A LITERATURE SURVEY ON DUAL AUTHENTICATION AND KEY MANAGEMENT TECHNIQUES FOR SECURE DATA TRANSMISSION IN VEHICULAR AD HOC NETWORKS

Ms.B.Manimekala[1], Prof Dr.R.Ravichandran[2]
[1]Research Scholar, KG College of Arts and Science Department of Computer Science
[1]Assistant Professor, Department of Computer Science, AJK College of Arts and Science
[2]Research Guide & Director, Department of Computer Science
KG College of Arts and Science
Coimbatore, Tamil Nadu, India.

Abstract

Vehicular ad hoc networks (VANETs) are an important communication paradigm in modern-day mobile computing for exchanging live messages regarding traffic congestion, weather conditions, road conditions, and targeted location-based advertisements to improve the driving comfort. In such environments, security and intelligent decision making are two important challenges needed to be addressed. In this paper, a trusted authority (TA) is designed to provide a variety of online premium services to customers through VANETs. Therefore, it is important to maintain the confidentiality and authentication of messages exchanged between the TA and the VANET nodes. Hence, we address the security problem by focusing on the scenario where the TA classifies the users into primary, secondary, and unauthorized users. In this paper, first, we present a dual authentication scheme to provide a high level of security in the vehicle side to effectively prevent the unauthorized vehicles entering into the VANET. Second, we propose a dual group key management scheme to efficiently distribute a group key to a group of users and to update such group keys during the users' join and leave operations. The major advantage of the proposed dual key management is that adding/revoking users in the VANET group can be performed in a computationally efficient manner by updating a small amount of information. The results of the proposed dual authentication and key management scheme are computationally efficient compared with all other existing schemes discussed in literature, and the results are promising.

Keywords: Vehicular Adhoc network, Trusted Authority, Primary User, dual key

I. INTODUCTION

The life of VANET lies in the communication that takes place between different vehicles. The data being gathered and exchanged by the vehicles requires some protocols or rules through which transmission can take place in a systematic and organized way. The data exchange between nodes in a VANET happens via routing protocols. These protocols define how a packet of data will be distributed among different nodes.

VANET usually incorporate Trusted Authority (TA) that is meant to source online premium service to nodes in network. It is required to keep up the authentication and confidentiality of the messages transmitted between the TA and nodes.

A trusted authority (TA) is designed to provide a variety of online premium services to customers through VANETs. Therefore, it is important to maintain the confidentiality and authentication of messages exchanged between the TA and the VANET nodes.

Hence, we address the security problem by focusing on the scenario where the TA classifies the users into primary, secondary, and unauthorized users.

II. PROBLEM STATEMENT

- The security issues and challenges where TA classifies the VANET nodes into primary, secondary and unauthorized users
- The communication overhead increases when the density of vehicles is higher.
- The main limitation of this method is that if there is no verifier to verify messages, then the malicious messages may be consumed by vehicle users.

- All these schemes fail to propose an integrated approach to provide the authentication as well as confidentiality services in VANET.
- Take more computational time
- Vulnerable to various attacks (i.e. Sybil Attack, Collusion Attack)
- More storage consumption

III. LITERATURE SURVEYS

Shen, et al., published a paper on "Cooperative message authentication in vehicular cyber-physical systems"[6]. In this scheme, CMAP which stands for cooperative message authentication protocol is used. It is for finding out the malicious data being broadcasted in the road transport system by the unauthorized vehicles. This favorable technique called cooperative message authentication is used to reduce the computational overhead required for verification of the messages. As the number of vehicle increases in the road transport system, the communication overhead also increases. The main disadvantage of this scheme is that there is no verifier in the system to verify the messages, so the unwanted messages will be communicated between the vehicles.

Perring et al., publication is "The TESLA broadcast authentication protocol". This scheme introduced a protocol with the name timed efficient stream loss-tolerant authentication (TESLA) protocol[7]. This protocol uses symmetric keys for encrypting and decrypting the messages instead of using the asymmetric keys. Symmetric key system uses same key at both the sender and receiver side. Denial of service attacks will be prevented in this scheme as the symmetric keys are being used which are proved to be faster than the signatures. But the limitation of this scheme is that non-repudiation cannot be achieved using symmetric keys.

"A group signature based secure and privacy preserving vehicular communication framework" published by [8]J. Gua, J. P. Baugh and S. Wang . In this scheme, group signature technique is used to provide the security to the messages being communicated between the vehicles in the VANET. Here, public key of one group will be connected with the private keys of the multiple groups. In this particular group signature method, it is easy for an attacker to find out the group from which the message is sent but the sender of the message cannot be tracked.

[9]C. Wong, M. Gouda and S. Lam published a paper with the title "Secure group communications using key graphs" . A novel solution for the scalability problem is presented in this scheme of work. As the scalability to the different groups is the biggest problem seen in the network, a concept called key graph is introduced here for the groups. Secure distribution of the rekeying messages is also included in this strategy which will be conducted as a join and leave operation takes place in the system. These join and leave protocols of the rekeying process is implemented in a prototype key server built by them. The main disadvantage of this scheme is that it has high computational complexity.

X. L. Zheng, C. T. Huang, and M. Matthews published a paper on "Chinese remainder theorem based group key management"[10]. In this scheme, a two centralized group key management protocols is proposed based on the Chinese remainder theorem (CRT). Here the number of the messages broadcasted for distributing the group keys to the vehicle users is minimized. Key computation time is reduced. Key computation overhead of the vehicle users is also minimized. The main drawback of this system is it introduces high computational complexity on the server during key generation process.

They are conducted on VANETs which worked on the schemes that provide authentication only. One of the approach used in existing system Anonymous Batch authentication which provides value-Added Services to VANET's .This scheme was introduced to verify miscellaneous requests which are forwarded from distinct vehicles. It authenticates multiple requests efficiently by a single authentication operation. The main issue with this system was scalability problem. Another approach was to provide secure group communication using key graphs Here key graphs are introduced to specify secure groups. Three strategies are defined for distributing rekey messages securely after a join/leave. [17]The Group key management service is scalable to large groups with frequent joins and leave operations. The major drawback with this system is the usage of user-oriented rekeying on the sever side and group oriented rekeying on the client side which effects the performance. Next approach is a Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework. It achieves authenticity, data integrity, anonymity, and accountability at the same time. It provides authenticity and

ensures secrecy of the data. Here Vehicles use their own identity. A Scalable Robust Authentication protocol for Secure Vehicular Communications[19] is another technique proposed by Sun et.al., publishers. In this system each RSU maintains and manages an on-the-fly group within its communication range. Here vehicles broadcast V to V messages, which are verified instantly by the vehicles in the same group. It uses an ID-based cryptography which actually increases storage space. [6]Co-operative Message Authentication (CMAP) is another approach which identifies malicious information that is being broadcasted by a malicious user. The main disadvantage of this system is that if no verifier is present then the malicious information can be broadcasted to legitimate users also. Yet another approach Certificate Management Scheme for Vehicular Networks which offers a flexible way of certificate management as well as provides a way for OBU's to update the certificate anywhere at any time. This system can reduce the complexity of certificate management and can achieve excellent security. Major drawback of this system is long delay incurred in checking the revocation status of a certificate.

Yong Hao proposed [5]A Distributed Key Management Framework With Co-operative Message Authentication in VANET which is to tackle the large computation overhead due to the group signature implementation. A cooperative message authentication protocol [9] is proposed to alleviate the verification burden. Malicious vehicle cannot enter into VANET and privacy is preserved. Security attacks are possible. A. Dhamgaye and N. Chavhan proposed a scheme which routes the data efficiently from source to destination[2]. Many protocols such as Proactive and Reactive routing Protocols, Source routing or hop by hop routing is used. It selects the best path with least time and least expensive route. The best route from source to destination is found. Different types of attack on routing protocols in VANET. Irfan Syamsuddina, Tharam Dillonb, Elizabeth Changc, and Song Hand which is used to tackle the security and the privacy problems in RFID communications. There are several protocols have been proposed to overcome those problems. Hash chain is commonly employed by the protocols to improve security and privacy for RFID authentication. Although the protocols able to provide specific solution for RFID security and privacy problems, they fail to provide integrated solution.

WENLONG SHEN, LU LIU, XIANGHUI CAO (Member, IEEE), YONG HAO AND YU CHENG (Senior Member, IEEE) proposed a scheme which is used to tackle large computation overhead caused by the safety message authentication. A cooperative message authentication protocol (CMAP) is developed to alleviate vehicles' computation burden. All the vehicles share their verification results with each other in a cooperative way, so that the number of safety messages that each vehicle needs to verify reduces significantly. Security is the major issue. Huang, misra,verma,xue proposed a scheme which is used to solve the generation of pseudonyms for anonymous communication. We have proposed a novel PACP (Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs) protocol for the vehicles in VANETs for such that the pseudonyms are only known to the vehicles but have no other entities in the network. Confidential privacy is provided to the vehicles. It is suitable only for

small scale VANET test bed.

Jiun-Long Huang proposed an ABAKA (An Anonymous Batch Authenticated and Key Agreement Scheme) which is to tackle the problems, including security, efficiency, and scalability problem. ABAKA scheme is to build a secure environment for value-added services in VANETs[3]. The concept of batch verification to authenticate multiple requests sent from different vehicles using elliptic curve cryptography (ECC). ABAKA scheme to authenticate multiple requests sent from different vehicles and establish different ensure the confidentiality session keys. ABAKA is a suitable scheme for value-added services in VANETs. Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri propsed a Short-lived Key Management scheme which is used to tackle the problems such as connectivity is limited and communication with a central certification authority might be problematic[15]. The group-keys are derived from a couple of independent hash chains for generating onetime passwords.MD-5, SHA-1.Symmetric cryptographic algorithm to offer group-level confidentiality and group level integrity services. No per-user authentication and non-repudiation is provided.

IV.METHODS AND MATERIAL

A.PREVIOUS WORK

- Centralized Time Division Multiple Access (TDMA) based scheduling protocol based on a new weight-factor-

based scheduler in a Vehicular network. A Roadside Unit (RSU), is a centralized controller, which collects the state information of a channel and also the individual information of the communication links within its communication coverage. It then calculates their respective scheduling weight factors followed by scheduling decisions, which are made by the RSU. The Scheduling weight factor has three parts, namely the channel quality factor, the speed factor, and the access category factor. In this system, a resource-reusing mode can be permitted among multiple vehicle-to-vehicle (V2V) links, provided the distances between the two vehicles of these V2V links are greater than a predefined interference interval. The centralized TDMA-based scheduling protocol in this system can improve the network throughput when it is compared with the existing system, medium-access-control protocols in vehicular networks, and can be easily incorporated into practical vehicular networks.

- The RFID authentication protocols which provides privacy and anonymity. Hash chain method is used in these RFID authentication protocols in various ways and it provides a unique solution for security and also for privacy problems of RFID technology. As a result, while problems in particular cases can be addressed, other problems tend to occur. Thus, the proposed system can be concluded that recent RFID authentication protocols with hash chain failed to satisfy an integrated security and privacy solutions for RFID.
- Many existing techniques are available in the literature for providing authentication in the VANET. Among the various existing techniques, Johnson *et al.* proposed an Elliptic Curve Digital Signature Algorithm (ECDSA), which is mathematically derived from the basic digital signature algorithm.
- ECDSA uses an asymmetric key pair which consists of a public key and a private key. The public key used in this technique is a random multiple of the base point, where the multiples are generated from the private key. Here, both the public and the private keys are used for user authentication.

B.PROPOSED WORK

We proposed a new dual authentication scheme for improving the security of vehicles that are communicating with the VANET environment. For providing such authentication in dual mode, we used two components such as hash code and fingerprint, finger knuckle of each communicating vehicle user. Therefore, the fingerprint authentication technique is integrated into a hash code creation method in this paper to avoid malicious users to use the secret key of any VANET users in order to participate in the VANET communication. Moreover, to avoid malicious users from spoofing the authentication code issued for any VANET users and sending erroneous messages to other

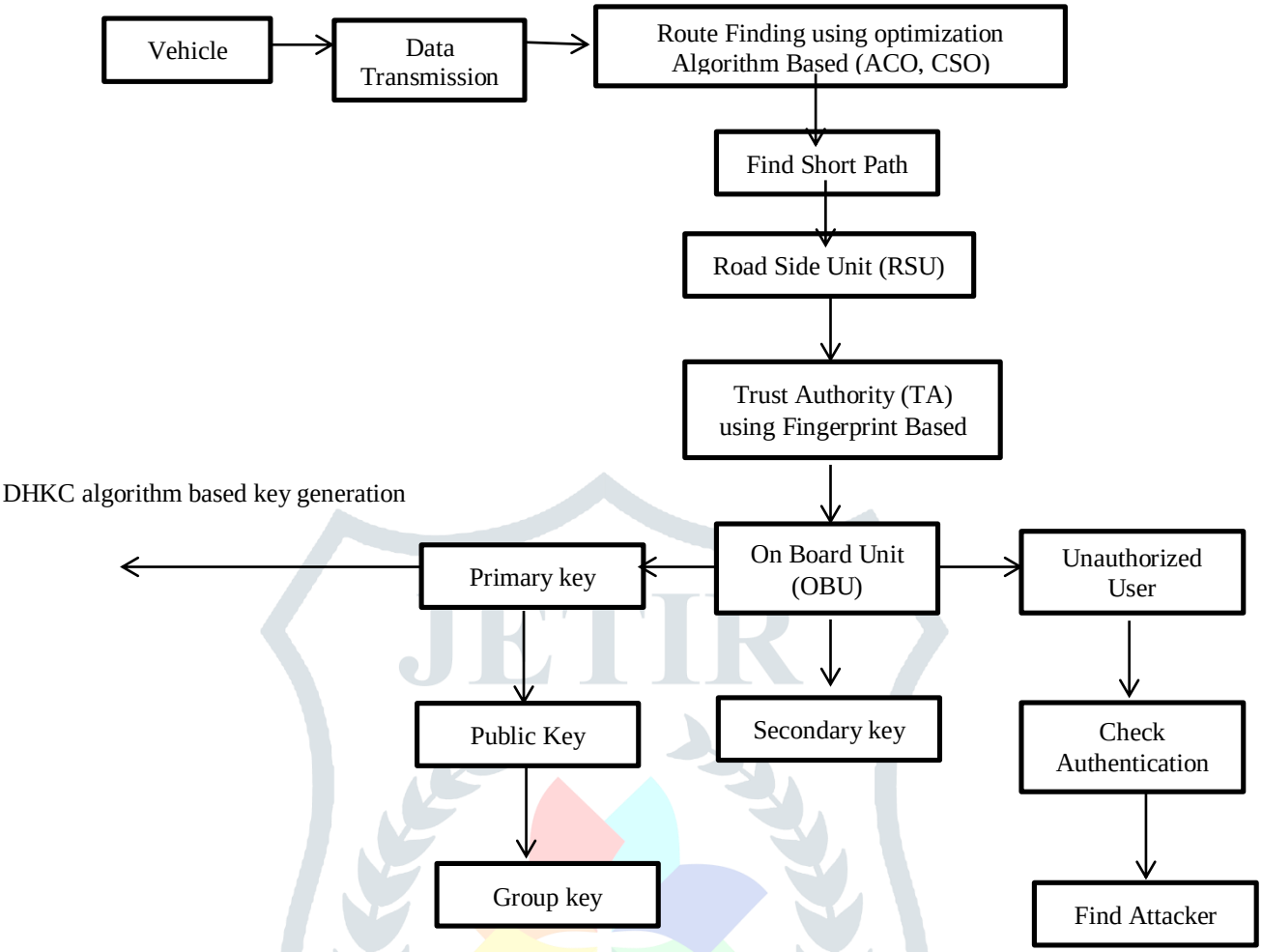

Fig 1. Proposed Work Flow

vehicles we have introduced a new dual key management scheme in this research work.

The main objective of developing a dual authentication scheme is to improve the security in the vehicle side. The dual authentication scheme depends on the Vehicle Secret Key (VSK) which is given to the user at the time of registration by the Trusted Authority

C.ADVANTAGES OF PROPOSED SYSTEM

The proposed dual group key management scheme minimizes the computational cost of the TA and group

members in the rekeying operation. To achieve this goal, the TA performs only simple addition and subtraction operations to update the group key. Similarly, each vehicle user of the multicast group performs only one modulo division operation for recovering the updated key when the group membership changes.

- We propose a secure dual authentication technique with the capability of preventing malicious vehicles entering into the VANET system.
- We introduce a dual key management technique into the VANET to disseminate the information from the TA side to the group of vehicle users in an intelligent and secure way.
- We get the computational complexity of our proposed dual key management scheme as *O* (1) in both the TA and vehicle users and hence it is suitable for VANETs.
- The communication complexity of our proposed dual key management scheme is also *O* (1) which means that our scheme takes only one broadcast to inform the updated keying information from the TA to vehicle group.
- Even if the VSK value of any user is lost, the intruder cannot use that VSK for getting service from the TA. To prevent the intruder to use other users VSK, we have included fingerprint of each authenticated user in the smart card issued by the TA.

- Moreover, the proposed dual authentication technique is a computationally efficient authentication technique.
- The computation complexity of the TA and VANET user is reduced substantially by minimizing the number of arithmetic operations taken by the TA and VANET user.
- Decrease computation time
- Provide data security
- Decrease storage consumption

V.CONCLUSION

In this paper, we proposed a dual authentication scheme to authenticate both the OBU and authority for an authorized the users entering into the network. We manage key techniques for secure data transmission smart card device in vehicular ad hoc networks. The dual group key management scheme to efficiently distribute a group key to a group of users and to update such group keys during the users join and leave operations. The primary user will directly link with the authority and secondary users receive the information from the primary user. It also has been verified by the primary user by the group key. The future development of this project provides a numbers for authentication but in future strings will be used for authentication purpose and transmit text messages to the users, in future system will transmit images and videos too to the users.

REFERENCES

[1]. X. Sun, et al., "Secure vehicular communications based on group signature and ID-based signature scheme," in Proc. IEEEICC, 2007, pp. 1539–1545.

[2]. A. Dhamgaye and N. Chavhan, "Survey on security challenges inVANET," Int. J. Comput. Sci., vol. 2, no. 1, pp. 88–96, 2013.

[3]. 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.

[4]. 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.

[5]. Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. P. Vijayakumar, S. Bose, and A. Kannan, "Centralized key distribution protocol using the greatest common divisor method," Comput. Math.Appl., vol. 65, no. 9, pp. 1360–1368, May 2013.

[12]. N. V. Vighnesh, N. Kavita, R. Shalini, and S. Sampalli,"Anovel sender authentication scheme based on hash chain for vehicular ad-hoc networks,"in Proc. IEEE Symp. ISWTA, Langkawi, Malaysia, 2011, pp. 96–101.

[13]. P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communicationsassumptions, requirements, and principles," in Proc. 4th Workshop ESCAR, Lausanne, Switzerland, 2006, pp. 5–14.

[14]. C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks,"in Proc. IEEE ICC, Beijing, China, May 19–23, 2008, pp. 1451–1457.

[15]. L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari, "A novel batch based group key management protocol applied to the Internet of things," Ad Hoc Netw., vol. 11, no. 8, pp. 2724– 2737, Nov. 2013.

[16]. S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived key management for secure communications in VANETs," in Proc. IEEE Int. Conf. ITST, St. Petersburg, Russia, 2011, pp. 613–618.

[17]. X. Lv, H. Li, and B. Wang, "Group key agreement for secure group communication in dynamic peer systems," J. Parallel Distrib. Comput.,vol. 72, no. 10, pp. 1195–1200, Oct. 2012.

[18]. P. Vijayakumar, S. Bose, and A. Kannan, "Chinese remainder theorem based centralized group key management for secure multicast communication,"IET Inf. Security, vol. 8, no. 3, pp. 179–187, May 2014.

[19]. X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and id-based signature scheme," in Proc. IEEE ICC,Jun. 2007, pp. 1539–1545.

[20]. K. Matusiewicz, J. Pieprzyk, N.Pramstaller, C. Rechberger, and V. Rijmen, "Analysis of simplified variants of SHA-256," in Proc. WEWoRC, Louvain, Belgium, Jul. 2005, pp. 112.