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

Dr. C. Kalaiselvi* & G. Aruna Senbagam**

*Associate Professor and Head, Department of Computer Applications, Tiruppur Kumaran College for Women, Tirupur, Tamilnadu, INDIA.
**Research Scholar (M.Phil), Department of Computer Applications, Tiruppur Kumaran College for Women, Tirupur, Tamilnadu, INDIA.
E-Mail: arunagopal2208{at}gmail{dot}com

***Abstract*—**VANET is a self-organizing communication network that is created among the moving vehicles. VANET have recently become popular for research, with attention to advance the driving experience and road protection. 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. Hence the address security issues and challenges where TA classifies the VANET nodes into primary, secondary and unauthorized users. So therefore, in this project have proposed a dual authentication scheme to produce advanced security level to effectively that stops the unauthorized vehicle entering into VANET environment using smart card. Second, we tend to propose a Batch Level Signature (BLS) group key management theme with efficiency distributing a group key to different VANET nodes. From this project, must send the messages or some safety information from the Trusted authority to the primary user and then primary user to the secondary user with full of secured process..

***Keywords*—**Authentication; Chinese Remainder Theorem; Group Key Management; Vehicle Street Key; VANET.

***Abbreviations*—**Anonymous Batch Authenticated and Key Agreement Scheme (ABAKA); Batch Level Signature (BLS); Trusted Authority (TA); Vehicular Ad Hoc Networks (VANET).

I. INTRODUCTION

WITH the increasing number of vehicles on the streets, an increasing population of vehicle manufacturers are looking for value-added services for providing their customers with increased safety and information. Toward this goal, Vehicular Communication (VC) is likely to play a major role. VC involves the use of short-range radios in each vehicle, which would allow various vehicles to communicate with each other and with road-side infrastructure. These vehicles would then form an instantiation of ad hoc networks in vehicles, popularly known as Vehicular Ad Hoc Networks (VANET). VANET are envisioned to provide safety-related information, traffic management, and infotainment services. These are the major areas in which applications are likely to develop and find commercial deployment. The first two, that is, safety and traffic management, require real-time information, and this conveyed information can affect life or death decisions. Without security, a VANET system is vulnerable to a number of attacks such as propagation of false warning messages and suppression of actual warning messages, thereby causing accidents [Wischhof et al., 1]. This makes security a factor of paramount importance in building such networks. However, many forms of attacks against VANET have emerged recently and alarmed the unsettling situation of these networks security. Being an implementation of Mobile Ad hoc network (MANET). Those properties include the particular nature of communication in VANET. Connections in a VANET in particular and in any Wireless Ad hoc Network in general are based on node-to-node communications: every node is able to act as either a host inquiring data or a router forwarding data. There are two types of nodes: (i) Road Side Units (RSUs) standing for fixed nodes provisioned along the route and (ii) On Board Unit (OBU) referring to mobile nodes (i.e., vehicles) equipped with some sort of radio interface that enables connecting to other nodes in wireless manner. It is worth mentioning that the speed of mobile nodes- vehicles in VANET may be much higher than in MANET. This reason makes VANET are very

dynamic in nature. A number of nodes can communicate once as a group but can then rapidly change their own structure caused by leaving of a member or joining of another node. Therefore, it is expected that nodes are continuously "keeping in touch" with other nodes in the group to maintain the survival of the network.

II. LITERATURE REVIEW

2.1. Survey on Security Challenges in VANET

Recent advances in development of Wireless Communication in Vehicular Adhoc Network (VANET) has provided emerging platform for industrialists and researchers. Vehicular Adhoc networks are multihop networks with no fixed infrastructure. It comprises of moving vehicles communicating with each other. One of the main challenge in VANET is to route the data efficiently from source to destination. Designing an efficient routing protocol for VANET is tiresome task [Lalitha & Kalaiselvi, 13]. Also because of wireless medium it is vulnerable to several attacks. Since attacks mislead the network operations, security is mandatory for successful deployment of such technology. This survey paper gives brief overview of different routing protocols. Also attempt has been made to identify major security issues and challenges associated with different routing protocols. Hence, the network topology change frequently, and the routing protocol used has to adapt itself to these instantaneous changes continuously [Dhamgaye & Chavhan, 2].

2.2. An Anonymous Batch Authenticated and Key Agreement Scheme (ABAKA)

In this paper, we introduce an anonymous batch authenticated and key agreement (ABAKA) scheme to authenticate multiple requests sent from different vehicles and establish different session keys for different vehicles at the same time. In vehicular ad hoc networks (VANET), the speed of a vehicle is changed from 10 to 40 m/s (36–144 km/h); therefore, the need for efficient authentication is inevitable. Compared with the current key agreement scheme, ABAKA can efficiently authenticate multiple requests by one verification operation and negotiate a session key with each vehicle by one broadcast message. Elliptic curve cryptography is implemented to reduce the verification delay and transmission overhead.

ABAKA enjoys the following unparalleled features: 1) Multiple vehicles can be authenticated at the same time rather than one after the other. It is an appealing solution to elaborately solve the possible bottleneck problems. 2) Not only can batch authentication be achieved but batch key agreement can also be accomplished. Depending on different key agreement parameters sent from the requesting vehicles, ABAKA could negotiate a distinct session key with each vehicle to ensure the confidentiality of subsequent messages. 3) By creating distinct pseudo identities and the corresponding private keys, the privacy regarding the real identity of a vehicle and private information is guaranteed. 4) The real identities of the vehicles can be uniquely revealed by the service provider (SP) under specific conditions. 5) Due to the advantage of tamperproof devices in vehicles, the efforts on the storage cost and the transmission overhead can be significantly alleviated [Huang et al., 3].

2.3. Efficient Data Acquisition Mechanism In Vehicular Adhoc Networks

Recent advances in wireless inter-vehicle communication systems enable the establishment of Vehicular Ad-hoc Networks (VANET) and create significant opportunities for the deployment of a wide variety of applications and services to vehicles. VANETs enable vehicles to communicate with each other and with road side units (RSU). The deployment of vehicular communication systems is strongly dependent on their security and privacy features. Security and privacy are major research concerns in VANETs due to the frequent vehicles movement, time critical response and hybrid architecture of VANETs that make them different than other Ad hoc networks [Karthikambal & Kalaiselvi, 14]. In order to meet presentation goals, it is widely agreed that vehicular ad hoc networks must rely heavily on node-to-node communication, thus allowing for malicious data traffic [Lalitha & Kalaiselvi, 15]. At the same time, the easy access to information afforded by VANETs potentially enables the difficult security goal of data validation. Here a collection of novel security and privacy mechanism is proposed using the HARDY function, i.e. hierarchical-based encryption function, and thus evaluating and improving the performance.

Some of the more common attacks against privacy are:

- Monitoring and Eavesdropping: This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents.
- Traffic Analysis: Even when the messages transferred are encrypted, it still leaves a high opportunity analysis of the communication outlines. This can potentially reveal enough information to enable an adversary to cause malicious harm to the network [Mershad & Artail, 4].

2.4. Secure Vehicular Ad Hoc Networks

Significant increasing in the number of vehicle accidents around the world and the resulting losses in both aspects human and material necessitate us to find efficient, innovative solutions to this passive phenomenon. Vehicular Ad hoc NETwork (VANET) is an emerging technology that attracts many research interests in the field of wireless communications due to its benefits in providing more road safety and enhancing traffic management. Security is one of the most critical issues that face VANETs. VANETs are vulnerable to different types of attacks as long as they are still a fertile network with their malicious attacks. This paper presents an introduction to VANETs and its structure and provides an overview of fundamental security challenges and requirements in VANETs. It also discusses and investigates

major security attacks and its effects on the security requirements. Afterwards, it studies, compares and finally classifies a variety of possible countermeasures that have been proposed to cope with these attacks. The safety applications attempt to improve road safety and avoid accidents as possible, examples of these applications are collision avoidance, traffic management, traffic signal violation warning, emergency vehicles warning, curve speed warning, post accident warning, work zone warning, and road condition warning applications. The prime purpose of safety application is to minimize road accidents as well as save humans' lives. As for non-safety applications, whose purpose is to enhance the road experience and make it more comfort and enjoyable for passengers, they will be used as infotainment applications, for examples, music and video sharing, games, internet services, emails, weather, payment services, nearest restaurants, hotels, petrol stations, parking applications, etc [Raya & Hubaux, 5].

2.5. Key Management Framework with Cooperative Message Authentication

In this paper, we propose a distributed key management framework based on group signature to providing privacy in vehicular ad hoc networks (VANET). Distributed key management is expected to facilitate the revocation of malicious vehicles, maintenance of the system, and heterogeneous security policies, compared with the centralized key management assumed by the existing group signature schemes. In our framework, each road side unit (RSU) acts as the key distributor for the group, where a new issue incurred is that the semi-trust RSUs may be compromised. Thus, we develop security protocols for the scheme which are able to detect compromised RSUs and their colluding malicious vehicles. Moreover, we address the issue of large computation overhead due to the group signature execution. To propose a more efficient and practical cooperative message authentication protocol (CMAP) with an assumption that each safety message carries the location information of the sender vehicle (which can be generated by a global positioning system (GPS) device). Verifiers of each message are defined according to their locations in relation to the sender. Only the selected verifiers check the validity of the message while other vehicles rely on verification results from these verifiers. Compared with our protocol has smaller packet loss ratio, less computation and communication overhead, as well as better security performance [Hao et al., 6].

2.6. Elliptic Curve Digital Signature Algorithm (ECDSA)

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). It was accepted in 1999 as an ANSI standard, and it was accepted in 2000 as IEEE and NIST standards. It was also accepted in 1998 as an ISO standard, and is under consideration for inclusion in some other ISO standards. The normal discrete logarithm problem and the integer factorization problem, no sub exponential-time algorithm is known for the elliptic curve discrete logarithm problem. For this reason, the strength-per-key-bit is substantially greater in an algorithm that uses elliptic curves. In this paper defines the ANSI X9.62 ECDSA, and converses related security, implementation, and interoperability issues.

The advantages that can be gained from smaller parameters include speed (faster computations) and smaller keys and certificates. These advantages are especially important in environments where processing power, storage space, bandwidth, or power consumption is constrained. This paper is concerned with asymmetric digital signatures schemes with appendix. "Asymmetric" means that each entity selects a key pair consisting of a private key and a related public key. The entity maintains the secrecy of the private key which it uses for signing messages, and makes authentic copies of its public key available to other entities which use it to verify signatures. "Appendix" means that a cryptographic hash function is used to create a message digest of the message, and the signing transformation is applied to the message digest rather than to the message itself [Johnson et al., 7].

2.7. Cooperative Message Authentication Protocol

The vehicular ad hoc network presents a very complex cyber-physical system with involved interaction between the physical and cyber domains. In the physical domain, vehicles need to frequently broad cast their geographic information. The safety message broadcasting in an area with a high density of vehicles tends to acquire a large data traffic rate that should be properly processed in the cyber domain. In this paper, we address the issue of large computation overhead caused by the safety message authentication. Furthermore, we study the verifier selection algorithms for a high detection rate of invalid messages in a practical 2-D road scenario. Another important impact in this paper is that we develop an analytical model for CMAP and the existing probabilistic verification protocol, considering the hidden terminal impact. Simulation results over a practical map are presented to demonstrate the performance of the proposed CMAP with comparison to the existing method. The VANET presents a very complex cyber-physical system (CPS) with intricate interplay between the physical domain and the cyber domain. On one side, the complicated physical domain of VANET incurs many challenging issues to the cyber domain. Only the selected verifiers check the validity of the message, while those non-verifier vehicles rely on verification results from those verifiers. A brand new research issue with CMAP is how to select verifiers in the city road scenario [Shen et al., 8].

2.8. RFID Authentication Protocols based on Hash-Chain Method

Security and privacy are the inherent 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. This article is a survey to closely observe those protocols in terms of its focus and limitations. Generally, RFID systems consist of Radio Frequency Identification (RFID) tags and RFID readers. Automatic identification is the basic characteristic of RFID. In its simplest form, identification can be binary, e.g., paid or nor paid which is useful for alerting. Therefore, alerting is become the next powerful feature of RFID. Also, RFID enable real time monitoring to a large number of in a short time. In addition, RFID has ability to perform on-chip computation, accordingly it support cryptographic protocol for authentication. In general, RFID has four basic capabilities, identification, alerting, monitoring, and authentication [Syamsuddin et al., 9].

2.9. The TESLA Broadcast Authentication Protocol

One of the main challenges of securing broadcast communication is source authentication, or enabling receivers of broadcast data to verify that the received data really originates from the claimed source and was not modified en route. This problem is complicated by mutually untrusted receivers and unreliable communication environments where the sender does not retransmit lost packets.

This TESLA (Timed Efficient Stream Loss-tolerant Authentication) broadcast authentication protocol, an efficient protocol with low communication and computation overhead, which scales to large numbers of receivers, and tolerates packet loss. Simply deploying the standard point-to-point authentication mechanism does not provide secure broadcast authentication. The problem is that any receiver with the secret key can forge data and impersonate the sender. Consequently, it is natural to look for solutions based on asymmetric cryptography to prevent this attack; a digital signature scheme is an example of an asymmetric cryptographic protocol [Wong et al., 10].

2.10. Secure Group Communications using Key Graphs

Many emerging network applications are based upon a group communications model. As a result, securing group communications, i.e., providing confidentiality, authenticity, and integrity of messages delivered between group members, will become a critical networking issue. We present, in this paper, a novel solution to the scalability problem of group/multicast key management. We formalize the notion of a secure group as a triple (U,K,R) where U denotes a set of users, K a set of keys held by the users, and a R user-key relation. We then introduce key graphs to specify secure groups. For a special class of key graphs, we present three strategies for securely distributing rekey messages after a join/leave and specify protocols for joining and leaving a secure group. The rekeying strategies and join/leave protocols are implemented in a prototype key server we have built. We present measurement results from experiments and discuss performance comparisons. We show that our group key management service, using any of the three rekeying strategies, is scalable to large groups with frequent joins and leaves. In particular, the average measured processing time per join/leave increases linearly with the logarithm of group size.

For a more concrete illustration of this point, we outline a typical procedure for securing unicast communications between a client and a server. Initially, the client and server mutually authenticate each other using an authentication protocol or service; subsequently, a symmetric key is created and shared by them to be used for pairwise confidential communications. This procedure can be extended to a group as follows. Let there be a trusted server which is given membership information to exercise group access control. When a client wants to join the group, the client and server mutually authenticate using an authentication protocol. Having been authenticated and accepted into the group, each member shares with the server a key, to be called the member's individual key. For group communications, the server distributes to each member a group key to be shared by all members of the group [Zheng et al., 11].

2.11. Chinese Remainder Theorem based Group Key Management

In this paper, we present two new centralized group key management protocols based on the Chinese Remainder Theorem (CRT). By shifting more computing load onto the key server we optimize the number of re-key broadcast messages, user-side key computation, and number of key storages. The first protocol is the base Chinese Remaindering Group Key (CRGK) protocol, which with a group of n users requires the key server to do O(n) XORs, additions, multiplications, and Extended Euclidean Algorithm computations and broadcast 1 re-key message; each individual user is required to do only 1 modulo arithmetic and 1 XOR operation for each group key update. The second protocol is the Fast Chinese Remaindering Group Key (FCRGK) protocol, which only requires the key server to do O(n) XORs, additions, and multiplications most of the times with no change to the number of re-key messages and user computation per group key update. For both protocols each user only needs to store 2 keys all the time. While our protocols require more computation power from the key server, it does not need to maintain any complex hierarchical structure. With the tremendous advantage on re-key broadcasting message number, user key computation, user key storage, and the relatively simple nature compared to other protocols, we consider our protocols are well worth exploring. While this paper deals with group key management for dynamic group, our protocols are based on the assumption that certain authentication protocol involving two parties is needed before the key server grants group access to each user [Zhou & Ou, 12].

III. CONCLUSION

The potential of VANET applications is immense, considering the large amount of vehicles on the road. However, most of the VANET applications such as safety

messages and hazard warning have stringent time requirements and malfunctioning systems and malicious attackers can cause loss of life and injury due to accidents. It is, therefore, imperative to develop a strong security system for VANET. VANET technology has the ability to transform the way vehicles travel from one place to another and offer a whole gamut of services from safety messaging to infotainment It has been observed that the classification helps to deal with different types of attack on routing protocols in VANET [Aruna Senbagam & Kalaiselvi, 16; 17]. Security is the major issue to implement the VANET. Among all requirements authentication and privacy are the major issues in VANET. However confidentiality is not required in the VANET because generally packets on the network do not contain any confidential data.

REFERENCES

[1] L. Wischhof, A. Ebner & H. Rohling (2005), "Information Dissemination in Self-Organizing Intervehicle Networks", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 6, No. 1, Pp. 90–101.

[2] A. Dhamgaye & N. Chavhan (2013), "Survey on Security Challenges in VANET", *International Journal of Computer Science and Network*, Vol. 2, No. 1, Pp. 88–96.

[3] J.L. Huang, L.Y. Yeh & H.Y. Chien (2011), "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, Vol. 60, No. 1, Pp. 248–262.

[4] K. Mershad & H. Artail (2013), "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", *IEEE Transactions on Vehicular Technology*, Vol. 62, No. 2, Pp. 536–551.

[5] M. Raya & J. Hubaux (2007), "Securing Vehicular Ad Hoc Networks", *Journal of Computer Security*, Vol. 15, No. 1, Pp. 39–68.

[6] Y. Hao, Y. Cheng, C. Zhou & W. Song (2011), "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs", *IEEE Journal on Selected Areas in Communications*, Vol. 29, No. 3, Pp. 616–629.

[7] D. Johnson, A. Menezes & S. Vanstone (2001), "The Elliptic Curve Digital Signature Algorithm (ECDSA)", *International Journal of Information Security*, Vol. 1, No. 1, Pp. 36–63.

[8] W. Shen, L. Liu & X. Cao (2013), "Cooperative Message Authentication in Vehicular Cyber-Physical Systems", *IEEE Transactions on Emerging Topics in Computing*, Vol. 1, No. 1, Pp. 84–97.

[9] I. Syamsuddin, T. Dillon, E. Chang & S. Han (2008), "A Survey of RFID Authentication Protocols based on Hash Chain Method", *Proceedings of 3rd ICCIT*, Vol. 2, Pp. 559–564.

[10] C. Wong, M. Gouda & S. Lam (2000), "Secure Group Communications using Key Graphs", *IEEE/ACM Transactions on Networking*, Vol. 8, No. 1, Pp. 16–30.

[11] X.L. Zheng, C.T. Huang & M. Matthews (2007), "Chinese Remainder Theorem based Group Key Management", *Proceedings of 45th ACMSE*, Winston-Salem, NC, USA, Pp. 266–271.

[12] J. Zhou & Y.H. Ou (2009), "Key Tree and Chinese Remainder Theorem based Group Key Distribution Scheme", *Journal of the Chinese Institute of Engineers*, Vol. 32, No. 7, Pp. 967–974.

[13] J. Lalitha & C. Kalaiselvi (2016), "Energy Efficient and Congestion Control in Wireless Sensor Network using Firefly Algorithm", Vol. 23, No. 5.

[14] P. Karthikambal & C. Kalaiselvi (2016), "Growing Protocols and Architectural Design of Wireless Sensor Network", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 4, No. 10.

[15] J. Lalitha & C. Kalaiselvi (2016), "A Novel Stressing Protocol and Defense Approaches in Wireless Sensor Networks", ISO Vol. 5, No. 11.

[16] G. Aruna Senbagam & C. Kalaiselvi (2017), "An Overview of Statistical Pattern Recognition – A Review", *Journal of Environmental Nanotechnology*, Vol. 6, No.1, Pp. 75–78.

[17] G. Aruna Senbagam & C. Kalaiselvi (2017), "Efficient Group Key Management Protocol for DDOS Attack," *International Journal of Contemporary Research in Computer Science and Technology*, Vol. 3, Special Issue. 3.

