A Survey on the Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks

K. Shanmugapriya
M.phil Research Scholar,
PG and Research Dept of computer science,
Government Arts College,
Coimbatore, Tamil Nadu,India.

Dr. K. Saraswathi M.C.A, M.Phil., PhD.,
Assistant Professor,
PG and Research Dept of computer science,
Government Arts College,
Coimbatore, Tamil Nadu, India.

Abstract

vehicular ad-hoc network is an infrastructure less network associated by moving vehicles. In such cases security and decision making are two essential difficulties should be tended to. To built up a dual authentication scheme to keeping the malicious vehicles entering into the system framework. To presented a dual key management method into the VANET to scatter the data from the TA side to the group of vehicle users in an intelligent and secure way. The finding of this work demonstrates that double authentication and key management plan is superior to different systems. The study is done on the vanet techniques and also compared the vanet techniques in this work.

Index Terms: Chinese remainder theorem, dual authentication, vanet, key management, vehicle secret key,

I. INTRODUCTION

Objectives to built up a double authentication scheme and key management conspire in vehicular adhoc arrange for to enhance the security Driving means changing constantly location. This means a constant demand for information on the current location and specifically for data on the surrounding traffic, routes and much more. This information can be grouped together in several categories.A very important category is driver assistance and car safety. This includes many different things mostly based on sensor data from other car

One could think of brake warning sent from preceding car, tailgate and collision warning, information about road condition and maintenance, detailed regional weather forecast, premonition of traffic jams, caution to an accident behind the next bend, detailed information about an accident for the rescue team and many other things. One could also think of local updates of the cars navigation systems or an assistant that helps to follow a friend's car.

Another category is infotainment for passengers. For example internet access, chatting and interactive games between cars close to each other. The kids will love it. Next category is local information as next free parking space (perhaps with a reservation system), detailed information about fuel prices and services offered by the next service station or just tourist information about sights.

A possible other category is car maintenance. For example online help from your car mechanic when your car breaks down or just simply service information. So far no inter-vehicle communication system for data exchange between vehicles and between roadside and vehicles has been put into operation. But there are several different research projects going on [8] [9].

In an ad hoc network, computers are brought together to form a network "on the fly." As shown in there is no fixed structure to the network, there are no fixed points and usually every node is able to communicate with every other node in its communication range. Such networks are called Mobile Ad hoc Networks (MANET). One could even think of a combination of these two modes to a hybrid network structure. Like this it would be possible to grant internet access to a large number of mobile nodes over only a few base stations. But there is no standard for such a hybrid mode yet. intervehicle communication scenario, we have to face high mobility and large networks. The best combination for this situation would be an on demand topology based routing protocol.

AODV defines no special security mechanisms. So an impersonation attack can easily be done. Or even simpler, a misbehaving node is planted in the network. There are a few proposals how to solve this problem, but it is very hard because

AODV is not a source based routing protocol and such a solution would introduce a tremendous overhead the study is done on the vanet techniques and the also compared the vanet techniques in this work.

II. Literature Survey On The Vanet Technique

In [1] outlining an effective routing protocol for VANET is tedious task. Likewise due to wireless medium it is defenseless to several attacks. Since attacks deceive the system operations, security is obligatory for fruitful organization of such innovation. They give brief review of various routing protocols. Additionally endeavor has been made to distinguish significant security issues and difficulties related with various routing protocols. Different part of VANET like its surrounding, principal and network architecture has been examined; besides different qualities of VANET have been recorded which recognized it from different systems like MANET, Cellular, and WSN. Routing is an essential part which used for more prominent and convenient communication. They additionally incorporates definite working and designing of different VANET routing protocols, at last different attacks in VANET have been grouped relying upon the accessibility, verification, secrecy, security, non denial and information trust.

In [2] introduce an anonymous batch authenticated and key agreement (ABAKA) scheme to verify various solicitations sent from various vehicles and build up various session keys for various vehicles in the meantime. Elliptic curve cryptography is to be clarified for secure correspondence. The security of ABAKA is depends on the elliptic curve discrete logarithm issue, which is an unsolved NP complete problem.

In [3] developed a symmetric scheme to increase the security and communicate with vanet system. This paper explained which hand over technique is suitable for vanet, new cryptographic approach and novel mechanism for information secrecy and user location privacy. The achievement of information obtaining and conveyance frameworks relies on upon their capacity to protect against the diverse sorts of security and privacy attacks that exist in administration situated VANETs.

In [4] developed distributed key management framework for revocation of malicious vehicles, system maintenance and implement security polices in vanets. This paper also developed secure and efficient key distribution protocol with the capability of preventing RSUs from misbehaving and an efficient cooperative message authentication protocol and explained analytical model for verifying and authentication of messages on network utilization.

In [5] built up an Efficient Certificate Management plan for Vehicular networks. It gives adaptable interoperability for certificate management in various administrative specialists, and a productive path for any On-Board Units (OBUs) to redesign its certificate anyplace whenever. Also, an efficient time-limited certificate revocation for OBUs is explained. This paper discusses the hierarchical architecture, system initialization, and certificate issuance, update, and revocation of the ECMV scheme.

In [6] investigated address the issue of large computation overhead caused by the safety message conformation. Build up a CMAP for a general two-dimensional (2-D) city road scenario technique. In this paper develop an analytical model to quantitatively evaluate the performance of our CMAP protocol as well as the PVP protocol. Missed detection ratio of invalid messages, when maliious vehicles are present is also explained.

In [7] developed a hash chain to enhance the security and protection of RFID verification. One of a developing area in RFID literature is verification protocol with hash chain demonstrate which will be profoundly examined in this paper. This article is a review to nearly watch those conventions regarding its concentration and impediments.

In [8] presented at the TESLA (Timed Efficient Stream Loss-tolerant Authentication) broadcast authentication protocol in light of free time synchronization between the sender and the recipients. TESLA requires that the beneficiaries are freely time synchronized with the sender. In this paper, a basic protocol to accomplish this time synchronization is to be assessed and one-way chains are explained.

In [9] developed a novel group signature based security system for vehicular communications which depend on alter resistance devices for anticipating adversarial attacks on the system. In this paper depicted a an adaptable part based p get control approach for vehicular system and furthermore created probabilistic signature verification scheme that can productively distinguish the altered messages or the messages from an unauthorized node.

In [10] researched three techniques for securely distributing rekey messages after a join/leave and determine protocols for joining and leaving a protected gathering. In this paper introduce the rekeying techniques and protocols in a model key server. To convey rekey messages reliably to group members, an application program that utilizations Keystone can indicate one of two alternatives for rekey message conveyance: solid unicast or IP multicast with forward blunder rectification.

In [11] created two new brought together group key management protocols in lights of the Chinese Remainder Theorem. By moving all the more processing burden onto the key server, to optimize the quantity of re-key communicate message, user-side key calculation and number of key storages. While protocols require more computation power from the key server, it doesn't have to keep up any complex various leveled structure. In this paper clarify quickly about the Chinese remainder theorem.

In [12] developed a group key distribution scheme in view of static key tree structure and the Chinese Remainder Theorem. It manages the situation of a pre-defined static planned user set containing every potential customs of multicast services and focus on the stateless recipient case. The key server utilizes the root keys of the group member sub trees and the Chinese Remainder Theorem to disseminate a group key. In this paper group key management and dispersion strategies are to be examined.

III.CONCLUSION

There are many approaches used for improving security in vanets. The dual key management plan is computationally productive that backings secure information transmission from TA to PUs and Pus to SUs in light of two diverse gathering keys, one for PUs and another for SUs for further enhancing the security among various classes of vehicles.

IV. REFERENCES

1. A. Dhamgaye and N. Chavhan, “Survey on security challenges in VANET,” *Int. J. Comput. Sci.*, vol. 2, no. 1, pp. 88–96, 2013
2. J. L. Huang, L. Y. Yeh, and H. Y. Chien, “ABAKA: An anonymous batch

authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011.

3. K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular Ad Hoc networks," *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 536–551, Feb. 2013.
4. Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel.*
5. *Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011.
6. A. Wasef, Y. Jiang, and X. Shen, "ECMV: Efficient certificate management scheme for vehicular networks," in *Proc. IEEE GLOBECOM*, New Orleans, LA, USA, 2008, pp. 1–5.
7. W. Shen, L. Liu, and X. Cao, "Cooperative message authentication in vehicular cyber-physical systems," *IEEE Trans. Emerging Topics Comput.*, vol. 1, no. 1, pp. 84–97, Jun. 2013.
8. I. Syamsuddin, T. Dillon, E. Chang, and S. Han, "A survey of RFID authentication protocols based on hash chain method," in *Proc. 3rd ICCIT*, 2008, vol. 2, pp. 559–564.
9. A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLAbroadcast authentication protocol," *RSA Crypto.*, vol. 5, no. 2, pp. 2–13, Aug. 2002.
10. J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy preserving vehicular communication framework," in *Proc. IEEE INFOCOM*, Anchorage, AK, USA, May 2007, pp. 103–108.
11. C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," *IEEE/ACM Trans. Netw.*, vol. 8, no. 1, pp. 16–30, Feb. 2000.
12. X. L. Zheng, C. T. Huang, and M.Matthews, "Chinese remainder theorem based group key management," in *Proc. 45th ACMSE*, Winston-Salem, NC, USA, 2007, pp. 266–271.