ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

ETAM Enhanced Trust Authentication Mechanism for Vehicular Ad Hoc Networks

J. Martina Jasmine[1]

Second year M.E. (CSE), Sri Vidya College of Engineering & Technology, Virudhunagar Tamilnadu, India[1]

ABSTRACT - VANETs are vulnerable to malicious attacks. A number of secure authentication schemes based on asymmetric cryptography have been proposed to prevent such attacks. However, these schemes are not suitable for highly dynamic environments such as VANETs, because they cannot efficiently cope with the authentication procedure. Hence, this still calls for an efficient authentication scheme for VANETs. In this paper, we propose a decentralized lightweight authentication scheme called trust-extended authentication mechanism (ETAM) for vehicle-to-vehicle communication networks. ETAM adopts the concept of transitive trust relationships to improve the performance of the authentication procedure and only needs a few storage spaces. Moreover, ETAM satisfies the following security requirements: anonymity, location privacy, mutual authentication, forgery attack resistance, modification attack resistance, replay attack resistance, no clock synchronization problem, no verification table, fast error detection, perfect forward secrecy, man-in-the-middle attack resistance, and session key agreement.

KEYWORDS- Authentication, decentralized, lightweight, trust extended vehicular ad hoc networks (VANET)

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) have been attracted increasing attention from both industry and academia. The major components of a VANET are the wireless on-board unit (OBU), the roadside unit (RSU), and authentication server (AS). OBUs are installed in vehicles to provide wireless communication capability, while RSUs are deployed on intersections or hotspots as an infrastructure to provide information or access to the Internet for vehicles within their radio coverage. The AS is responsible for installing the secure parameters in the OBU to authenticate the user. Based on IEEE 802.11p, the dedicated short range communication system supports two kinds of communication environments: vehicle-to-infrastructure (V2I) and vehicle-to vehicle (V2V) communications.

However these schemes do not consider the security problem. Recently, the security issue in VANETs has become a hot topic, and then many researchers provide the V2I and V2V authentication mechanisms to protect valid users. However, the design for an efficient V2V authentication mechanism is more challenge than that for V2I authentication mechanism in VANETs because the vehicle cannot be authenticated via the infrastructure directly in V2V communications. Therefore, we focus on V2V network environments and propose an efficient authentication scheme in this paper. To address the above need, we propose a decentralized authentication scheme, called ETAM, for V2V communication networks. There exists no centralized authority to perform the authentication procedures of vehicles. ETAM is a lightweight authentication scheme because it only uses an XOR operation and a hash function. Although ETAM needs low computation cost, it still satisfies the following security requirements: anonymity, location privacy, mutual authentication, resistance to stolen-verified attacks, forgery attacks, modification attacks and replay attacks, as well as no clock synchronization problem, fast error detection, perfect forward secrecy, man-in- the-middle attack resistance, and session key agreement. Moreover, our scheme only requires a few storage spaces than other schemes because the vehicle does not need to store the authentication information (e.g., public key) of the entire vehicle.

II. RELATED WORK

Raya and Hubaux [6] preloaded each vehicle with a large number of anonymous public and private key pairs, as well as the corresponding public key certificates. Then, traffic messages are signed with a public key-based scheme, and each pair of public and private key has a short lifetime to preserve its privacy. However, this approach works with high computation cost, high storage cost, and high communication overhead. Freudiger et al. [7] used the cryptographic MIXzoneto enhance the location privacy, and Sampigethava et al.[8] provided location privacy by utilizing the group navigation of vehicles. However, these approaches do not work well in highly dynamic environments like VANETs because they use asymmetric cryptography or a digital signature verification scheme, which results in high computation costs, long authentication latency.

Zhang et al. [9] proposed an RSU-aided messages authentication scheme (RAISE), which uses the symmetric key hash message authentication code, instead of a public key infrastructure-based message signature, to reduce the signature cost. However, in RAISE, the key agreement process still executes the exponent operations, which leads to a high computation cost. Moreover, the RSU needs to maintain the extra ID-Key table, resulting in more storage cost. Hence, there is still a need for an efficient authentication scheme for VANETs with low computation and low storage costs.

Korkmaz et al. [2] propose a link-layer broadcast protocol to help disseminate the data. The protocol relies on link-layer acknowledge mechanisms to improve the reliability of the multihop broadcast. More specifically, only one vehicle is used to forward and acknowledge the broadcast packet to reduce the broadcast storm problem. However, in the case of network congestion, the link-layer solution is not enough. Furthermore, since many information sources may exist in a given urban area, the amount of broadcasted data from these sources can easily consume the limited bandwidth. Thus, it is important to study the maximum amount of data that can be disseminated in a given area [i.e., the dissemination capacity (DC)].

Xu et al. [3] propose an opportunistic dissemination (OD) scheme. In this approach, the data center periodically broadcasts some data, which will be received and stored by passing vehicles. Whenever two vehicles move into the transmission range of each other, they exchange data. This scheme does not rely on any infrastructure and, hence, is suitable for highly dynamic VANETs. However, after a data item has been propagated into the network, it is hard to timely remove the outdated information, particularly when it is frequently updated. In addition, the performance of the OD scheme is poor in areas with high vehicle density due to media access control (MAC)- layer collisions . This can easily lead to severe congestion and significantly reduce the data delivery ratio. To mitigate the excessive transmissions and congestion.

III. ETAM

A ETAM is a decentralized authentication scheme, and the LEs need not to keep the authentication information of the entire vehicles. The proposed scheme involves eight procedures: initial registration, login, general authentication, password change, trust-extended authentication, key update, key revocation, and secure communication. Before a vehicle can join a VANET, its OBU must register with the AS.

A vehicle wants to access the service; it has to perform the login procedure. Next, the OBU checks the authentication state itself (i.e., the lifetime of the key). If the lifetime of the key is reduced to zero, the vehicle is mistrustful, and vice versa. The MV performs the general or trust-extended authentication procedure to be authenticated. The trustful vehicles assist other MVs in performing the authentication procedure or communicate with other trustful vehicles (i.e., secure communication procedure) to access the Internet. The trustful vehicle performs the key update procedure with the LE when the key lifetime is below the predefined threshold. Moreover, we also consider the password change procedure for user friendly.

IV. TRANSITIVE TRUST RELATIONSHIP

In VANETs, vehicles can be classified into to the following roles: a law executor (LE), a mistrustful vehicle (MV), and a trustful vehicle (TV) . An LE, such as police car or authorized public transportation (e.g., buses), acts like a mobile AS. Moreover, the LE is trustful permanently. A normal vehicle is regarded as trustful if it can be authenticated successfully; otherwise, it is deemed to be mistrustful. In addition, the TV becomes the MV when the key lifetime is over. To provide a secure communication environment, the OBU should be authenticated successfully before it can access the service. However, in V2V communication networks, as the number of LEs is finite, an LE is not always in the vicinity of the OBU. Even if the user is well meaning, the vehicle must still wait for the nearest LE and then perform the authentication procedure. Hence, there is an urgent need for an efficient authentication scheme The ETAM is based on the concept of transitive trust relationships. Initially, there are three vehicles in a VANET: a trustful LE and two other MVs carrying OBUs (i.e.,OBUi and OBUj). The state of the first mistrustful OBU (i.e., OBUi) becomes trustful and obtains the sufficient authorized parameter to authorize other mistrustful OBUs when it is authenticated successfully. Then, it plays the LE role temporarily to assist with the authentication procedure of OBUj . Thus, the other mistrustful OBUs can be authenticated by any trustful OBU without necessarily finding an LE, and all vehicles in a VANET can complete the authentication procedure quickly. Therefore, the key design issues of the authentication procedure based on the transitive trust relationship sare:1) how to let the TV own the authentication ability; 2) how to reduce the computational cost; 3) how to prolong the trustful state of the TV; and 4) how to use as little storage cost as possible.

A. Adversary Model

The following possible attack models can be used during the V2V authentication procedure.

1) Modification attack: The adversary modifies the packet resulting in the message against the integrity of the information.

2) Message replay attack: The adversary resends valid messages sent previously in order to disturb the traffic flow.
3) Movement tracking: Since wireless communication is based on a shared medium, an adversary can easily eavesdrop on any traffic. After intercepting a significant number of messages in a certain region, the adversary could trace the physical position and movement patterns of a vehicle by simply analyzing the information.
4) Impersonation attack: The adversary pretends to be a valid LE/TV to cheat the unauthenticated OBUs.

B. Security Requirements

1)Efficiency: In VANETs, the computational cost of vehicles must be as low as possible in order to have a real-time response.
2) Anonymity: The anonymous authentication procedure verifies that an OBU does not use its real identity to execute the authentication procedure.
3)Location privacy: An adversary collects the serial authentication messages of the OBU but it still failed to track the location of the vehicle.
4)Mutual authentication: A mutual authentication procedure is implemented whereby the LE must verify that the OBU is a legal user and the OBU must ensure that the LE is genuine.
5) Integrity: The message integrity means that data cannot be modified undetectably.

IV. CONCLUSION

ETAM to protect valid users in VANETs from malicious attacks. The amount of cryptographic calculation under ETAM was substantially less than in existing schemes because it only used an XOR operation and a hash function. Moreover, ETAM is based on the concept of transitive trust relationships to improve the performance of the authentication procedure. In addition, ETAM has a few storage spaces to store the authentication parameters.

REFERENCES

[1] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart \vehicles," IEEE Security Privacy Mag., vol. 2, no. 3, pp. 49–55, May– Jun. 2004.
[2] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner, "Urban multi-hopbroadcast protocol for inter-vehicle communication systems," in Proc.ACM VANET, Oct. 2004, pp. 76–85.
[3] B. Xu, A. Ouksel, and O. Wolfson, "Opportunistic resource exchange ininter-vehicle ad hoc networks," in Proc. IEEE Int. Conf. MDM, 2004,pp. 4–12.
[4] Dedicated Short Range Communications (DSRC) [Online].
[5] M. Nekovee and B. B. Bogason, "Reliable and efficient information dissemination in intermittently connected vehicular ad hoc networks," in Proc. IEEE Vehicular Technol. Conf., Apr. 2007, pp. 2486–2490.
[6] J. Zhao, Y. Zhang, and G. Cao, "Data pouring and buffering on the road: A new data dissemination paradigm for vehicular ad hoc networks," IEEE Trans. Vehicular Technol., vol. 56, no. 6, pp. 3266–3277, Nov. 2007.
[7] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix zones for location privacy in vehicular networks," in Proc. First Int. Workshop Wireless Netw. Intell. Transp. Syst., Aug. 2007, pp. 1–7.
[8] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE J. Selected Areas Commun., vol. 25, no. 8, pp. 1569–1589, Oct. 2007.
[9] 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 Int. Conf. Commun., May 2008, pp. 1451–1457.
[10] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," in Proc. IEEE Int. Conf. Consumer Electron., Commun. Netw., Apr. 2011, pp. 1758–1761.