International Journal of Engineering Research and Modern Education (IJERME)
Impact Factor: 7.018, ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume 3, Issue 1, 2018

DISTRIBUTED AGGREGATION OF ATTRIBUTED BASED SIGNATURE SCHEME FOR AUTHENTICATED COMMUNICATION IN VANET

S. Keerthana* & T. Geetha**

* M.E Scholar, Department of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Computer Science and Engineering, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Cite This Article: S. Keerthana & T. Geetha, "Distributed Aggregation of Attributed Based Signature Scheme for Authenticated Communication in VANET", International Journal of Engineering Research and Modern Education, Volume 3, Issue 1, Page Number 4-7, 2018.

Abstract:

Vehicular Ad hoc Networks (VANETs) consists of vehicles and distributed roadside units (RSUs). The vehicles can send safety related messages like speed, location of the vehicle, dangerous road conditions to any nearby vehicles and to the RSU and vice versa. In VANET, each vehicle broadcasts a message to nearby vehicles and RSUs every few hundreds of milliseconds. A vehicle or an RSU may receive hundreds of messages in a short period. If the messages cannot be processed in time, occurrence of traffic jams and accidents is possible. Hence, it is critical to devise security and privacy mechanisms that never lead to an unaffordable reaction delay. As the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may want to keep private. Pseudonym based schemes have been proposed to preserve the location privacy of vehicles. However, those schemes require the vehicles to store a large number of pseudonyms and certifications, and do not support some important secure functionality such as authentication and integrity. Existing secure and privacy preserving protocols in VANETs are fast and does not depend on ideal tamper proof devices embedded in the vehicles. This is a major concern when it comes to privacy.

Notations:

RSU	Road Side Unit
TPD	Tamper Proof Device
ITS	Intelligent Transportation System
HMAC	Hash Message Authentication Code
PKG	Private Key Generation
IBC	Identify Based Cryptography
TA	Trusted Authority
LBC	Local Based Services
V2V	Vehicle to Vehicle
CAM	Cooperative Awareness Message
MTA-OTFABAS	Multi Trusted Authority one time frequency attribute based aggregation signature scheme
IBOOS	ID based Online/Offline Signature
CLR	Certificate Revocation List

Introduction:

Existing secure and privacy-preserving vehicular communication protocols in vehicular ad hoc networks face the challenges of being fast and not depending on ideal tamper-proof devices (TPDs) embedded in vehicles. To address these challenges, propose a vehicular authentication protocol referred to as distributed aggregate privacy-preserving authentication. The pro- posed protocol is based on our new multiple trusted authority one-time identity-based aggregate signature technique. With this technique a vehicle can verify many messages simultaneously and their signatures can be compressed into a single one that greatly reduces the storage space needed by a vehicle or a data collector (e.g., the traffic management authority). Instead of ideal TPDs, our protocol only requires realistic TPDs and hence is more practical.

In VANET some serious network attacks such as man in middle attack, masquerading is possible. Vehicle privacy is also a critical concern. A vehicular message usually contains information on a vehicle's speed, location, direction etc. From those messages, a lot of private information about the driver can be inferred. Furthermore, malicious vehicles may send fake messages to misguide other vehicles into accidents. This implies that privacy should be conditional in the sense that the message generators should be traceable when fake messages cause harms. For this purpose, the vehicle-generated messages must be stored by the receiving vehicles and other entities (e.g., the traffic management authority). In VANET, each vehicle broadcasts a message to nearby vehicles and RSUs every few hundreds of milliseconds. A vehicle or an RSU may receive

hundreds of messages in a short period. If the messages cannot be processed in time, traffic jams and even accidents may ensue.

Hence, it is critical to devise security and privacy mechanisms that do not lead to an unaffordable reaction delay. Existing secure and privacy-preserving vehicular communication protocols in vehicular ad hoc networks face the challenges of being fast and not depending on ideal tamper-proof devices (TPDs) embedded in vehicles. The proposed protocol is based on a new multiple trusted authority one-time identity based, frequency and attribute - based aggregate signature technique. A vehicle is able to verify many messages at the same time and their signatures can be compressed as a single unit. This reduces the storage space required by a vehicle or a data collector to a considerable extend. A practical cooperative message authentication protocol is proposed to elevate the verification burden, where each vehicle just needs to verify a small amount of messages. The details of possible attacks and the corresponding solutions are also discussed.

Vanet Architecture:

Vehicular ad hoc networks (VANETs) are created by applying the principles of mobile ad hoc networks (MANETs) – the spontaneous creation of a wireless network for data exchange – to the domain of vehicles. VANETs were first mentioned and introduced in 2001 under "car-to-car ad hoc mobile communication and networking" applications, where networks can be formed and information can be relayed among cars. It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation and other roadside services. VANETs are a key part of the intelligent transportation systems (ITS) framework.

VANETs are referred as Intelligent Transportation Networks. VANET became mostly synonymous with the more generic term Inter-Vehicle Communication (IVC) although the focus remains on the aspect of spontaneous networking, much less on the use of infrastructure like Road Side Units (RSUs) or cellular networks. VANETs can use any wireless networking technology as their basis. The most prominent are short range radio technologies like WLAN (either standard Wi-Fi or ZigBee. In addition, cellular technologies or LTE can be used for VANETs. The latest technology for this wireless networking is visible light communication.

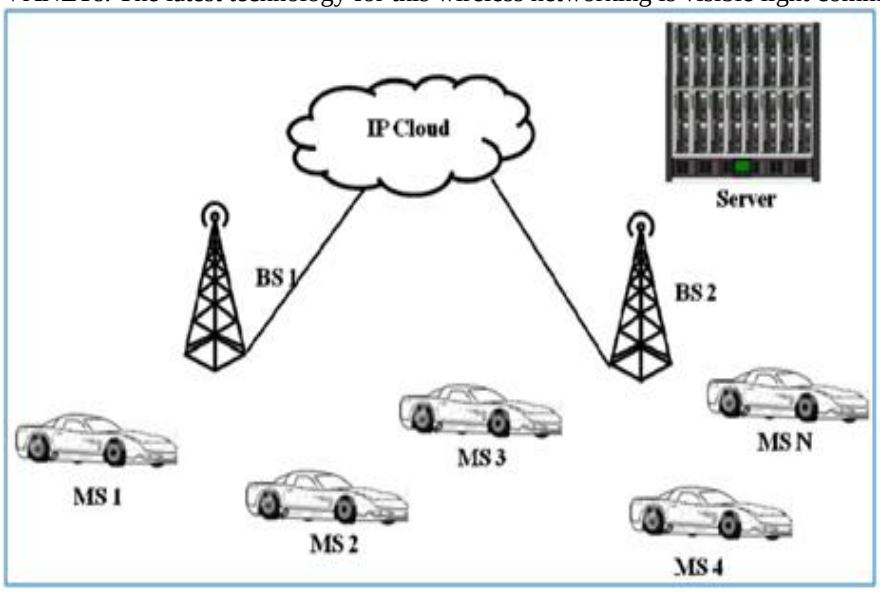

Figure 1: Architecture of Vanet

Applications of Vanet:

VANETs support a wide range of applications – from simple one hop information dissemination of, e.g., cooperative awareness messages (CAMs) to multi-hop dissemination of messages over vast distances. Most of the concerns of interest to mobile ad hoc networks (MANETs) are of interest in VANETs, but the details differ. Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. And finally, most vehicles are restricted in their range of motion, for example by being constrained to follow a paved highway. The various applications of VANETS are listed below.

Safety Applications:

Safety applications include monitoring of the surrounding road, approaching vehicles, surface of the road, road curves etc. The Road safety applications can be classified as:

- ✓ Real-time traffic: The real time traffic data can be stored at the RSU and can be available to the vehicles whenever and wherever needed. This can play an important role in solving the problems such as traffic jams, avoid congestions and in emergency alerts such as accidents etc.

- ✓ Co-operative Message Transfer: Slow/Stopped Vehicle will exchange messages and co-operate to help other vehicles. Though reliability and latency would be of major concern, it may automate things like emergency braking to avoid potential accidents. Similarly, emergency electronic brake-light may be another application.
- ✓ Post Crash Notification: A vehicle involved in an accident would broadcast warning messages about its position to trailing vehicles so that it can take decision with time in hand as well as to the highway patrol for tow away support.
- ✓ Road Hazard Control Notification: Cars notifying other cars about road having landslide or information regarding road feature notification due to road curve, sudden downhill etc.
- ✓ Cooperative Collision Warning: Alerts two drivers potentially under crash route so that they can mend their ways.

Commercial Applications:

Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video. The Commercial applications can be classified as:

- ✓ Remote Vehicle Personalization/ Diagnostics: It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure.
- ✓ Internet Access: Vehicles can access internet through RSU if RSU is working as a router.
- ✓ Digital map downloading: Map of regions can be downloaded by the drivers as per the requirement before traveling to a new area for travel guidance. Also, Content Map Database Download acts as a portal for getting valuable information from mobile hot spots or home stations.
- ✓ Real Time Video Relay: On-demand movie experience will not be confined to the constraints of the home and the driver can ask for real time video relay of his favorite movies.
- ✓ Value-added advertisement: This is especially for the service providers, who want to attract customers to their stores. Announcements like petrol pumps, highways restaurants to announce their services to the drivers within communication range. This application can be available even in the absence of the Internet.

Convenience Applications:

Convenience application mainly deals in traffic management with a goal to enhance traffic efficiency by boosting the degree of convenience for drivers. The Convenience applications can be classified as:

- ✓ Route Diversions: Route and trip planning can be made in case of road congestions.
- ✓ Electronic Toll Collection: Payment of the toll can be done electronically through a .Toll Collection Point. A Toll collection Point shall be able to read the OBU of the vehicle. OBUs work via GPS and the on-board odometer or techograph as a back-up to determine how far the Lorries have travelled by reference to a digital map and GSM to authorize the payment of the toll via a wireless link. TOLL application is beneficial not only to drivers but also to toll operators.

Productive Applications:

The Productive applications can be classified as:

- ✓ Environmental Benefits: AERIS research program is to generate and acquire environmentally-relevant real-time transportation data, and use these data to create actionable information that support and facilitate “green” transportation choices by transportation system users and operators.

Methods:

System Analysis:

Existing System: Vehicular ad hoc network (VANET), consisting of a network of vehicles, moving at a relatively high speed, that communicate among themselves with different purposes, being the main purpose that of improving security on the road. In VANET, each vehicle broadcasts a message to nearby vehicles and RSUs every few hundreds of milliseconds. A vehicle or an RSU may receive hundreds of messages in a short period. If the messages cannot be processed in time, occurrence of traffic jams and accidents is possible. Five categories of proposals have addressed security and privacy concerns in VANETs. The first category is based on digital signatures combined with anonymous certificates. To cope with the privacy issue, digital signatures must be combined with short-lived anonymous certificates. The second category is based on group signatures. This approach is free from traditional certificate management.

The third category is based on identity-based cryptography (IBC). In IBC, an entity uses a recognizable identity as its public key and its private key is generated by a trusted authority (TA) using a master secret. To achieve privacy, the identity of an entity is replaced with pseudonyms. This approach is similar to the one based o25n anonymous certificates. The fourth category is about the IBV protocol which is based on an ideal tamper-proof device (TPD)

Disadvantages:

- ✓ Suffers from a heavy certificate management burden to maintain all the anonymous certificates of all the vehicles.

- ✓ The verification and transmission costs of a group signature are very much higher than those of a traditional signature.
- ✓ The overheads of signature verification and transmission are very high.
- ✓ Experiences the problem of pseudonym burden.

Proposed System:

A new multiple trusted authority one – time identity based protocol is proposed to solve the mentioned disadvantages in the existing system. This protocol is based on frequency and attribute – based aggregate concept. A vehicle in the VANET is able to verify many messages at the same time and all their signatures can be compressed as a single unit. This paves way to reduce the storage space required by a vehicle or a data collector to some extent. A co – operative message authentication protocol is proposed to elevate the verification burden where each vehicle needs to verify a small amount of messages. This protocol consists of a root TA, several lower-level TAs and users. Each lower-level TA is enrolled by the root TA. A user can register to any lower-level TA and compute a signature on a message if the user has obtained a private key from the lower-level TA. The signature is only valid under the user's identity and the public information of the lower-level TA. This protocol is resistant to side – channel attacks. The possibility of various attacks and their corresponding solutions are discussed. Also developed a system analytical model for analyzing various information about the traffic conditions and carry out NS2 simulations to examine the key distribution delay and missed detection ratio of malicious messages, with the proposed key management framework. Instead of ideal TPDs, this protocol only requires realistic TPDs and hence is more practical.

Advantages:

- ✓ Attribute based encryption scheme is used in this protocol
- ✓ Handle large number of messages
- ✓ Signature based SHA algorithm

Conclusion:

Proposed a Multi Trusted Authority One Time Frequency Attribute based Aggregate Signature Scheme (MTA-OTFABAS), a protocol for secure vehicular communications. This protocol is based on frequency and attribute based aggregate concept. MTA-OTFABAS achieves enhanced privacy (i.e., conditional unlink ability), key escrow freeness, robustness and fast message processing, without requiring an ideal TPD. Simulations show that our protocol is practical.

References:

1. V. Daza, J. Domingo-Ferrer, F. Sebe, and A. Viejo, "Trustworthy privacy preserving car-generated announcements in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 58, no. 4, pp. 1876–1886, May 2009
2. J. Domingo-Ferrer, Q.Wu and U. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.
3. P. Golle, D. Greene, and JStaddon, "Detecting and correcting malicious data in VANETs," in Proc. VANET, 2004, pp. 2937.
4. E. Kiltz and K. Pietrzak, "Leakage resilient ElGamal encryption," in Proc. ASIACRYPT, 2010, pp. 595–612 C.
5. Laurendeau and M. Barbeau, "Probabilistic localization and tracking of malicious insiders using hyperbolic position bounding in vehicular networks," EURASIP J. Wireless Commun. Netw, vol. 2, pp. 1–13, 2009
6. J. Li, H.\ Lu, and M. Guizani, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 4, pp. 938–948, Apr. 2015
7. X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacypreserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, 2007.
8. R. Lu, C. Zhang, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," in Proc. IEEE INFOCOM, 2008, pp. 246–250.B.
9. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proc. Hot Nets-IV, 2005, pp. 1–6.
10. www.sciencedirect.com/science/article
11. www.ibm.com/support/knowledgecenter