Security and Location Privacy using RSU in VANET

[1]Manivannan Krishnamoorthi, [2]Arikaran Krishnamoorthy,
[3]Arun Sembulingam, [4]Gowshikan Shanmugam, [5]Nandhakumar Nagappan

[1]*Assistant Professor, V.S.B. Engineering College, Karur, Tamilnadu, India.*
[2][3][4][5]*Student, V.S.B. Engineering College, Karur, Tamilnadu, India.*

Abstract:

Security and Location privacy are the core issues in vehicular ad-hoc networks. Due to the openness of today's networks, the lack of location privacy protection could result in severe consequences that make users the target of fraudulent attacks. Cryptographic mixed zone (CMIX) is an assurance tool to strengthen vehicle privacy, in which the safety messages of vehicles are encrypted using a group secret key. In that way, internal details of its implementation should be invisible by an outsider. Existing CMIX protocols need fully trusted dealers to distribute group secret keys and/or suffer from the problem of efficient key update. Group key agreements are widely employed for secure group communications in modern collaborative and group-oriented applications. In this paper, we propose a novel framework, named as one-time identity based dynamic asymmetric group key agreement (DAGKA) protocol, which allows a group of members to dynamically establish a public group encryption key while each member has a different secret decryption key in an identity-based cryptosystem to create CMIX-es, which withstand malicious eavesdroppers. Different from the existing solutions, our proposal does not rely on the existence of fully trusted dealers and deals with efficient key update in CMIX for the first time. In our protocol, any vehicle in a CMIX could be a group secret key distributor. Knowing the group encryption key, any entity can encrypt to the group members so that only the members can decrypt. Furthermore, once the group secret key of the CMIX has to be updated, a vehicle in the CMIX just needs to broadcast a short cipher text and than all the vehicles in the CMIX may refresh the group secret key to the new one efficiently. The proposed protocol is shown to be secure under the k-bilinear Diffie-Hellman exponent assumption.

Index terms: *Vehicular ad hoc networks, Communication security, Asymmetric group key agreement, Cryptographic mix-zones, Diffie-Hellman algorithm.*

1:INTRODUCTION

1.1:OVERVIEW OF THE PROJECT

Vehicular Ad-Hoc Network is the network in which communication has been done in between road side units to cars, car to car in a short range of 100 to 300 m. They are receiving increasing attentions from academia and deployment efforts from industry, due to the various applications and potential tremendous benefits they offer for future VANET users. Safety information exchange enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging and plays a key role in VANET applications. In a VANET, vehicles will rely on the integrity of received data for deciding when to present alerts to drivers. The communication between car to car, car to roadside unit done through wireless communication. That is why security is an important concern area for vehicular network application. For authentication purpose so many bandwidth is consumed and the performance becomes low.

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.

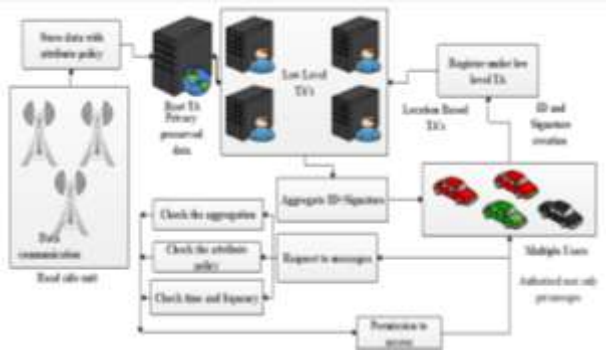

Fig:-System Architecture

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.

1.2:VANET

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.

1.3: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:

a) 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.

b) 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.

c) 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.

d) 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.
e) Cooperative Collision Warning: Alerts two drivers potentially under crash route so that they can mend their ways.
f) Traffic Vigilance: The cameras can be installed at the RSU that can work as input and act as the latest tool in low or zero tolerance campaign against driving offenses.

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:
a) Remote Vehicle Personalization/ Diagnostics: It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure.
b) Internet Access: Vehicles can access internet through RSU if RSU is working as a router.
c) 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.
d) 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.

e) 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:

a) Route Diversions: Route and trip planning can be made in case of road congestions.

b) 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.

c) Parking Availability: Notifications regarding the availability of parking in the metropolitan cities helps to find the availability of slots in parking lots in a certain geographical area.

2: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 on anonymous certificates. The fourth category is about the IBV protocol which is based on an ideal tamper-proof device (TPD) (i.e., a device from which no attacker can ever extract any stored data) using a variant of IBC. It requires the master secret of TA to be stored in a TPD. This approach can avoid certificate management and achieve un linkable privacy. The final category is about the APPA protocol which is built on a one-time identity-based aggregate signature (OTIBAS) and the multiplicative secret sharing (MSS) technique and, also requires the master secret (shares) of TA to be stored in a TPD. MSS is used to achieve leakage resiliency (ie) that the scheme remains secure in the presence of bounded information leakage of the master secret stored in the TPDs.

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.
- The attacker may collect substantial information through side-channel attacks.
- Once the master secret is extracted, the attackers can fully control the entire VANET.

4: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. These messages will be sent to the Root TA using the optimal RSU. The optimal RSU will be identified using Genetic Algorithm. 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 verification message from the Root TA. The signature is only valid under the user's identity and the public information of the Root 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.

4:NETWORK SIMULATOR 2

NS2 is an open-source simulation tool that runs on Linux. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired and wireless (local and satellite) networks. It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms. Queuing algorithms include fair queuing, deficit round-robin and FIFO.

NS2 started as a variant of the REAL network simulator in 1989 (see Resources). REAL is a network simulator originally intended for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks. Currently NS2 development by VINT group is supported through Defense Advanced Research Projects Agency (DARPA) with SAMAN and through NSF with CONSER, both in collaboration with other researchers including ACIRI. NS2 is available on several platforms such as FreeBSD, Linux, SunOS and Solaris. NS2 also builds and runs under Windows.

Simple scenarios should run on any reasonable machine; however, very large scenarios benefit from large amounts of memory. Additionally, NS2 requires any one of the following packages to run: TCL release 8.3.2, OTCL release 1.0a7 and TCL release 1.0b11.

TOOL COMMAND LANGUAGE

TCL is Tool command language. TCL is developed initially for Unix. It is then ported to Windows, DOS, OS/2, and Mac OSX. TCL is much similar to other unix shell languages like Bourne Shell (Sh), the C Shell (csh), the Korn Shell (sh), and Perl. It aims at providing ability for programs to interact with other programs and also for acting as an embeddable interpreter. Even though, the original aim is to enable programs to interact, full-fledged applications are written in TCL. Commands are the most vital part of this language. TCL commands are

built in-to the language with each having its own predefined function.

FEATURES OF TCL

The features of TCL are:

- Reduced development time.
- Powerful and simple user interface kit with integration of TK.
- Write once, run anywhere. It runs on Windows, Mac OS X, and almost on every UNIX platform.
- You can easily extend existing applications with TCL. Also, it is possible to include TCL in C, C++, or Java to Tcl or vice versa.
- Has a powerful set of networking functions.

APPLICATIONS

- The applications of TCL are:
- Scalable websites that are often backed by databases.
- High performance web servers build with TclHttpd.
- TCLwith CGI based websites.
- Desktop GUI applications.
- Embedded applications.

5:MODULES

- Network Formation
- Communication among nodes and RSU
- Issue of Digital Signature
- Verification of Digital Signature
- Fitness function for RSU
- Performance Evaluation

5.1:MODULE DESCRIPTION

- **Network Formation**

Explains how the network is formed using the Nodes, Road Side Units (RSU), Low Level TA and TA.

- **Communication among nodes and RSU**
    - Each vehicle communicates with unknown and unspecified vehicles neighbouring on the road.
    - Single Hop & Multi Hop Communication is explained.

- **Issue of Digital Certificate**
    - A vehicle should register with the location and name
    - These data will be communicated to the TA.
    - Trust Authority issues a digital certificate
- **Verification of Digital Certificate**
    - The vehicle have to send the digital certificate to the TA for verification.

  If the verification process is successful, the vehicle can communicate with other vehicles in the network
- **Fitness function for RSU**
    - Find the optimal path from source to destination vehicles
    - Find the fitness value of each RSU.
    - Choose the optimal RSU using the fitness function.
- **Performance Evaluation**
    - Performance factors are evaluated.
    - Implemented using NS 2 and the graphs are obtained.

6:CONCLUSION

In this paper, we propose a novel method to establish CMIXes which withstand malicious eavesdroppers. Our CMIX protocol is realized by using our new security tool called OTIBAAGKA. Compared with the existing CMIX protocols, our protocol does not rely on the existence of fully trusted dealers, and enables efficient group secret key update. Any vehicle in a CMIX may distribute a (new) group secret key to all the vehicles in the CMIX efficiently. The efficiency of our CMIX protocol are confirmed by detailed simulations. Attribute based encryption scheme is used in this protocol. Handle large number of messages.

References:

[1] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: an effective strategy for location privacy in VANETs," IEEE Trans. Veh. Technology, vol. 61, no. 1, pp. 86–96, 2012

[2] M. Jadliwala, I. Bilogrevic, and J. Hubaux, "Optimizing mix-zone coverage in pervasive wireless networks," J. Comput. Secur., vol. 21, no. 3, pp. 317–346, 2013.

[3] B. Palanisamy, and L. Liu, "Attack-resilient mix-zones over road networks: architecture and algorithms" IEEE Trans. Mobile Computing, vol. 14, no. 3, pp. 495–508, 2015.
[4] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, Privacy preserving vehicular communication authentication with hierarchical aggregation and fast response, IEEE Trans. Comput., vol. 65, no. 8, pp. 2562–2574, 2016.
[5] J. Li, L. Zhang, "Sender dynamic, non-repudiable, privacy preserving and strong secure group communication protocol", Inform. Sciences, vol. 414, pp. 187–202, 2017.
[6] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), 2012, pp. 972– 980.
[7] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569–1589, 2007.
[8] A. Fiat, and M. Naor, "Broadcast encryption," in Proc. 13th Annu. Int. Cryptology Conf. (CRYPTO), 1993, pp. 480–491.
[9] M. Naor, and B. Pinkas, "Efficient trace and revoke schemes," in Proc. 4th Int. Conf. Financial Cryptography (FC), 2000, pp. 1–20. [10] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer, "Asymmetric group key agreement," in Proc. 28th Annu. Int. Conf. Theory Applicat. Cryptographic Technol. (EUROCRYPT), 2009, pp. 153–170. [30] L.