Accelerate TESLA Protocol for VANETs

# **K.Madhurima** [1], M.Tech, Computer Science Engineering, madhurimakotte@gmail.com
# P.Kalyani [2] Sr. Asst. Professor, Department of CSE, kalyanip07@gmail.com
TallaPadmavathi Engineering College, Warangal, Telangana, India

Abstract: ***Efficient and easy-to-manage security and privacy-enhancing mechanisms are essential for the wide-spread adoption of the VANET technology. In this paper, we are concerned with this problem: EMAP (Expedite Message Authentication Protocol) responsible for distributing secret keys to all OBUs in the network. This paper introduced TESLA (Timed Efficient Stream Loss-Tolerant Authentication) is used as an authentication method for distributing secret keys to all OBUs in multicast and broadcast network communications with minimum delay. TESLA uses symmetric cryptography with delayed key disclosure to prove that the sender was the authenticated source of the message. TESLA++ offers a more secure User Authentication mechanism than TESLA. TESLA++ is an efficient means of Information Broadcasting in case of very high computational load.***

Keywords: Vehicular Ad Hoc Networks, Expedite Message Authentication Protocol, symmetric cryptography, Timed Efficient Stream Loss-Tolerant Authentication.

1. Introduction

` Vehicular Ad hoc Network (VANET), is generalized from mobile ad hoc networks (MANETs), is a promising approach for the intelligent transportation system (ITS). The original motive behind vehicular communication was safety on roads, because million of lives were lost and much more injuries have been incurred due to car crashes. Safety messages which are of highest priority need to be delivered to the destination node on time to prevent from accidents. VANET have wide applications in Automobile Industry including Intelligent Transportation System (ITS) to avoid collision and route vehicles efficiently to improve safety. VANET includes vehicle to vehicle (V2V) communication and vehicle to road side communication. The broadcast storm problem seriously affects the successful rate of message delivery in VANETs. The key challenge is to overcome these problems to provide routing protocols with the low communication delay, the low communication overhead, and the low time complexity.

Vehicular ad hoc networks (VANETs) aim at enhancing safety and efficiency in transportation systems. They comprise network nodes, that is, vehicles and road-side infrastructure units (RSUs), equipped with on-board sensory, processing, and wireless communication modules. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication can enable a range of applications. Among these, primarily safety will be enabled, as numerous research and development initiatives indicate, by vehicles frequently *beaconing* their position, along with warnings on their condition or environment. Nonetheless, VANETs can be vulnerable to attacks and jeopardize users' privacy. For example, an attacker could inject beacons with false information, or collect vehicles' messages, track their locations, and infer sensitive user data.

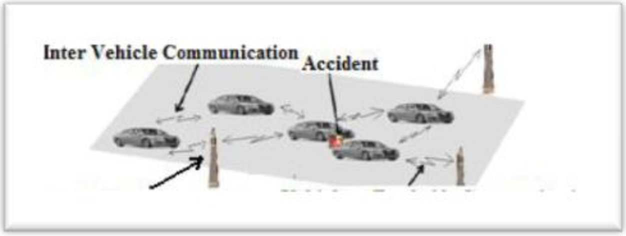

Figure1. Communication in VANET systems.

In VANETs, a vehicle's *On Board Unit (OBU)* communicates with other vehicles' OBUs and fixed infrastructure called *Road Side Units (RSUs)*. For VANETs to operate securely and reliably, participants needs to validate received messages; otherwise, an attacker can easily inject bogus messages to disrupt the normal operation of VANETs. To allow authentication, we need to build key management mechanisms that allow senders to establish and update keys for security-sensitive operations.

2. RELATED WORK

User Authentication can be confirmed by a number of protocols and algorithms. Practically, we use a combination of these protocols as they have higher efficiency as compared to individual protocols. We discuss here a few of them that are considered most efficient and thus, used widely.

In VANETs, the primary security requirements are identified as entity authentication, message integrity, nonrepudiation, and privacy preservation. The PKI (Public Key Infrastructure) is the most viable technique to achieve these security requirements.

PKI employs CRLs to efficiently manage the revoked certificates. Since the CRL size is expected to be very large, the delay of checking the revocation status of a certificate included in a received message is expected to be long.

In VANETs, a vehicle's *On Board Unit (OBU)* communicates with other vehicles' OBUs and fixed infrastructure called *Road Side Units (RSUs)*. For VANETs to operate securely and reliably, participants needs to validate received messages; otherwise, an attacker can easily inject bogus messages to disrupt the normal operation of VANETs. To allow authentication, we need to build key management mechanisms that allow senders to establish and update keys for security-sensitive operations. While RSUs can utilize traditional Public Key Infrastructure approaches, designing an OBU key management mechanism for secure VANET operation turns out to be a surprisingly intricate and challenging endeavor, because of multiple seemingly conflicting requirements.

The user ensures the integrity of the message by signing the encoded message using *Digital Signatures*. This ensures the reliability of the message. The trustworthiness of the message can be increased by Certificate Authorities (CA) who will digitally sign the data and binds the public keys with private keys effectively to ensure User Authentication. In other words, CA issues certificates to the vehicles which mark the validity of the users.

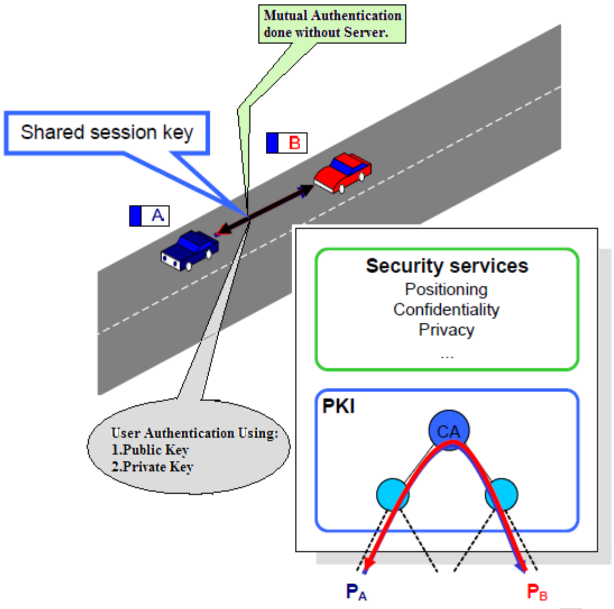

Figure 2. User Authentication using PKI.

3. Authentication method TESLA

TESLA is an acronym for „Timed Efficient Stream Loss-Tolerant Authentication‟. It is used as an authentication method for multicast and broadcast network communications. In VANET systems, PKI is not the only option to confirm User Authentication. There is a completely different technique called TESLA which provides an efficient alternative to signatures.

Instead of using Asymmetric Cryptography, TESLA uses symmetric cryptography with delayed key disclosure (which provides the necessary element of „asymmetry) to prove that the sender was the authenticated source of the message. In other words, we can describe TESLA as a lightweight broadcast authentication mechanism. TESLA performs broadcast authentication mechanism in the same manner and applies the same approach that is applied in the unicast authentication mechanism. This proves to be a more efficient way of broadcasting messages. TESLA is compliant to computational Delay of Service (DoS) attacks because symmetric cryptography is significantly faster than signatures and thus delay is avoided. In spite of these versatilities, TESLA is susceptible to attacks arising due to memory-based Denial of Service.

In TESLA, the information send by the source is stored at the receiver's end until the corresponding key is disclosed. Malicious attackers can deluge receivers with a huge collection of invalid messages which never have a corresponding key. This leads to a situation referred as "pollution attack". In "pollution attack", the attacker continuously fills receiver's memory with the junk data that affects the system's performance. With large amount of junk data, Performance of the system deteriorates.

The system can even crash if the amount of junk exceeds the maximum workload the system can successfully sustain. TESLA uses symmetric key cryptography for broadcast authentication. TESLA depends completely on time to provide the necessary asymmetry in the authentication scheme, allowing only the sender to generate a broadcast authentication at a given point of time. Though symmetric cryptography significantly reduces computation, but still it fails to prevent the occurrence of repudiation.

TESLA is used in VANET system to reduce the overhead associated with user authentication. But TESLA is vulnerable to storage based Denial of Service attacks. This becomes the basis for the development of TESLA++.

3.1 TESLA++

TESLA++ is a more efficient and advanced form of Timed Efficient Stream Loss-Tolerant Authentication (TESLA). TESLA++ is functionally more efficient and more secure than TESLA. TESLA++ has the following advantages over TESLA:

(i)TESLA++ prevents occurrence of memory based Denial of Service (DoS) attacks which are prevalent in TESLA.

(ii) TESLA++ reduces the memory requirements at receiver's end without affecting the efficiency of its broadcast authentication mechanism.

(iii) TESLA++ not only prevents the memory based Denial of Service (DoS) attacks but also the computation-based Denial of Service (DoS) attacks with equal priority.

(iv) TESLA++ makes use of those cryptographic techniques which are easier to manage and control than the techniques used in TESLA.

(v) TESLA++ offers a more secure User Authentication mechanism than TESLA.

(vi) TESLA++ is an efficient means of Information Broadcasting in case of very high computational load.

TESLA++ is similar to TESLA in functioning. The mechanism for broadcast authentication in TESLA++, just like in TESLA, uses symmetric cryptography and delayed key disclosure. TESLA++ offers reduced memory requirements at receiver's end as the receiver need not to store all the Message Authentication Codes but only the self generated ones. In TESLA++ Message Authentication Codes are broadcasted earlier than the message and the corresponding keys.

4. Security Model

There are certain requirements for authentication in VANET's, which provide secure and authenticated vehicular communication using TESLA.

1. Computation overhead: the amount of cryptographic operations a node has to compute for an authentication request in CPU time, for example, the time needed for verifying a digital signature.

2. Control overhead the bandwidth overhead (in bytes per second) for an authentication request, for example, exchanging cipher keys or certificates.

3. Latency: the time needed to respond to an authentication request.

4. Initialization time: the time needed to initialize the authentication system, for example, setting up a certificate authority and key distribution.

5. Strong authentication: Authentication in VANET's should be strong.

6. Scalable: Authentication should be scalable.

7. Support for re-authentication and revocation procedures.

The complete procedure of authenticating the validity of user in TESLA++ has been concisely provides an extensive explanation of the steps followed in TESLA++ to authenticate a user. They also provide an effective mechanism for memory management during flooding by any malicious user. Their paper proposes to discard irrelevant MACs to free the memory in case of flooding. The following steps are to be followed to discard irrelevant MACs:

(i) Discard all MACs whose key indices are older than the last authentic message received from that sender.

(ii)Discard the message whose verification is oldest in the future.

This scheme discards messages on the basis that either the older MACs were stored because a malicious user injected those messages or the message and the corresponding disclosed key were lost or the attacker made the receiver store the messages for a long duration.

5. COMMUNICATION OUTLINE

Communications are possible in homogenous and heterogeneous vehicle network without being need to change in underline technology in TESLA. For that we have specify three types of pattern in which vehicles sharing same geographic or different can communicate with each other smoothly. We can classified this patterns based on local and global communication.

There are two types of patterns depend on localization: -

1. Vehicle to Vehicle (V2V)

A. Motivation: - When an emergency is occurred, each vehicle transmit emergency message using V2Vpattern to warn other vehicle in the roadway.

B. Way of communication: - This pattern involves communication between vehicles to vehicles.

2. Vehicle to Local Server (Road Side Server):

A. Motivation: - This is only type of communication pattern that involve sending of periodic, information and emergency message. When an unusual situation happen in roadway, this pattern is used by vehicle to send emergency message to other vehicles and local server. Local server will send information message to inform this scenario to other vehicles on road. On other hand, local server will periodically inform each vehicle about nearest hospital, petrol pump, police station and other necessary information by using periodic message.

B. Way of communication: - This pattern involves communication between vehicles to local server and local server to vehicles.

There are only one type of pattern belong to global communication.

3. Local Server to Main Server

A. Motivation: - This communication pattern used in different cases.

Case 1: When vehicle was register on their local network. Local network circulate this information to global server via several local server.

Case 2: When there is any unusual any situation occurred in road way, it is responsibility of local server to give this information to global server. These types of information need in post investigation of accident.

Case 3: To maintain log records of every vehicle, this communication pattern play very important role.

B. Way of communication: - This pattern involves bidirectional communication between road side server and main server.

6. CONCLUSION

The authentication system for VANET communication results in smooth Vehicular Ad Hoc Networks for data exchange. We believe it is worthwhile to consider the potential threat associated with an increased reliance on wireless communication for the smooth flow of traffic using TELSA authentication protocol. It solved the problems of distributing secret keys to all OBUs in multicast and broadcast network communications with minimum delay. This makes local communication very efficient and reliable. On the other hand, if a message is identified as an abuse of the VANET, authorities can trace the certificate request back to the signer. The authorities can revoke the misbehaving OBU so that it is no longer able to participate in the VANET. Also message integrity and confidentiality is ensured thereby enhancing the security efficiently.

7. REFERENCES

[1] Chae Duk Jung, Chul Sur, Yougho Park and Kyung-Hyune Rhee. A Robust Conditional Privacy-Preserving Authentication Protocol in VANET. In the 1st International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec 2009), 2009.

[2] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007.

[3] R. Lu, X. Lin and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks", in *Proc. IEEE INFOCOM*, San Diego, California, 2010.

[4] J.P. Hubaux, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.

[5] Mohamed Kafsi, Panos Papadimitratos , Olivier Dousse , Lausanne, "VANET Connectivity Analysis" Switzerland Nokia Research Center, Lausanne, Switzerland T-Labs, Berlin, Germany

[6]Ghassan M. T.,"Current Trends in Vehicular Ad Hoc Networks" AbdallaUniversity of Plymouth School of Computing, Communications & Electronics, UK France Telecom Recherche et Développement CORE, France

[7] Neha Verma, Rakesh Kumar, "Efficient Data Delivery For Secured Communication in Vanet" IOSR Journal of Computer Engineering

[8] P. Salvo, F. Cuomo, A. Baiocchi "Infotainment applications support in VANET" DIET Department - University of Roma, Via Eudossiana 18, 00184
Roma, Italy

[9]Sriram Chellappan and Vamsi Paruchuri,"Integrating Smart Cards with Vehicular Networks: Architecture and Applications"

[10] Emad Eddin A. Gamati, Evitm Peytchev, Richard Germon, Li, Yueyue "Utilization of Broadcast Methods for detection of the road conditions in VANET" Nottingham Trent University - School of Science and Technology - Computing and

Informatics Building, Clifton Lane, Nottingham, NG11 8NS, UK.

[11] Andreas Festag, Alban Hessler, Roberto Baldessari,Long Le, Wenhui Zhang, “Vehicle-to-Vehicle and road-side sensor communication for enhanced road safety”.