International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 8 (August '2016)

MESSAGE AUTHENTICATION PROCESS IN VANET DATA COMMUNICATION

K.S.Saravanan,
Assistant Professor,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Science College for Women, (Autonomous),
Elayampalayam, Namakkal, Tamilnadu

N.Boomathi,
M.Phil Scholar,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Science College for Women,(Autonomous),
Elayampalayam, Namakkal, Tamilnadu

Abstract: Vehicular Ad-hoc Networks (VANET) are constructed to manage the communication between the vehicles. Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication methods are supported under the VANET environment. In cryptography, a message authentication code (MAC) is a short piece of information used to authenticate a message—in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed in transit (its integrity).On Board Unit and Road Side Infrastructure (RSI) are used to carry out the communication process. In vehicular networks, broadcast communications are critically important, as many safety-related applications rely on single-hop beacon messages broadcast to neighbor vehicles. However, it becomes a challenging problem to design a broadcast authentication scheme for secure vehicle-to-vehicle communications. Especially when a large number of beacons arrive in a short time, vehicles are vulnerable to computation-based Denial of Service (DoS) attacks that excessive signature verification exhausts their computational resources.

Keywords: Vehicular Ad-hoc Networks, Message Authentication code, Denial of Service

I.INTRODUCTION

VANETs are a subset of mobile ad hoc networks composed of network-equipped vehicles and infrastructure points, which will allow vehicles to communicate with other vehicles and with roadside infrastructure points. A Trusted Authority, which is responsible for providing anonymous certificates and distributing secret keys to all OBUs in the network. So that communication overheads and consumes delay in message authentication[1]. Vehicular ad hoc network (VANET) can offer various services and benefits to users and thus deserves deployment effort. Attacking and misusing such network could cause destructive consequences. It is therefore necessary to integrate security requirements into the design of VANETs and defend VANET systems against misbehavior, in order to ensure correct and smooth operations of the network. A security system for VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, nonrepudiation, message integrity, and confidentiality.

Moreover, a privacy-preserving defense technique for network authorities to handle misbehavior in VANET access, considering the challenge that privacy provides avenue for misbehavior. The system employs an identity-based cryptosystem where certificates are not needed for authentication. We show the fulfillment and feasibility of our system with respect to the security goals and efficiency. Prediction Based Authentication (PBA) scheme is an efficient broadcast authentication scheme [2]. The authentication scheme handles computation-based DoS attacks and also resists packet losses caused by high mobility of vehicles. PBA is an efficient and lightweight scheme since it is primarily built on symmetric cryptography. PBA is designed to exploit the sender vehicle's ability to predict future beacons in advance to further reduce the verification delay for some emergency applications. In addition, to prevent memory-based DoS attacks, PBA only stores shortened re-keyed Message Authentication Codes (MACs) of signatures without decreasing security.

II. PROBLEM STATEMENT

To secure vehicular networks, an authentication scheme is indispensable to ensure messages are sent by legitimate vehicles and not altered during transmissions. Otherwise, an attacker can easily disrupt the normal function of VANETs by injecting bogus messages. Therefore, vehicles should broadcast each message with a digital signature. Therefore, vehicles should broadcast each message with a digital signature.

However, the current VANET signature standard using Elliptic Curve Digital Signature Algorithm (ECDSA) would cause high computational overhead on the standard OBU hardware, which has limited resources for cost constraints. Prior work has shown that one ECDSA signature verification requires 20 milliseconds on a typical OBU with a 400 MHz processor. When a large number of signed messages are received in a short time period, an OBU cannot process them before their dedicated deadline.

III. RELETED WORK

1.Flooding-Resilient Broadcast Authentication for VANETs

In this work, we observe that signature flooding can be mitigated by broadcast authentication schemes whose

overheads match the *entropy* of the broadcast messages [2]. We study this approach in the context of VANETs and propose two flooding-resilient broadcast authentication schemes, FastAuth and SelAuth, for different VANET applications. Our schemes are based on digital signatures thus providing non-repudiation. To the best of our knowledge, prior work on lightweight broadcast authentication either lacks the non-repudiation property or fails to operate efficiently in dynamic VANET environments. We briefly summarize our schemes.

2.ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks

To tackle the aforementioned problems, including security, efficiency, and scalability problems, we proposed an anonymous batch authentication and key agreement (ABAKA) scheme to build a secure environment for value-added services in VANETs [3]. To avoid bottleneck problems, ABAKA is inspired by the concept of batch verification to simultaneously authenticate multiple requests sent from different vehicles using elliptic curve cryptography (ECC), which is adopted by the Trial-Use standard. Meanwhile, multiple session keys for different vehicles can also be negotiated at the same time. To the best of our knowledge, this is the first study that provides batch authenticated and key agreements for value added applications in VANETs

3. Reconstruction of a Secure Authentication Scheme for Vehicular Ad Hoc Networks Using a Binary Authentication Tree

This necessitates and urges the development of a functional, reliable and efficient security architecture before all other implementation aspects of VANETs. Fundamentally, VANET security design should guarantee source authentication and message integrity. Besides these security requirements, sensitive information such as identities and location privacy should be preserved from the vehicle owner's perspective against unlawful tracing and user profiling. In contrast, traceability is required where the identity information needs to be revealed by law enforcement authorities for liability issues in the event of an accident or crimes[4]. Thus, privacy must be preserved and conditional. To ensure both source authentication and message integrity in VANETs, one appealing solution is to sign each message with a digital signature before the message is sent.

4. Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks

One fundamental security problem in VANETs is message authentication. Achieving message authentication consists of two essential security checks, i.e., an integrity check and identification check. Message authentication must be implemented to allow vehicle users to differentiate reliable information from bogus information and to resist modification attacks and impersonation attacks [5]. An appealing solution to this problem in VANETs is to digitally sign messages before sending them; not only does this allow the receiver to identify the sender, but the signature also prevents the message contents from being modified in transit. Several schemes have been proposed in the literature and can be mainly divided into the following two categories: traditional public-key-infrastructure (PKI)-based digital signature schemes and group signature-based security schemes. In both categories, each message needs to be signed by the sender using an asymmetric algorithm, and its receiver needs to verify the message that is received. Both of these schemes can effectively ensure secure communication while simultaneously protecting user privacy, but traditional PKI-based schemes may fail to satisfy the stringent time requirements of vehicular communication applications. Particularly as the traffic density increases, a vehicle may become unable to verify the authenticity of the messages sent by its neighbors in a timely manner, which results in message loss and, in turn, an increased risk to public safety.

5. An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks

Fundamentally, VANET security design should guarantee authentication, nonrepudiation, integrity, and in some specific application scenarios, confidentiality, to protect the network against attackers. Besides the fundamental security requirements, sensitive information such as identity and location privacy should be preserved from the vehicle owner's perspective, against unlawful tracing and user profiling, since otherwise it is difficult to attract vehicles to join the network [6]. On the contrary, traceability is required where the identity information need be revealed by law enforcement authorities for liability issues, once accidents or crimes occur. In addition, privilege revocation is required by network authorities once misbehavior is detected during network access. It is less difficult to prevent misbehavior of unauthorized users since legitimate users and roadside units (RSUs) can simply disregard communication requests from outsiders by means of authentication.

IV.PROPOSED WORK

A)The Prediction-based Authentication Scheme

This section presents PBA, which makes use of both ECDSA signatures and TESLA-based scheme to authenticate beacons. Similar to the TESLA scheme, PBA also requires loose time synchronization. In VANETs, it is naturally, supported since messages sent by GPSequipped vehicles are timestamped with nanosecond level accuracy. By looking into beacons, we find that the information in a beacon except a vehicle's position is almost deterministic based on its previous beacons. As also mentioned the entropy of beacons is relatively low from the sender vehicle's point of view. Given the past trajectory, a vehicle's future position can be predicted as the vehicle's movement is mainly restricted by the road topology and speed limit. We mainly use this fact to construct our PBA scheme. We will next describe how it authenticates beacons.

Protocol Overview: Our PBA includes the process of generating a signature by a sender and verifying the signature by a receiver. We introduce them separately. First, each vehicle splits its timeline into a sequence of time frames. Each time frame is also divided into a sequence of beacon intervals, which we remark I_0, I_1, ….,I_n. In a time frame, to send the first beacon B_0 for I_0, a vehicle will

perform four steps: chained keys generation, position prediction, Merkle hash tree construction, and signature generation.

To send other beacons in that time frame, the vehicle only operates the last three steps.

1)Chained Keys Generation: At the beginning of a time frame, each vehicle generates n chained private keys for the next n beacons. It uses one interval worth of private key for authentication as the TESLA scheme. In the following description, we call these private keys TESLA keys.

2)Position Prediction: At each beacon interval, each vehicle predicts its position broadcast in the next beacon. To do so, vehicles model all the possible results of movements between two consecutive beacons based on information of the past trajectory, as shown in Fig. 1(a).

3)Merkle Hash Tree Construction: After position prediction, the vehicle will construct one interval worth of a public key and private keys. These private keys are associated with the results of movements. We propose a MHT, which ties these pre-computed keys together and then generates a single public key or prediction outcome for all the possible movements. As illustrated in Fig. 1(b), Rooti is the prediction outcome for all the results of movements from I_{i-1} to I_i.

4)Signature Generation: After position prediction and MHT construction, a vehicle signs the commitment of the hash chain and the prediction outcome from MHT using ECDSA signatures, and broadcasts it along with the first beacon B_0 in the time frame. For the rest of beacons such as B_1,B_2, …B_n, the vehicle signs the message and the prediction outcome from MHT using the TESLA keys assigned in the intervals I_1, I_2,…., I_n (shown in Figure 1). After receiving a beacon, a vehicle will perform the following two steps:

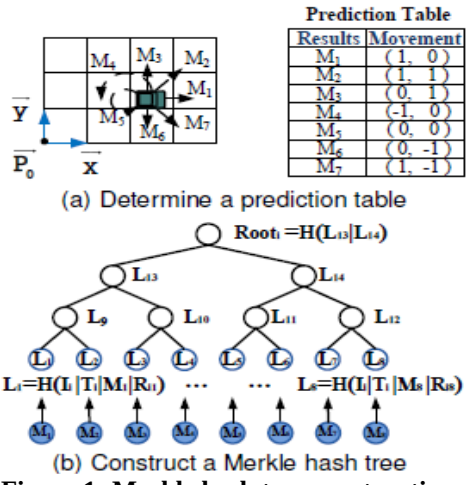

Figure 1: Merkle hash tree construction

Each leaf node in a tree corresponds to one entry in the prediction table, and the inner node is the hash of the two children.

1) **Self-Generated MAC Storage:** To reduce the storage cost of unverified signatures, the receiver only records a shortened re-keyed MAC. When the receiver keeps the used key secret, PBA provides security guarantees according to the size of beacon interval and network bandwidth.

2) **Signature Verification:** For the first beacon, the receiver verifies the ECDSA signature. To verify the following signed B_i, the receiver will get the corresponding TESLA key, and reconstruct the prediction outcome from MHT (shown in Fig. 2). If a matching MAC of prediction outcome is found in the memory, the receiver authenticates the beacon instantly. Otherwise, the receiver authenticates it with the later TESLA key.

B) Chained Keys Generation

Before sending any beacon, a vehicle first generates chained keys for signing and a commitment K0 like the TESLA scheme, as shown in Fig. 2. As we mentioned before, the drawback of the TESLA scheme is that the receiver needs to buffer packets some intervals before it can authenticate them. This might not be practical for certain single-hop relevant applications where timing is usually critical. We modify the basic TESLA scheme to support instant authentication, which allows the receiver to verify packets as soon as they arrive.

In our TESLA-based scheme, the sender predicts the next interval's message m_{i+1} in the interval Ii, and gets the prediction outcome $Root_{i+1}$. To construct the beacon packet B_i, the sender picks the TESLA key K_i for Ii, and appends the MAC over mi and $Root_{i+1}$ with K_i'. Here, the notion j stands for message concatenation. We now briefly present how our TESLA-based scheme works. In Fig. 2, when the beacon Bi with the disclosed key K_{i+1} arrives at a receiver, it allows the receiver to verify the beacon B_{i+1} sent in interval I_{i+1}. B_{i+1} carries the prediction outcome $Root_i$ for m_i. Therefore, the message mi can be immediately verified with $Root_i$and K_{i+1}.

Dealing with packet losses. If certain previous beacon, such as B_{i+1}, is lost or dropped due to the poor quality of wireless channel, we cannot immediately authenticate the incoming beacon Bi. However, we are able to authenticate it with the original TESLA signature MACK0 I (mi), where the TESLA key K_i is disclosed in or after interval I_{i+1}.

C) Position Prediction

As position is the main source of uncertainty in beacons, we discuss how the sender vehicle predicts its own future positions. For every two consecutive beacons, such as B_{i+1} and Bi, PBA requires the sender to model all the possible results of the distance vector differences or movements between them. The output of this step is a prediction table PT_i in which each entry represents one possible movement between I_{i+1} and Ii. Inspired by the work we also use a local coordinate to express the sender's future positions. We place the origin of this local coordinate at the beginning position P_0 of the current time frame. A pair of orthogonal vectors (i.e., ~x and ~y) are also required, the scalar of which can be chosen according to a desired level of positioning accuracy. Then, every future position ~ Pi could be represented as $P_i = P_0+a_ix+b_iy$, where ai and bi are rounded to integers. Hence, the movement from the interval I_{i+1} to Ii is:

$$M_i = P_i - \sim P_{i-1} = (a_i - a_{i-1})x + (b_i + b_{i+1})y \quad (1)$$

which can be briefly given by a pair of integers (a_i, a_{i-1}, b_i, b_{i-1}).

As shown in Fig. 1(a), the prediction table PT_i collects all the possible results of M_i. Here, we are not interested in accurately modeling the mobility of a vehicle given the past

trajectory, which is orthogonal to our work. In this work, we would like to design a broadcast signature scheme working with an arbitrary prediction model.

D) Signature Generation

After generating the commitment K_0, constructing the prediction table with a local coordinate, and producing the MHT's root $Root_1$ for the next beacon B_1, the sender broadcasts the first beacon in a time frame. It contains public keys, time stamp T_0, and other important parameters (such as, its local coordinate system). We format the first beacon as $B_0 = \{m_0, S_0, C_{ert}\}$, where $m_0 = \{T_0, I_0, P_0, K_0, x, ,y, Root_1\}$ is signed by ECDSA, and a Cert is issued by a CA. For Ii, being at the position P_i and time Ti, the vehicle will locate the leaf node corresponding to P_i in the MHT, and broadcast the necessary values and off-path nodes of this leaf in m_i. We define off-path nodes are the siblings of the nodes on the path from one leaf to the root of MHT. For example, in Fig. 2, the car shows the leaf associated with the current location and time.

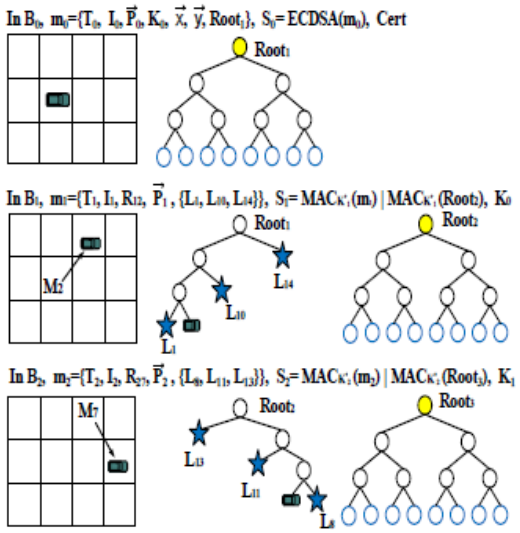

Figure 2: Signature broadcast and verification. To verify B_1 or B_2, the receiver gets the TESLA key K_0 or K_1, rebuilds the root of MHT with the information in B_1 or B_2, and then checks whether the root matches the one signed in B_0 or B_1.

At T1, the sender moves to $P_1 = P_0 + M_2$, associated with L_2. Hence, m_1 includes the random value and off-path nodes: $\{R_{12}, L_1, L_{10}, L_{14}\}$. Similarly, m_2 also includes the random value and off-path nodes for I_2. To construct the signature of mi, the sender first picks the TESLA key K_i for the interval Ii. Then, by performing the steps of position prediction and MHT construction, it obtains the root value $Root_{i+1}$ for I_{i+1}. Finally, the sender signs mi and $Root_{i+1}$ with $K_{i'}$. As shown in Fig. 2, the signature of m1 includes the TESLA signature $MAC_{K'1}$ (m_1) and $MAC_{K'1}(Root_2)$. Thus, except the first beacon, the broadcast B_i includes the message m_i, the signature Si, and the TESLA key K_{i+1} which is disclosed for receivers to verify previous beacons.

Reducing the communication overhead

As the random value and off-path nodes are contained in the message, the size of beacon is larger than before. To reduce the communication overhead, we could decrease the number of off-path nodes with Huffman hash tree instead of Merkle hash tree. Note that, if Huffman hash tree is used to reduce the communication overhead, it will take effect only when an OBU predicts its movement accurately.

The Prediction Based Authentication (PBA) scheme is enhanced to handle single hop and multi hop broadcast models. Network load analysis mechanism is integrated with the system to improve the accuracy levels. Pseudonym based anonymity management methods are integrated with the system to provide privacy features.

CONCLUSION

The Prediction Based Authentication (PBA) scheme is enhanced to handle single hop and multi hop broadcast models. Network load analysis mechanism is integrated with the system to improve the accuracy levels. Pseudonym based anonymity management methods are integrated with the system to provide privacy features. PBA performs the verification process with low storage cost, high density traffic environment and lossywireless environment.The system performsmessage verification with low storage cost under high density environment and the Attack detection system accuracy is improved in the system. The system supports single hop and multi hop broadcast models and user level privacy is supported in the system.

REFERENCE

[1]. C.SelvaLakshmi, Secured Multi Message Authentication Protocol for Vehicular Communication on International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013.

[2]. Hsu-Chun Hsiao, flooding –reailient broadcast authentication for VANETs.

[3]. Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu ChienABAKA: An Anonymous Batch Authenticatedand Key Agreement Scheme for Value-Added Services in vehicular ad hoc networks in ieee transactions on vehicular technology, vol. 60, no. 1, january 2011.

[4]. Kyung-Ah Shim Reconstruction of a Secure Authentication Scheme for Vehicular Ad Hoc NetworksUsing a Binary Authentication tree in ieee transactions on wireless communications, vol. 12, no. 11, november 2013.

[5]. Xiaodong Lin Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networksin ieee transactions on vehicular technology, vol. 62, no. 7, september 2013

[6]. Jinyuan sun-An identity-Based Security System for User Privacy in vehicular Ad Hoc Networks in IEEE transactions on parallel and distributed systems, vol.21, No 9, September 2010.

[7]. Yong Hao- A distributed key management framework with cooperative message authentication in VANETs in IEEE Journal on selected areas in communication, VOL.20, NO. 3 March 2011.