A Survey on the Authentication Protocols in Vanet

K.Susitra[1],S.Lakshmi Narasimman[2],Cuddalore, INDIA

Abstract—**Security issue is an essential factor mainly required in the transport system. The vanet data transfer mainly involves the messages used to communicate between the vehicles as signals. This is to be provided with the authentication to improve the efficiency in the transport system communication. Here we are to provide the various algorithms used in the vanet and their features.**

Index Terms— **vanet authentication, security, attacks.**

I. INTRODUCTION

Security is an essential one because approximately about 1.3 million people are killed every year due to road accidents. Vehicular ad-hoc networks (VANETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are the two basic communication modes, which respectively allow OBUs to communicate with each other and with the infrastructure RSUs. Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the disseminated messages can be easily launched. A security attack on VANETs can have severe harmful or fatal consequences to legitimate users[1]. Privacy is an important issue in VANETs as the wireless communication channel is a shared medium. Exchanging messages without any security shield over the air can easily leak the information that users may want to keep confidential. Pseudonym based schemes [2]–[4] have been proposed to preserve the locality privacy of vehicles evertheless, those schemes need the vehicles to store a large number of pseudonyms and certification and also they do not sustain some important secure functionality such as authentication and integrity.

To the best of our knowledge, all of the existing group signature schemes in VANETs are based on centralized key management which preloads keys to vehicles off-line. The disadvantages of the centralized key management are that: the system maintenance is not flexible and that many existing schemes assume a tamper-proof device being installed in each vehicle. This tamper-proof device normally costs several thousand dollars as in [9] that uses IBM 4764card. The framework to be developed in this paper does not require the exclusive tamper-proof device.

According to the Dedicated Short Range Communication (DSRC) [5] that is part of the WAVE standard every OBU has to broadcast a message every 300 msec about its information. In this case, each OBU may receive a large number of messages every 300 msec. And also it has to check the current CRL for all the received certificates that may acquire long authentication delay depending on the CRL size and the number of received certificates. It is an inevitable challenge for VANETs ability to check a CRL for a large number of certificates in a timely manner.

Most of the existing works overlooked the authentication delay resulting from checking the CRL for each received certificate. Each OBU should be able to check the revocation status of all the received certificates in a timely manner in order to ensure reliable operation of VANETs and increase the amount of authentic information gained from the received messages. An expedite message authentication protocol 1 (EMAP) which replaces the CRL checking process by an efficient revocation checking process using a fast and secure HMAC function is introduced here. EMAP is suitable not only for VANETs but also for any network employing a PKI system. This is the first solution to reduce the authentication delay resulting from checking the CRL in VANETs.

Attacks in the VANET

To get better protection from attackers we must have the knowledge about the attacks in VANET against security requirements. Attacks on different security requirement are given below [6]:

• **Impersonate:** In impersonate attack attacker assumes the identity and privileges of an authorized node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network.This type of attack is performed by active attackers. They may be insider or outsiders. This attack is multilayer attack means attacker can exploit either network layer, application layer or transport layer vulnerability.

• **Identity revealing**: Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.

• **Location Tracking**: The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.

• **Repudiation:** The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.

• **Eavesdropping** is a most common attack on confidentiality. This attack is belongs to network layer attack and passive in nature. The main goal of this attack is to get access of confidential data.

• **Denial of Service:** DoS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node.

II. TELSA PROTOCOL FOR AUTHENTICATION TESLA

is an acronym for „Timed Efficient Stream Loss-Tolerant Authentication‟[8]. 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.

III. EMAP PROTOCOL WITH Tack

A Trusted Authority responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. The Roadside units (RSUs) that are fixed units are distributed all over the network. RSUs can communicate securely with the TA and OBUs are embedded in vehicles. All the OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.

Each of these algorithms is performed one after another as the order is described doing specific functions at every stage. The entire EMAP working can be divided in to three main processes[7].

- System Initialization
- Message Authentication
- Revocation

System Initialization

The system model under consideration is mainly a PKI system in which each OBUs has a set of anonymous certificates (CERTu) used to secure its communications with other entities in the network. In specific PKu, included in the certificate certu and the secret key S Ku are used for verifying and signing messages. Each OBUs is preloaded with a set of a symmetric keys (secret keys in RSu and the corresponding public keys in RPu). The keys are necessary for generating and maintaining a shared secret key Kg between unrevoked OBUs.

Message Authentication:

The details of the TA signature on a certificate and an OBU signature on a message are not discussed in this paper for the sake of generality since we adopt a generic PKI system. We only focus in how to accelerate the revocation checking process that is conventionally performed by checking the CRL for every received certificate. Then the message signing and verification between different entities in the network are performed.

Authentication is performed by the two following steps:

- Message signing
- Message Verification

Revocation

An important feature of the proposed EMAP is that it enables an OBU to update its compromised keys corresponding to previously missed revocation processes provided that it picks one revocation process in the future. A rekeying mechanism capable of updating compromised keys corresponding to rekeying processes previously missed is introduced. Revocation process consists of 3 algorithms implemented in EMAP system model after authentication is achieved.

Performance evaluation

During simulation time the events are traced by using the trace files. The performance of the network is evaluated by executing the trace files. The events are recorded into trace files while executing record procedure. In this procedure, we trace the events like packet received, Packets lost, and delay etc. These trace values are write into the trace files. This procedure is recursively called for every 0.05 ms. so, trace values recorded for every 0.05 ms. All the graphs obtained can be used to conclude that EMAP is efficient for the VANET operations.

- Packet Receive Ratio is high
- Packet loss is low
- Delay is minimal

IV. Conclusion

Thus the survey of the algorithms used in the vanet is being given along to provide the security against the attacks caused due to various factors in the network. To overcome the attacks it is necessary toauthenticate the users of the vehicular adhoc networks
.

V. References

[1] Albert Wasef and Xuemin (Sherman) Shen" EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks" *IEEE TRANSACTIONS ON MOBILE COMPUTING VOL.12 NO.1 YEAR 2013.*

[2] A. Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks," *IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.*

[3] M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. *Computer Security, vol. 15, no. 1, pp. 39-68, 2007.*

[4] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong PrivacyPreservation for Vehicular Communications," *IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.*

[5] A. Wasef and X. Shen, "MAAC: Message Authentication AccelerationProtocol for Vehicular Ad Hoc Networks*," Proc. IEEEGlobeCom, 2009.*

[6] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", *Handbook of Research on Mobility and Computing, 2010.*

[7] R. Priya, Dr. C. Kumar Charlie Paul" PERFORMANCE ANALYSIS OF AN EXPEDITE MESSAGE AUTHENTICATION PROTOCOL FOR VANETS" *International Journal For Technological Research In Engineering Volume 1, Issue 5, January – 2014*

[8] K.Madhurima, P.Kalyani," Accelerate TESLA Protocol for VANETs*" International Journal of Research and Computational Technology, Vol.6 Issue.2September, 2014*