increases. The speed of HLAR protocol is better when compared to Pro active and Re active protocols because the delay in HLAR protocols is very low.

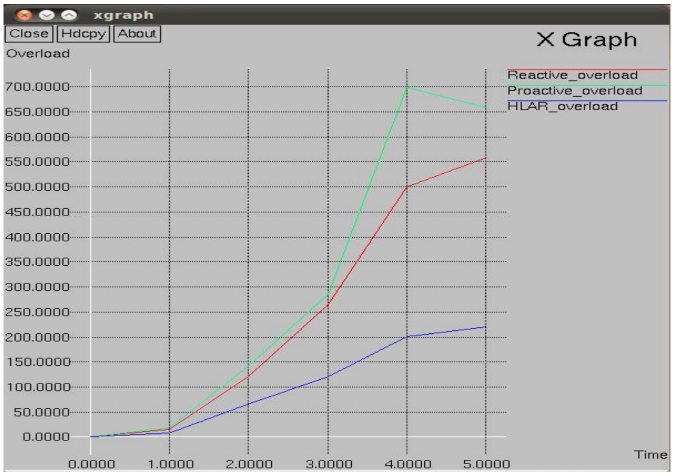


Fig.6 Overload

In Vehicular Ad hoc Networks using HLAR algorithm and, the routing overhead get decreased. So the delay gets reduced and speed gets improved. In Fig.6, the routing overload of the data transmission decreases with time. The routing overload of HLAR protocol is less compared to the Pro active and Re active routing protocols because the HLAR protocol uses Re active routing with location based routing.

V. CONCLUSION

In this paper we have proposed a Diffie Hellman Key Exchange scheme in which a shared secret key is used to improve the privacy protection especially against the passive attacks in vehicular ad hoc networks. Then the HLAR protocol has the feature of switching between location based routing and the re active routing is used to reduce the routing overhead in vehicular ad hoc networks. Also the throughput, packet to delivery ratio and Speed gets increased. NS2 is chosen to simulate this algorithm and analyze the graphical results.

For further work we concentrate on a Directed clustering Protocol (DCP) [7] that increases the life time of network can be used together with the HLAR Routing algorithm. DCP is a clustering algorithm. Clustering is a new approach to efficiently utilize the energy of sensor nodes. This routing mechanism will come up with better throughput, energy consumption and less packet loss.

REERENCES

[1] Arif. S, Khalil. I, Olariu. S, Wang. J, Yan. G and Yang. W, (2013), “ Towards providing Scalable And Robust Privacy In Vehicular Networks,’ IEEE Transactions On Parallel And Distributed Systems, Vol. 99, pp.45-30.

[2] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, “Enforcing privacy using symmetric random key-set in vehicular networks,” in Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems, 2007, pp. 344–351.

[3] Mohammad Al-Rabayah and Robert Malaney, “A New Scalable Hybrid Routing Protocol for VANETs”, IEEE Trans. Vehicular technology, vol. 61, no. 6, July 2012.

[4] G. Yan, W. Yang, D. B. Rawat, and S. Olariu, “A Scalable Robust Authentication Protocol for Secure Vehicular Communications,” IEEE Transactions on Vehicular Technology, Vol. 59, No. 4, pp. 1606-1617, May 2010.

[5] P. C. Kocher, “Timing Attacks on Implementations of Diffie–Hellman, RSA, DSS, and Other Systems,” In Advances in Cryptology—Crypto 1996, Vol. 1109, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1996, pp. 104–113.

[6] Rakesh Kumar, Mayank Dave, “A Comparative Study of Various Routing Protocols in VANET**”,** IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

[7] R. Senthil Kumaran and P. Paruthi Ilam Vazthuthi, “A New Cluster based Protocol for Wireless Sensor Actor Network” CiiT International Journal of Networking and Communication Engineering, June 2012.

[8] J. Sun, C. Zhang, Y. Zhang, and Y. M.Fang, “An identity-based security system for user privacy in vehicular ad hoc networks,” IEEE Transactions on Parallel Distributed System, vol. 21, pp. 1227–1239, September 2010.

[9] G. Yan, S. Olariu, and M. Weigle,“Providing location security in vehicular ad hoc networks,”IEEE Wireless Communications, vol. 16, no. 6, pp. 48 – 55, 2009.

[10] G. Yan, S. Olariu, and M. C. Weigle, “Providing location security in vehicular ad-hoc networks,” IEEE Wireless Communications, Special Issue on On-the-Road Communications, vol. 16, no. 6, pp. 48–55., Dec 2009.

[11] G. Yan, S. Olariu, and M. C. Weigle, “Providing VANET security through active position detection,” Computer Communications: Special Issue on Mobility Protocols for ITS/VANET, vol. 31, no. 12, pp. 2883–2897, Jul. 2008.