International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

Proxy Based Authentication Scheme Using Distributed Computing in Vehicular Ad Hoc Networks

CH. SHIREESHA[1] , P PROMAD KUMAR[2]
[1]M.Tech Student, CSE, SR Engineering College, Warangal,Telangana,India.
[2] Assistant prof, CSE, SR Engineering College, Warangal,Telangana,India.

Abstract - ***generally, authentication in vehicular ad-hoc net-works (VANETs) used Public Key Infrastructure to check the Message integrity and the of message senders. The problems considered in the authentication schemes are the level of security and computational efficiency in verification processes. Most of existing schemes focus mainly on the security and privacy of VANET information. However, these schemes may not work well in VANET scenarios. For instance, it is difficult for a Roadside to verify each vehicle's signature sequentially when a large number of vehicles emerge in the coverage areas of an Road Side. To reduce the computational overhead of Road Side, we propose a Proxy Based Authentication Scheme using distributed computing. In this scheme proxy vehicles are used to authenticate multiple messages with the help of verification function at the same time. In addition to that Road Side Vehicle is able to independently verify the outputs from the verification function of the proxy vehicles. We also design an explicitly key negotiation scheme for transmitting sensitive messages. It is shown from the analysis and simulations with the help of the proxy vehicles. It is better compared to existing batch-based authentication schemes.***

KEY Terms—Public Key Infrastructure, Proxy based authentication Scheme,Vehicular ad-hoc network

I. INTRODUCTION

VANETs have attracted a lot of attention due to its potential to offer better driving experience and road safety, as well as many other value-added services [1] [2]. Security issue [3] [4] is critical in VANETs because many different forms of attacks [3] against VANETs may emerge due to the use of wireless devices in VANET communications. Such security attacks may lead to bad user experience (thus causing the loss of revenue for those value-added service providers) or create even more Catastrophic consequences such as the loss of lives due to the traffic accidents due to the failure of VANET communications.

Some sophisticated security schemes have been proposed in the literature as an effort to ensure that all information exchanged in VANETs is authenticated and thus can be fully trusted. In particular, Raya et al. presented a Public-Key Infrastructure based scheme for vehicular signature applications [1], where an RSU verifies received messages one after another. Because vehicles normally forward messages on the fly at any time, it may not be able to be predicted and known by RSU. Also, those PKI-based schemes [1] [5] [6] are time-consuming processes and may fail to satisfy the computational efficiency requirement under dynamic traffic patterns, where the computational complexity and transmis-sion overhead of RSUs increase linearly with the number of vehicles that need to be authenticated.

Zhang et al. in their work published in [7] introduced an efficient batch signature verification scheme for the communi-cations between vehicles and RSUs, in which an RSU can verify multiple received signatures at the same time, such that the total verification time required can be significantly reduced. In their proposed scheme, an RSU can simultaneously verify approximately 1600 messages per second, which is not bad but still not fast enough to meet the requirement of VANET authentication speed. According to the Dedicated Short Range Communications (DSRC) protocol [8] [9], each vehicle broadcasts a traffic safety message every 100-300 ms. This implies that an RSU must verify around 2500←5000 messages per second when there are 500 vehicles within the coverage of an RSU, which is indeed a great challenge for any current batch-based digital signature scheme reported in the literature [10] [11] [12] [13]. In this paper, our goal is to tackle the aforementioned efficiency problem of the existing authentication schemes.

II EXISTING SYSTEM

On the other hand, batch verification offers an efficient way for verifying signatures in VANETs. Zhang et al. in [7] in-troduced an Identity-based Batch signature Verification (IBV) scheme for vehicular-to-infrastructure (V2I) communications, which works based on identity-based encryption algorithms [17] [18] proposed by Boneh et al. In the IBV scheme, an RSU can also verify multiple received signatures at the same time such that the computation time can be significantly reduced. Meanwhile, the certificates are not needed in the verification processes, and thus the transmission overhead can be reduced substantially. The IBV scheme can achieve conditional privacy preservation using pseudo identities, and a Trust Authority (TA) is capable of tracing a vehicle's real identity from its pseudo identity. In [19], Zhang et al. made their effort to enhance the IBV scheme via adopting a group testing technique. The objective of the group testing is to find invalid signatures with a minimal batch verification workload. In [10], Huang et al. proposed an Anonymous Batch Authenticated and Key Agreement (ABAKA) scheme for different value-added services, which can authenticate multiple messages sent from different vehicles and establish different session keys for different vehicles at the same time. The security of the ABAKA scheme is ensured based also on ECDSA. Compared with the basic ECDSA scheme, relatively short signatures are adopted by the ABAKA scheme to reduce the computation and transmission overheads of RSUs. In [20], Chim et al. introduced a Secure and Privacy Enhancing Communications Scheme (SPECS), where any vehicle can form a group with the other vehicles after batch authenticating and can communicate with one another securely without RSUs. However, in [11], Shi-Jinn Horng et al. found out that SPECS is vulnerable to impersonation attacks, and a malicious vehicle can act as an ar-bitrary vehicle to broadcast fake messages or even counterfeits another group member to send fake messages securely among themselves. To deal with this issue, they proposed b-SPECS+ to overcome the weaknesses of SPECS. In [12], Shim et al. proposed a Conditional Privacy preserving Authentication Scheme (CPAS), which is based on Computational Diffie-Hellman (CDH), to bridge the gap between the privacy and non-repudiation requirements. In [13], Li et al. proposed a Rapid Certification Scheme (RCS), in which a VANET leader is responsible to collect the messages of n distinct vehicles, and then sends them to RSU. The RSU verifies the batch of messages. The RCS is able to reduce the transmission overhead of RSUs by integrating messages into batches.

III. PROPOSED SYSTEM

we will propose a Proxy Based Authentication Scheme (PBAS) for this purpose. In this proposed scheme, each proxy vehicle plays an important role, which is adopted to authenticate multiple messages with the help of a verifi-cation function at the same time. In this way, the distributed computing can be used to shed the time-consuming centralized computing loads at RSUs. We also design a systematic and independent mechanism for RSUs to verify the output of the verification function from different proxy vehicles,
by which an RSU can evaluate the validity levels of different messages in the same way as done in separate verification schemes. In addition, batch key negotiations can also be accomplished in the proposed scheme, in which an RSU can complete the batch process of vehicles' key negotiations by Broadcasting a single
Proxy

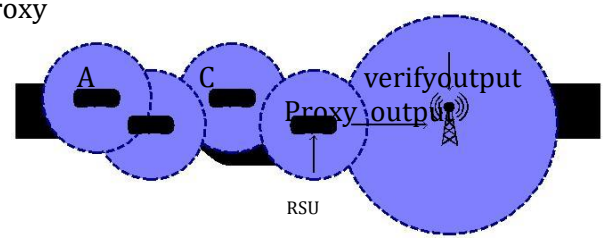

Fig. 1. PBAS reduces the computation load of RSUs via the cooperation amongst proxy vehicles,
Specifically, the design requirements of the proposed PBAS can be summarized as follows:

1)The scheme should be designed to meet the computational efficiency requirements of VANETs

2)The scheme should be designed to meet the general security requirements of VANETs, such as message integrity and authentication, privacy preservation, etc.

3)The scheme has the property that enables the verification process to continue even in the event that a small number of proxy vehicles have been compromised in VANETs

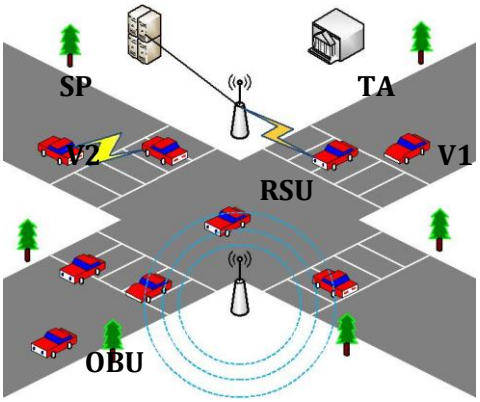

Fig. 2. A VANET communication system

System Model

Fig. 2 introduces a two-layer network model of VANETs with its underlined security layer and communication layer the security layer is comprised of a Trust Authority (TA) and tamper proof devices. The TA is trusted by all entities in the system, it is in charge of distributing the secret keys to all entities, and it has an ability for tracing back to the real identity of a vehicle whenever any uncertainty occurs. According to the VANET standard [8] [9], a tamper proof device installed in the OBU of a vehicle is responsible for storing security materials and implementing all crypto operations. On the other hand, the communication layer is comprised of V2I and V2V modules.

The V2V communication system provides a 360-degree view
of all its peer vehicles within the communication range. The V2I communication and broadcast systems provide traffic and entertainment information for the drivers.

Security Model

In [1], Raya et al. defined five basic attacks, including bogus information, cheating with sensor information, ID disclosure of the other vehicles in order to track their locations, Denial of Service (DoS), and masquerading. [32] [33] extended the attack types by introducing replay attack. In this section, we take all those basic attacks into consideration in a VANET of interest, except for ”cheating by sensor information” because the research on this particular topic belongs to data-centric trust establishment [34] [35] [36].

The work reported in [37] indicated that security mech-anisms of the VANET framework should support different applications and services. Hence, before discussing the se-curity requirements of our scheme, we first consider two application scenarios, namely safety related applications and value-added applications. For the safety related applications, vehicles in danger will send (broadcast or unicast) safety related messages to other entities in VANETs. The entities need to authenticate these messages before utilizing them. In the safety related applications, there are typically no confiden-tiality requirements on these safety related messages. For the value-added applications, the confidentiality is required. RSUs are registered as the gateways for Internet access, via which the vehicles that request for the services can establish secrecy links with Internet Service Provider (ISP) because most of the services levy charges. Hence, the messages from ISP can satisfy confidentiality through the key generation process between vehicles and RSUs. In summary, the following four security requirements are needed in PBAS:

1)Message integrity and authentication: Messages sent by vehicles can be authenticated to prove that they are indeed sent by authorized entities without being mod-ified or forged. Moreover, RSUs should have an ability to authenticate a large amount of signatures for many vehicles.

2)Identity privacy preserving and traceability: The real identity of a vehicle should be kept anonymous, which is heterogeneous with the other pseudo identities. Any third party should not be able to reveal the real identity of
a vehicle by analyzing multiple messages sent from it. However, when the vehicles send malicious information, TA has an ability to reveal the real identities from the pseudo identities of the misbehaved vehicles.

3)Resisting signature replay attacks: Signature replay
at-tacks can be prevented by such a carefully designed scheme. The definition of a signature replay attack can be generalized as an attack that replays the signatures from a different vehicle for the intended or expected RSUs, thereby to fool the RSUs to believe that they have successfully completed the verification of the owner of these signatures.

4)Confidentiality: A server can establish a secure

5)Communication link with a requesting vehicle for subsequent communications. For instance, ISP and parking pay-ments systems require that the session key negotiation process generates the keys for confidentiality of their transmitted messages.

IV. CONCLUSION

we assume that the traffic density is equal to the number of signatures in a verification period, and each vehicle periodically broadcasts a traffic related message every 300 ms. At least m vehicles should work as the proxy vehicles to verify the messages, and a proxy vehicle can act on at most 300 messages. Thus, m = 300 . In addition, we assume that the communication coverage of an RSU is one square kilometer. the relationship between the number of messages within an RSU's coverage area and the computation overhead of the RSU. We can see from the figure that the computation overhead increases as the number of messages increases. In addition, we can also see that the computational overhead of previous methods is the highest when the number of messages is larger than ten. In other words, the current standard ECDSA scheme is incompatible with the dynamic traffic patterns. PBAS is more efficient when verifying a large number of signatures: when there are more than 40 messages, the computation overhead of PBAS in a RSU is much lower than the others. For instance, in one second, the maximum number of signatures that can be verified by the RSU is approximately 2450, 1000, 1100, and 2000 for other methods respectively. In PBAS, this number reaches 26500. PBAS makes use of vehicles' computational capacity to reduce the burden of RSUs, where the proxy vehicles can authenticate multiple messages from the other vehicles. PBAS also provides RSUs with a systematic and independent mech-anism to verify the messages from the proxy vehicles. In addition, PBAS can negotiate a session key with every other vehicle for the confidentiality of sensitive information. The evaluation model of PBAS showed that PBAS offers fault tolerance, which enables the scheme to continue operating properly even if a small number of proxy vehicles are compro-mised in VANETs. Moreover, we analyzed and compared the performance of PBAS with the other authentication schemes in terms of their computation and transmission overheads. We also used simulations to verify the efficiency of PBAS in realistic environments, showing that PBAS is a promising security scheme for efficient VANET authentication. In this work on PBAS, we focused on cryptography algorithm under an assumption that any vehicle having completed system initialization can act as a proxy vehicle. However, it is crucial to make sure that these vehicles have incentives to serve for the others under the condition of efficient message delivery. In the future, we will exploit the game theory to study incentives mechanism. The redundant authentication is another issue, in which different proxy vehicles may work on the same message. To minimize the redundant authentication events, we should design a selection strategy that combines extra computation resource utilization optimization and redundant authentication reduction.

REFERENCES

[1]M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks",
Journal of Computer Security, vol. 15, pp. 39-68, 2007.
[2]T. W. Chim, S. M. Yiu, C. K. Hui, and O.K. Li, "VSPN: VANET-based secure and privacy-preserving navigation", IEEE Trans. on Computers, vol. 63, pp. 510-524, 2014.

[3]J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks", IET, Communications, vol. 4, pp. 894-903, 2010.

[4]S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", Telecom-munication Systems, vol. 50, pp. 217-241, 2012.

[5]A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication", Journal of Communications and Networks, pp. 574-588, 2009.

[6]C. Zhang, X. Lin, R. Lu, P. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications", IEEE Trans. on Vehicular Technology, vol. 57, pp. 3357-3368, 2008.

[7]C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks", in Proc. IEEE INFOCOM 2008, pp. 246-250, 2008.

[8]Dedicated Short Range Communications (DSRC), [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

[9]1609.2-2013-IEEE standard for wireless access in vehicular environments-security services for applications and management messages, IEEE Std 1609, 2013.

[10]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. on Vehicular Technology, vol. 60, pp. 248-262, 2011.

[11]S. J. Horng, S. F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "b-SPECS+: Batch verification for secure pseudonymous authentication in VANET", IEEE Trans. on Information Forensics and Security, vol. 8, pp. 1860-1875, 2013.

[12]K. A. Shim, "CPAS: An efficient conditional privacy-preserving au-thentication scheme for vehicular sensor networks", IEEE Trans. on Vehicular Technology, vol. 61, pp. 1874-1883, 2012.

[13]X. Li and L. Wang, "A rapid certification protocol from bilinear pairing for vehicular ad hoc networks", in IEEE Conf. Trust, Security and Privacy in Computing and Communcations (TrustCOM) 2012, pp. 890-895, 2012.

[14]D. Johnson and A. Menezes, "The elliptic curve digital signature algorithm (ECDSA)", International Journal of Information Security, vol. 1, pp. 36-63, 2001.

[15]J. Petit, "Analysis of ECDSA authentication processing in VANETs", in IEEE Conf. New Technologies, Mobility and Security (NTMS) 2009, vol. 1, pp. 1-5, 2009.

[16]A. Perring, R. Canetti, D. Song, and D. Tygar, "Efficient and secure source authentication for multicast", in Proc. Network and Distributed Systems Security (NDSS), pp. 35-46, 2001.

[17]D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", Springer-Verlag, pp. 213-229, 2001.

[18]H. Yoon, J. H. Cheon, and Y. Kim, "Batch verification with ID-based signatures", in Proc. Information Security and Cryptology, pp. 233-248, 2004.

[19]C. Zhang, P. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications", Wireless Networks, vol. 17, pp. 1851-1865, 2011.

[20]T. W. Chim, S. M. Yiu, C. K. Hui, and O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs", Ad Hoc Networks, vol. 12, pp. 189-203, 2011.

[21]A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks]", IEEE Wireless Communications, vol. 17, pp. 22-28, 2010.

[22]A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation", in Proc. ACM conf. Computer and communications security, pp. 417-426, 2008.

[23]A. Wasef and X. Shen, "EDR: Efficient decentralized revocation protocol for vehicular ad hoc networks", IEEE Trans. on Vehicular Technology, vol. 58, pp. 5214-5224, 2009.

[24]A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed-certificate-service scheme for vehicular networks", IEEE Trans. on Vehicular Technology, vol. 59, pp. 533-549, 2010.

[25]A. Wasef and X. Shen, "EMAP: Expedite message authentication proto-col for vehicular ad hoc networks", IEEE Trans. on Mobile Computing, vol. 12, pp. 78-89, 2013.

[26]R. Lu, X. Lin, H. Luan, "Pseudonym changing at social spots: an effective strategy for location privacy in VANETs", IEEE Trans. on Vehicular Technology, vol. 61, pp. 86-96, 2012.

[27]Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications", IEEE Trans. on Vehicular Technology, vol. 59, pp. 3589-3603, 2010.

[28]J. Choi, S. Jung, "A security framework with strong non-repudiation and privacy in VANETs", in IEEE Conf. Consumer Communications and Networking Conference (CCNC) 2009, pp.1-5, 2009.

[29]R. Lu, X. Lin, Z. Shi, and X. Shen, "A lightweight conditional privacy-preservation protocol for vehicular traffic-monitoring systems", IEEE Intelligent Systems, vol. 28, pp. 62-65, 2013.

[30]X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks", IEEE Trans. on Vehicular Technology, vol. 63, pp. 907-919, 2014.
[31]Y. Qian, K. Lu, and N. Moayeri, "A secure VANET MAC protocol for DSRC applications, in Proc. IEEE GLOBECOM 2008, 2008.

[32]G. Samara, W. A. H. A. Salihy, R. Sures, "Security analysis of vehicular ad hoc networks (VANET)", in IEEE Conf. Network Applications Protocols and Services (NETAPPS) 2010, pp.55-60, 2010.
[33]application-oriented VANETs", in Proc. IEEE VTC Spring 2008, 2008.

[34]X. Lin and X. Li, "Achieving efficient cooperative message authen-tication in vehicular ad hoc networks", IEEE Trans. on Vehicular Technology, vol. 62, pp. 3339-3348, 2013