ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 10, pp. 20557-20560, October, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

THE DUAL AUTHENTICATION AND KEY MANAGEMENT TECHNIQUES FOR SECURE DATA TRANSMISSION IN VEHICULAR AD HOC NETWORK

Shanmugapriya K and Saraswathi K

Department of Computer Science, Government Arts College (Autonomous)
Coimbatore, Tamilnadu, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0810.0915

ARTICLE INFO

Article History:

Received 15th July, 2017
Received in revised form 25th August, 2017
Accepted 23rd September, 2017
Published online 28th October, 2017

Key Words:

Dual Authentication VANET key Management, Vehicle Secret Key, Hierarchical Privacy Preserving Pseudonym Authentication Protocol(HPPPAP).

ABSTRACT

In mobile computing, the Vehicular Ad-hoc Networks (VANET) plays the most important role in transfering informations, weather conditions, and road conditions. The main goal is to enhanc security, quick decision making and authenticated communication in the VANETs system. The authentication may be the user personal information of useer like the identity and location information. Privacy in mainly improved in the of a VANET system. The dual authentications provide high level security in the vehicle side for preventing the unauthorized vehicles entering into the VANET. The Hierarchical Privacy Preserving Pseudonym Authentication Protocol is proposed for preserving the privacy of location of vehicles from the intruders.

INTRODUCTION

Vehicular Ad-hoc Network is considered as a special class in Mobile Ad-hoc networks (MANET) that consists of number of vehicles the capability of communicating with each other without a fixed infrastructure. In Vehicular Ad-hoc Networks, the vehicles are able to communicate with the other on-going vehicles, fixed infrastructure and road-side unit (RSU) for the benefit of passenger's safety, concern and comfort. Vehicles communicate with the other moving vehicles in its vicinity, as it supports highly dynamic network topology with high speed, self-configured and decentralized constraints.

LITERATURE SURVEY

Vehicular ad hoc networks (VANETs) [1] has appealed a lot of research interests from academic circles and consumption efforts in industries. The VANETs system predicts the location through the road side units which is embedded with the vehicle. The developments of intelligent transportation system [2] mainly improves road safety and driving conditions.

The Pseudonym certificate [3] are the states of the art approach for secure and privacy friendly message authentication in VANETs.

This paper mainly surveys the benefits and limitations of the VANETs [4] and also explores the newest trends in privacy, anonymity, misbehaving nodes, the broadcasting of false information and secure data aggregation.

A Novel Adaptive Role playing (ARP) [5] strategy is proposed to enable VANET nodes in each hop to countermeasure the malfunctions and misbehaviors of individual nodes.

The efficient and secure payment protocol [6] proposed for restricted the connectivity scenario in VANET.

Dynamic privacy preserving key management scheme (DIKE) [7] proposed for improving the key update efficiency of location based services (LBSs) in VANETs.

An efficient and privacy aware revocation mechanism (EPA) [8] on the use of Merkle Hash tree (MHT) and crowds based anonymous protocol.

Existing Method

In existing system, dual authentication scheme with intelligent decision making was proposed for vehicle movement. The main objective of developing a dual authentication scheme was to improve the security in the vehicle side. The dual

Corresponding author:* **Shanmugapriya K
Department of Computer Science, Government Arts College (Autonomous) Coimbatore, Tamilnadu, India

authentication scheme depends on the vehicle secret key (VSK) which is given to the user during the time of registration by the Trusted Authority (TA) and the fingerprint of the individual user. To provide secure and reliable data transmission facility based on group communication in VANETs, a dual key management scheme was developed.

Issues in the Existing System

The privacy of vehicle's location from the intruders was preserved.

In some case, communication and storage overhead in group communication were expensive.

The performance of authentication delay cannot be guaranteed for multiply transmissions, especially when the packet low rate is high.

Proposed Work

In the proposed system, an efficient hierarchical pseudonymous authentication protocol with conditional privacy preservation is proposed and incorporated with the dual authentication and key management system. The proposed protocol is based on the idea of primary pseudonyms with relatively longer time periods that are used to communicate with semi-trusted authorities and secondary pseudonyms with a smaller life time that are used to communicate with other vehicles. The proposed protocol protects a user's privacy until the user honestly follows the protocol. In case of a malicious activity, the true identity of the user is revealed to the appropriate authorities.

Overview of Proposed System

- System Model
- Attack Model
- Dual Authentication and Key Management Protocol
- Hierarchical Privacy Preserving Pseudonyms Authentication Protocol
- Performance Evaluation

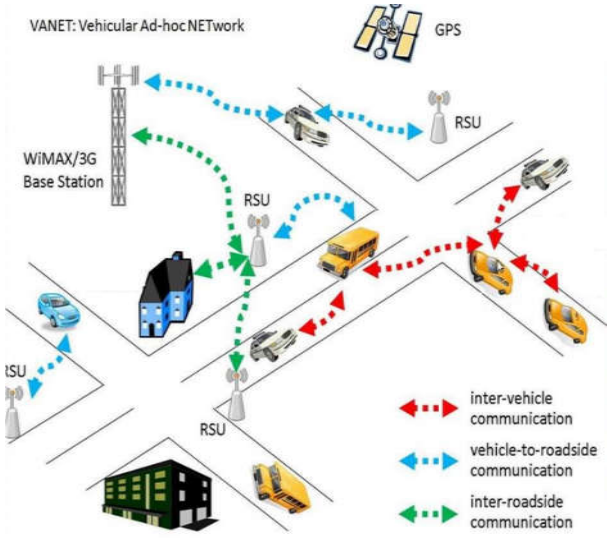

Figure 1 Architecture of VANET

Fig 1 Shows that the Road side unit plays a vital role in identifying the malicious node packets and clears those packets with correct packets with respect to all the vehicles in the scenario.

System Model

Trusted Authority

The TA is handling for the registration of RSUs, vehicle OBUs and the vehicle users and it is also in charge for key generation and distribution to support secure premium services in the VANET system.

Certification Authority (CA)

The CA provides the primary pseudonyms and keeps the association between the primary pseudonyms and the encrypted VID of vehicles.

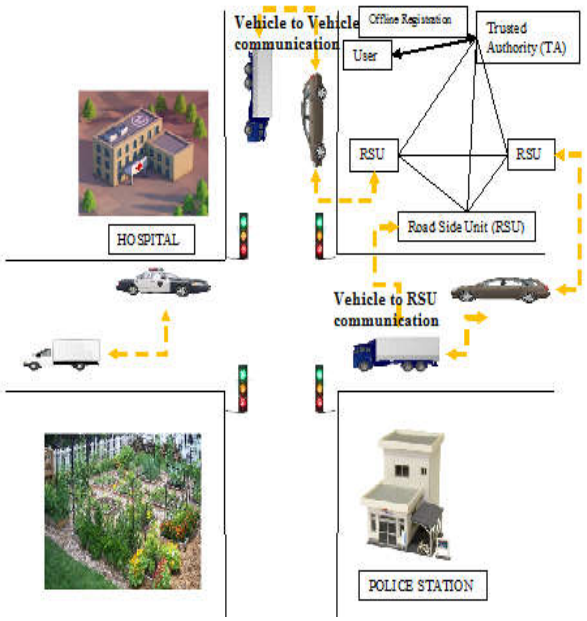

Figure 2 System Model

Road side unit (RSU)

RSUs are deploying at the roadsides and they regularly monitored the vehicles RSUs are managed by the TA.

Vehicles

Each vehicle contains On Board Unit (OBU) in the VANET system. By using OBU and RSUs the vehicle can communicate each other.

Sender Vehicle

The sender vehicle is mainly used to open the beacon message by using the private key.

Receiver Vehicle

The receiver vehicles confirm the message by using associated key.

Dual Authentication Key Management protocol
Registration through Offline Mode

The VANET's first approach is to directly visit the TA office while the time of registration and provide valid details such as name, address, phone number, email id etc. During the registration time the user must his or her fingerprint to the TA office. once the registration process is completet the TA

generates a unique secret key and send to every users. The TA maintains all the secret data with security.

Performance Comparison

In the performance evaluation of VANETs system the pseudonym protocol increase the privacy in between the TA, RSUs and users. Then restrict to leakage of the information through group management scheme. In existing system the information leakage occurs through group members. The proposed protocol performance evaluated by end to end delay, throughput and packet delivery ratio. The RSUs performance measured by evaluating the loss of packets at the time of receiving requests from vehicle and providing secondary pseudonym.

Merits in the Proposed System

- The privacy of vehicle's location is preserved.
- The communication and storage overhead are reduced.
- The computational complexity is also reduced.
- Applicability and feasibility are increased

SIMULATION AND RESULTS

Performance Evaluation

The performance evaluation presents the experimental results that are performed to prove the Hierarchical Privacy Preserving Pseudonym Authentication Protocol is achieving high security. The performance of the proposed Hierarchical privacy preserving pseudonym authentication protocol evaluated in terms of End to End Delay, Packet Delivery Ratio and Throughput using the NS2-Simulator.

End to End Delay

End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination. It is a common term in IP network monitoring, and differs from round-trip time (RTT).

$$\text{Average End to End Delay} = \frac{\text{sum of end to end delays for all received packets}}{\text{Total number of packets received by the sink node}}$$

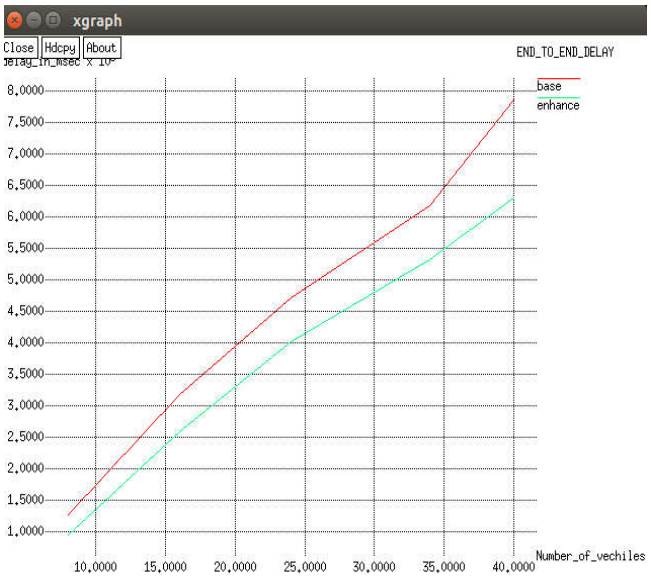

Figure 3 Comparison of End to End Delay

Fig 3 Shows that the Proposed algorithm is better than the existing algorithm. From the graph, we observed that comparison of end to end delay in terms of delay. In the X-axis no of vehicles taken and in the Y-axis delay taken.

Packet Delivery Ratio

The packet delivery ratio is defined as the number of data packets delivered to destination the number of data packets delivered to the receivers.

$$\text{Delivery Ratio} = \frac{\text{Packets Delivered}}{\text{Packets sent}}$$

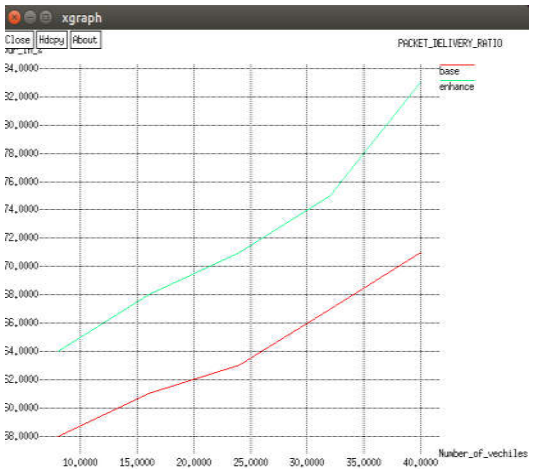

Figure 4 Comparison of Packet Delivery

Ratio

Fig 4 Shows that the comparison of packet delivery ratio. The analysis of the above graph proves that the proposed method increasing compare to existing method. In the X-axis no of vehicles taken and in the Y-axis packet delivery taken.

Through put

Throughput refers to how much data can be transferred from the source to the receiver in a given amount of time.

$$\text{Through put} = \frac{\text{Number of Packet Sent}}{\text{Time Taken}}$$

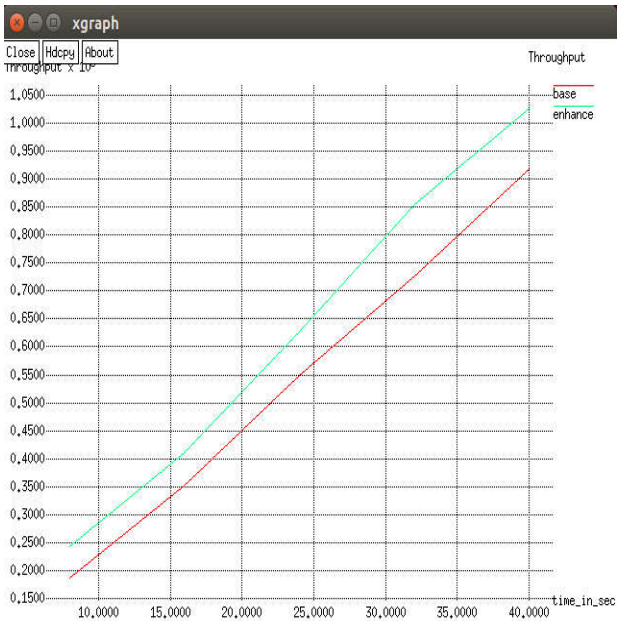

Figure 5 Comparison of Throughput

Show that the comparisons of throughput. The analysis of the above graph proves that the proposed method increasing compare to existing method. In the X-axis no of vehicles taken and in the Y-axis throughput value taken.

CONCLUSION

The proposed method is hierarchical privacy preserving pseudonym authentication protocol with conditional privacy preserving pseudonym. The proposed protocol is used to increase the security and also provides conditional anonymity in the VANETs. The proposed protocol exhibits several advantages over current approaches such as less trust on CA, RA and RSU and no disclosure of valuable information in case of attacks on these entities. Moreover, the protocol provides conditional anonymity to the users of the network and only the involvement of a vehicle in a malicious activity reveals the real identity. The protocol incurs no overhead related to CRL and group management tasks that are otherwise used consistently by current approaches. The security analysis of the proposed protocol exhibits the resilience against various security threats. Furthermore, the performance evaluation of the proposed protocol not only shows the low computational and communication overhead, but also shows the applicability by showing little or acceptable difference in network performance in comparison with the beacons without any security. The performance shows that increased security and efficiency in terms of End to End Delay, throughput, Packet Delivery Ration.

Future Work

In future, which include the proposed protocol with more number of RSUs in Urban and high way scenarios and improve the scheme for the given accurate prediction models. For some vehicular applications, it is also important to consider the privacy issues. The research will address how to satisfy both security and privacy requirements in the future work.

References

1. Huang, J. L., Yeh, L. Y., & Chien, H. Y. (2011). ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 60(1), 248-262.
2. Mejri, M. N., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2), 53-66.
3. Förster, D., Kargl, F., & Löhr, H. (2016). PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. *Ad Hoc Networks*, 37, 122-132.
4. Rivas, D. A., Barceló-Ordinas, J. M., Zapata, M. G., & Morillo-Pozo, J. D. (2011). Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation. *Journal of Network and Computer Applications,* 34(6), 1942-1955.
5. Li, Z., & Chigan, C. (2011). LEAPER: A lightweight reliable and faithful data packet relaying framework for VANETs. Ad Hoc Networks, 9(3), 418-429.
6. Li, W., Wen, Q., Su, Q., & Jin, Z. (2012). An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network. *Computer Communications*, 35(2), 188-195.
7. Lu, R., Lin, X., Liang, X., & Shen, X. (2012). A dynamic privacy-preserving key management scheme for location-based services in vanets. IEEE Transactions on Intelligent Transportation Systems, 13(1), 127-139.
8. Gañán, C., Munoz, J. L., Esparza, O., Mata-Díaz, J., & Alins, J. (2015). EPA: an efficient and privacy-aware revocation mechanism for vehicular ad hoc networks. *Pervasive and Mobile Computing*, 21, 75-91.

How to cite this article:

Shanmugapriya K and Saraswathi K.2017, The Dual Authentication And Key Management Techniques For Secure Data Transmission In Vehicular Ad Hoc Network. *Int J Recent Sci Res.* 8(10), pp. 20557-20560.
DOI: http://dx.doi.org/10.24327/ijrsr.2017.0810.0915

****