Communication Efficient Distributed Decentralized Key Management Framework for Message Authentication in Vanet

G. VinothChakkaravarthy[1], Raja Lavanya[2], and P. Alli[1]

[1] Department of Computer Science and Engineering,
Velammal College of Engg.&Tech., Tamilnadu, India
[2] Department of Computer Science and Engineering,
P.S.N.A College of Engg.&Tech., Tamilnadu , India

Abstract . To provide authentication in Vehicular Ad-Hoc Network (VANET), a cost effective and communication efficient distributed key management framework based on dynamic decentralized group key agreement is proposed. In VANET, the critical issue is exchanging the safety related information such as warning about curves, sharp turns, speed limit and other related information between the vehicles. The proposed Group Secret Key Protocol (GSKP) is a promising security scheme to provide privacy by offering authentication between vehicles in VANET. In this framework, each Road Side Unit (RSU) dynamically generates the GSK and securely distributes the key to the OBUs of Vehicle. By using this GSK, the vehicles can interactively exchanging the safety related information without doing authentication for each communication. GSK is generated dynamically based on the share taken from each vehicle, so the GSK is distributed to only the valid set of vehicles. This technology ensures the dynamic nature in the way that whenever new vehicle comes in to the group or existing member goes out of the group the new GSK is generated. In addition, cooperative verifiers are intelligently selected to significantly reduce the computation and communication overhead.

Keywords: authentication, GSKP, Group Key agreement, Group secret key(GSK).

1 Introduction

Vehicular ad-hoc networks (VANETs) are an emerging area of interest for the security community. The important components involved in VANETs are road-side units (RSUs) and on-board units (OBUs). RSUs are positioned on the sides of roads, at stop lights and the like and on-board units (OBUs) which vehicles are equipped with. OBUs enable communication between vehicles and with RSUs.

A major application of this technology is the distribution of safety-related information, such as turn warnings, curve warnings, speed limit information and other types of vital information between vehicles traveling over the road. In safety driving application, each vehicle periodically broadcasts messages including its current position, direction

V.V. Das and J. Stephen (Eds.): CNC 2012, LNICST 108, pp. 405–408, 2012.

and velocity, as well as road information, information about traffic congestion. Since safety information may contribute to the survival of humans driving the vehicles participating a VANET, security is of crucial importance to the system.

Various types of services can be offered for VANET to provide security. Confidentiality is not a primary concern here. But the safety information must be distributed among valid set of vehicles. So message authentication is the primary concern. Since, this is a reliable group communication platform and each vehicle must be authenticated each time when it starts exchanging. So communication delay and computation overhead are the two issues to be considered because in safety driving application, vehicles broadcast messages every 300ms. Group key management protocols between the groups of vehicles offer cost effective authentication. Here, the computation overhead relies on how effectively the key are managed in crypto systems.

1.1 Challenges in VANET Environments

First, the vehicles in a VANET are constantly roaming around and are highly dynamic. Second, Since this is a highly dynamic environment, the number of peers in VANET can become very large. Each vehicle receives a lot of data from the nearby vehicles in a congested area. Third key challenge in modeling trust in a VANET environment is difficult, because VANET is a decentralized, open system i.e. there is no centralized infrastructure and peers may join and leave the network any time respectively.

2 Related Work

Using pseudonyms is a one basic idea .The shortcoming of this protocol is that it requires vehicles to store a large number of pseudonyms and certifications, where a revocation scheme for abrogating malicious vehicles is difficult to implement.

TESLA is a protocol can be applied, which is a hash based protocol, to reduce the computation overhead. However, the malicious vehicles could not be identified in this protocol.

While all these studies assume a centralized key management scheme, hence a cost effective decentralized distributed key management framework is proposed in this paper to offer authentication which achieves privacy between the vehicles in VANET.

3 Proposed Group Secret Key Protocol (GSKP)

A protocol called **Group Secret Key Protocol (GSKP) is proposed to** for privacy preservation of VANETs. The proposed work is efficient to avoid the communication latency in reliable communication platform, without minimizing cryptographic operations. In reliable communication, communication latency increasingly dominating the key setup latency, Hence, the bottleneck is shifted from computation to communication latency. So to reduce the communication latency, the number of cryptographic operations and the number of rounds should be significantly reduced. The proposed scheme in this paper is efficient to avoid such latency without minimizing cryptographic operations. GSKP is based on the formation of a virtual Skinny Tree (VST) which is based on the approach that extends the 2-party Diffie-Hellman key exchange and supposes the formation of a secure **group**. This protocol involves the following computation and communication requirements: O(n) communication rounds and O(n) cryptographic operations [2]are necessary to establish a shared key in a group of ‘n’ members. This framework is extended to deal with dynamic groups in a communication-efficient manner for VANET.

In the proposed system, three types of entities can be incorporated namely, authorities, Road Side Unit (RSU), and nodes. Authorities are responsible for key generation and malicious vehicle judgement. Authorities have powerful firewalls and other security protections.

RSUs are deployed at the road sides, which are in charge of key management in the proposed framework. Traffic lights or road signs can be used as RSUs after renovation. RSUs communicate with authorities through wired network. It is assumed that a trusted platform module is equipped in each RSU. It can resist software attacks but not sophisticated hardware tampering. Nodes are ordinary vehicles on the road that can communicate with each other and RSUs through radio. The assumption is that each vehicle is equipped with a GPS receiver using DGPS[1] with an accuracy on the order of centimeters and an on board unit (OBU) which is in charge of all communication and computation tasks. Nodes have the lowest security level.

3.1 Group Secret Key(GSK) Generation

Fig 1 shows the Group Secret Key Protocol (GSKP) , in which the entire group shares the same secret key called as session-encrypting key (SEK).

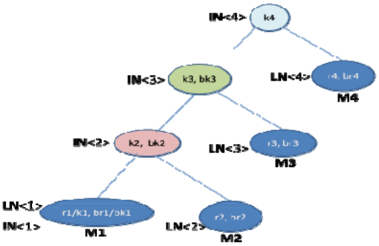

Fig. 1. Group Secret Key Formation

The tree has two types of nodes: leaf and internal. Each leaf node is associated with a specific group member. An internal node IN(i) always has two children: another (lower) internal node IN(i-1) and a leaf node LN(i). Each leaf node LN(i) has a session randomri chosen and kept secret by Mi. The public version thereof is bri = α^{ri} mod p. Every internal node IN(j) has an associated secret key kj and a public instant key (bkey) bkj = α^{kj} mod p[2]. The secret key ki (i> 1) is the result of a Diffie-Hellman key agreement between the node’s two children

$$\mathbf{ki = (bki\text{-}1)^{ri} \bmod p = (bri)^{ki\text{-}1} \bmod p = \alpha^{riki\text{-}1} \bmod p \text{ if } i> 1}.$$

The following membership changes are considered: Single member changes include member join or leave, and multiple member changes include group merge and group partition.

4 Protocol Discussion

In VST, the group key is calculated using a function of all the private keys of the vehicles, the session key for individual user. The dynamicity of the proposed scheme is shown whenever the Instant key gets varied on the arrival or departure of a user which doesn't allows impersonation of the user.

As the newly generated key is obtained from current user's hidden key, the valid currently operating users only can access it. Hence authentication is successfully ensured. It leads to secure communication.

Whenever a node joins/leaves, the RSU has to perform (n+l)/(n-1) computations respectively which in turn reduces the computational complexity. The above all points make our scheme is robust for offering privacy and also easy for verification.

5 Conclusion

In this paper, a novel dynamic decentralized distributed key management scheme based on the group key agreement is proposed to provision privacy in the VANETs. This protocol involves O(n) communication rounds and O(n) cryptographic operations to establish a GSK in a group of ‘n’ members. So it is communication efficient. The proposed design guarantees that RSUs distribute keys only to valid set of vehicles, so it offers strong authentication with less computation complexity and communication delay.

References

1. Hao, Y., Cheng, Y., Zhou, C., Song, W.: A Distributed Key Management Framework with Cooperative Message Authentication in VANETs. IEEE Journal on Selected Areas in Communications 29(3) (March 2011)
2. Yongdae, P., Tsudik: Group Key Agreement efficient in communication. IEEE Transactions on Computers
3. Langley, C., Lucas, R., Fu, H.: Key Management in Vehicular Ad-Hoc Networks
4. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. Journal of Computer Security 15(1), 39–68 (2007)
5. Freudiger, J., Raya, M., Feleghhazi, M., Papadimitratos, P., Hubaux, J.P.: Mix zones for location privacy in vehicular networks. In: Proc. International Workshop on Wireless Networking for Intelligent Transportation Systems, Vancouver, British Columbia (August 2007)
6. Duraiswamy, K., Shantharajah, S.P.: Key Management and Distribution for Authenticating Group Communication. IEEE Transactions on Computers (2006)