ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Implementing Efficient Prediction Based Algorithm for Vehicular Adhoc Networks

P.Sheela Rani, R.Vinston Raja

Assistant Professor, Dept of I.T, Panimalar Institute of Technology, Anna University , Chennai, India

Assistant Professor, Dept of I.T, Panimalar Institute of Technology, Anna University , Chennai, India

ABSTRACT: Broadcast communications are critically important, In vehicular networks. It becomes a challenging problem to design a broadcast authentication scheme for secure vehicular networks. 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. In this paper, we propose an efficient broadcast authentication scheme called Prediction-based Algorithm against computation-based DoS attacks, but also resist packet losses caused by high mobility of vehicles. In contrast to most existing authentication schemes, our Algorithm is an efficient and lightweight scheme since it is primarily built on symmetric cryptography. To further reduce the verification delay for some emergency applications, it is designed to exploit the sender vehicle's ability to predict future beacons in advance. In addition, this algorithm prevent memory-based DoS attacks, it only stores shortened re-keyed Message Authentication Codes (MACs) of signatures without decreasing security. We analyze the security of our scheme and simulate this Algorithm under varying vehicular network scenarios. The results demonstrate that PBA fast verifies almost 97% messages with low storage cost not only in high-density traffic environments but also in lossy wireless environments.

KEYWORDS: Broadcast communication, DoS attacks, Message Authentication Codes prediction-based algorithm, vehicular networks.

I. INTRODUCTION

In vehicular networkshas to enhancing road safety, as well as improving driving experience. By using a Dedicated Short-Range Communications (DSRC) [1] technique, vehicles equipped with wireless On-Board Units (OBUs) can communicate with other vehicles and fixed infrastructure, e.g., Road-Side Units (RSUs), located at critical points of the road [2]. Therefore, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are regarded as two basic typesof communications in VANETs. The broadcast beacons often contain information about position, current time, speed, direction, driving status, etc. For example, by frequently broadcasting and receiving beacons, drivers are better aware of obstacles and collision scenarios. They may act early to avoid any possible damage, or to assign a new route in case of a traffic accident in the existing route.

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 vehicular networks by injecting bogus messages. So vehicles should broadcast each message with a digital signature. Previous system they were [3] 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 [4]. When a large number of signed messages are received in a short time period, an OBU cannot process them before their dedicated deadline.

In this paper, we define this attack as computation-based Denial of Service (DoS) attacks. For example, when traffic related messages (beacons) are sent 10 times per second as suggested by the DSRC protocol [1], [3], a vehicle is overwhelmed with more than five neighbours within its radio range...It Furthermore, ifattackers inject false beacons,

10.15680/ijircce.2015.0302043

the receiver is hard tolocate them so that these schemes are also vulnerableto the computation-based DoS attacks [5]. Therefore,designing an effective authentication scheme underhigh-density traffic scenarios is a big challenge for vehicular networks

In this paper, we propose an effective broadcast authentication scheme: Prediction-based Algorithm (PBA) to defend against computation-based DoS attacks for vehicular networks.

Certain vehicular applications may require receivers to verify urgent messages immediately. To support instant verification, we exploit the property of predictability of a future beacon, constructing a Merkle Hash Tree (MHT) to generate a common public key or predication outcome for the beacon. With the prediction outcome known in advance, receivers can instantly verify the incoming beacon. Furthermore, we examine the storage overhead brought by our authentication scheme. If a mechanism brings a large storage burden, an attacker would initiate memory-based DoS attacks where an OBU is overwhelmed by storing a large number of unverified signatures. To defend against such attacks, PBA records shortened re-keyed Message Authentication Codes (MACs) instead of storing all the received signatures. We design PBA with an objective of providing effective, efficient, scalable broadcast authentication and also non-repudiation in vehicular networks.

The main contributions of this work are:

First, we analyse the security requirements for broadcast authentication in vehicular networks.

Second, PBA is designed to minimize the computational cost and storage overhead of authentication. Lightweight MAC and hash operations are mostly performed in PBA to defend against computation-based DoS attacks.

Third, PBA enables instant verification. With the predictability of a vehicle's position, we construct a MHT to commit all the possible results of the vehicle's movements between successive two beacons. Signature verification can be instantly performed based on prediction outcomes from MHTs integrated into beacons in advance.

Finally, analytical and empirical validations are done to evaluate our PBA scheme. We prove PBA is secure, and use Markov chains to analyse the effect of packet losses on the authentication delay and storage cost. Extensive simulations also indicate that PBA achieves excellent performance while incurring low delay and storage cost.

The rest of the paper is organized as follows.

Section 2 introduces background on vehicular networks cryptographic primitives. Section 3 describes the security requirement and threat model of proposed system. In Section 4, we present the construction of PBA. A detailed analysis of PBA is provided in Section 5. In Section 6, we present our evaluation results. Section 7 summarizes related work on authentication in vehicular networksfinally; weconclude our work in Section 8.

II. RELATED WORK

In this section, we provide an overview of the vehicular networks setting and the basic TESLA scheme.We divide VANET messages into two types based on the distance that they are going to spread, which means these packets are either single-hop beacons or multi-hop traffic data. For secure multi-hop traffic data, the standard ECDSA scheme [6] performs well when messages are sent infrequently. In this paper, we focus on the single-hop relevant applications, where vehicles periodically exchange beacons with nearby vehicles that are within the radio range.

As based on the IEEE 1609.2 standard, vehicles will periodically broadcast beacon information (e.g., position, velocity and time) 10 times per second to avoid the traffic accidents and react to unsafe situations. These information can be obtained from on-board devices such as GPS sensors, which could support nanosecond-level timing accuracy and meter-level positioning accuracy [7]. In the IEEE 1609.2 standard, a Public Key Infrastructure (PKI) is required for key management in vehicular networks. Each vehicle is equipped with a pair of ECDSA keys: a private key for signing and a public key for verification. These keys would be issued by a Certificate Authority (CA). Each key pair will be stored in the vehicle's OBU, with tamper-resistant property to defend against the compromising attack.

A vehicular networks beacon often contains a message body m, the sender's signature S, and the public key certificate of the sender Cert. The creation time is included in which could help receivers determine the message's deadline. S ensures that the sender is accountable for this message, and thus prevents drivers from releasing malicious information. Cert is used to announce the public key and identify the sender’s legality.

TESLA is an efficient scheme based on symmetric cryptography [12], [10]. It makes use of one-way hash chains with delayed disclosure of keys to achieve source authentication. For TESLA to operate securely, the sender and the receiver should be loosely time synchronized, which means that the synchronization does not need to be precise, but the receiver requires to know an upper bound on the sending time .

III. PROPOSED SYSTEM

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. 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 I0; I1; _ _ _; In. In a time frame, to send the first beacon B0 for I0, 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.

Design of the steps

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.

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,

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.

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 . After receiving a beacon, a vehicle will perform the following two steps:

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.

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.
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.

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 B_i, 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_iin which each entry represents one possible movement between $I_{i□1}$ and I_i. Inspired by the work [7], 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 ~ P_i could be represented as ~ P_i = ~ P_0+a_i~x+b_i~y, where $a_i$and b_i are rounded to integers. Hence, the movement from the interval $I_{i□1}$ to I_i is: ~M $_i$ = ~ P_i □ ~$P_{i□1}$ = (a_i□$a_{i□1}$)~x + (b_i □ $b_{i□1}$)~y; (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. 3(a), the prediction table PT_i collects all the possible results of ~M_i. Here, we are not interested in accurately modelling 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.

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 = fm$_0$; S_0;Certg, where m_0 = fT_0; I_0; ~ P_0;K_0; ~x; ~y;$Root_1$g is signed by ECDSA, and a Cert is issued by a CA.

For I_i, being at the position ~P_i and time T_i, 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.

Self-Generated MAC Storage

In a time frame, as the first beacon B_0 is signed by ECDSA, a receiver will directly store K_0, $Root_1$ and other local parameters if it passes the verification. Except B_0, when the receiver gets the signature of a beacon B_i, it will store a self-generated MAC to reduce memory cost. Algorithm 1 depicts the operations of the receiver.

Signature Verification

For the first beacon B_0, ECDSA signature can provide the property of non-repudiation. It helps the receiver ensure that the sender is accountable for the parameters such as the initial position ~ P_0 and the commitment of hash chains K_0, and thus prevents drivers from broadcasting malicious information. To verify the following signed B_i, the receiver verifies the validity of $K_{i□1}$ by following the one-way key chain back to K_0 signed with ECDSA. It recomputes the root value $Root_{0\ i}$ of MHT given relevant values in the m_i, and checks whether it matches $Root_i$stored in the memory; the receiver will verify m_i with the later TESLA key.

In the example .the receiver gets the tree root $Root_1$ from the first beacon. In I_1, it reconstructs L_2 from the values (e.g., R_{12}) in the message, and calculates the hash tree root based on L_2 and the off-path hashes fL_1;L_{10};L_{14}g. If the calculated root H(H(H(L_1jL_2)jL_{10})jL_{14}) matches $Root_1$, the receiver is convinced that the sender moves ~M_2 distance from I_0 to I_1, being located at ~P_1 = ~P_0 + ~M_2. In I_2, th receiver of B_2 reconstructs the hash tree root as before, and then does MAC operations towards the root with the keys $K_{0\ 1}$ and SK_{loc}. If the value matches MAC_{RS2}stored in the memory, the receiver is convinced thatthe sender moves ~M_7 distance from I_1 to I_2, beinglocated at ~P_2 = ~P_1 + ~M_7.

IV. ALGORITHM - AUTOMATIC GENERATED MACINTOSH

```
Require: Beacon atomic number 83, native secret key $SK_{loc}$
Check the safety condition;
if not satisfied then
    Drop the beacon
else
    Compute
```

```
            $MACRS_{i+1} = MACSK_{loc} (MAC_{Ki}{}^{1}(Root_{i+1}))$
        Store $MACRS_{i+1}$
    if $K_{i-1}$ is valid then
        Reconstruct the MHT's root node $Root_i{}^1$
        Recompute
            $MAC^1{}_{RSi}= MACSK_{loc} (MACK^1{}_{i-1}(Root^1{}_i))$
        if Search $(MAC^1{}_{RSi})$ == one then
            settle for mi
            Free memory for $MAC_{RSi}$
        else
            cypher
                $MAC_{MSi} = MACSK_{loc} (MACK^1{}_i(m_i))$
            Store $m_i$ and $MAC_{MSi}$
        end if
        Verify previously received messages
            Free memory for $m_g$ and $MAC_{MSg}$ (g <; i)
    end if
end if
```

V.SIMULATION RESULTS

To evaluate the performance of PBA, we use NS-3 to simulate the algorithm in a variety of VANET topologies. First, we consider a sender vehicle sends a beacon every 100 ms, and moves along the trajectory pre-defined for the simulation. The receiver vehicle receives the beacons with the probability 1 p. The parameters commonly used in VANETs are listed in Table 1. Moreover, a prediction table is required to model the vehicle's future positions. Actu-ally, some car suppliers or application providers of VANETs could offer advanced traffic statistics model to build the accurate prediction table. For simulation,

however, we construct a large prediction table to cover most of a vehicle's movements in a beacon interval, with 129 km/h of maximum speed limit. We set the block unit to be 2 meters with commodity GPS's positioning accuracy. For each beacon interval, we make use of 6 layers of MHT in our simulation.Fig. 1. The estimated maximum storage overhead Fs as the function of beacons' lifetime N and the packet loss rate p, with WB= 6 Mbps, tI =100 ms, Gm=160 Bytes, jmcj=100 Bytes, and Xs=Xm=4 Bytes.. Fig. 2 shows that the packet processing rate is affected by both p and N. When p begins to increase due to wireless losses or highly dynamic environ-ments, some beacons are lost so that the incoming beacons will be not verified instantly and buffered in the queue.

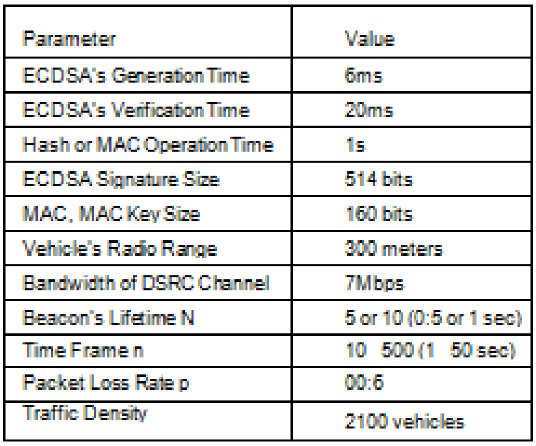
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

TABLE 1Parameters



Parameter	Value
ECDSA's Generation Time	6ms
ECDSA's Verification Time	20ms
Hash or MAC Operation Time	1s
ECDSA Signature Size	514 bits
MAC, MAC Key Size	160 bits
Vehicle's Radio Range	300 meters
Bandwidth of DSRC Channel	7Mbps
Beacon's Lifetime N	5 or 10 (0:5 or 1 sec)
Time Frame n	10 500 (1 50 sec)
Packet Loss Rate p	00:6
Traffic Density	2100 vehicles

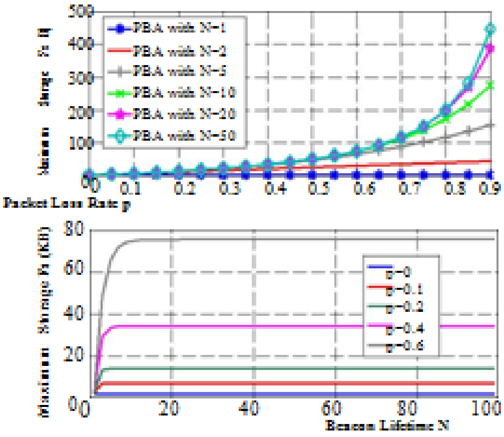


Fig. 1.Packet Loss Rate, Beacon Lifetime

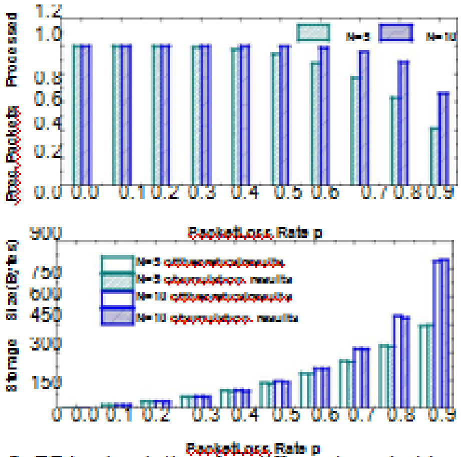


Fig. 2. PBA: simulation for different packet loss rate, and comparison with theoretical analysis

VI. CONCLUSION AND FUTURE WORK

For virtual networks communications, we propose an effective, efficient and scalable prediction based algorithm to resist the computation-based DoS attacks and packet losses in virtual networks.. Moreover, PBA has the advantage of the predictability of beacons lifetime for single hop relevant applications. To defend against memory based DoS attacks, PBA only keeps shortened MACs of signatures to reduce the storage overhead. By theoretical analysis, we show PBA is secure and robust in the context of virtual networks. Through a range of evaluations, PBA has been reduced the loss rate to perform efficient even under heavy traffic places. In the future, we will try to study how our scheme could be improved given accurate prediction models. We will address how to satisfy both security and privacy requirements in the future work.

REFERENCES

[1] Dedicated Short Range Communications (DSRC), http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] F. Bai, H. Krishnan, V. Sadekar, G. Holland, and T. Elbatt, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective," in Proceedings of IEEE Workshop on Automotive Networkingand Applications (AutoNet), pp. 1-25, 2006.

[3] IEEE Std 1609.2-2013 - IEEE standard for wireless access in vehicular environments - Security services for applications and management messages, Apr. 2013.

[4] H. C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur,V and A. Iyer, "Flooding-resilient broadcast authentication for vanets," in Proceedings of ACM Mobicom, pp. 193-204, Sep. 2011.

[5] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensornetworks," in Proceedings of IEEE INFOCOM, pp. 816-824, 2008.

[6] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks, " IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262, Jan. 2011.

[7] K. Shim, "Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree," IEEE Transactions on Wireless Communications, vol. 12, no. 11, pp. 5586-5393, Nov. 2013.

[8] M. Bellare, J. A. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures, " in Proceedings of EUROCRYPT, pp. 236-250, 1998.

[9] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps, " in Proceedings of EUROCRYPT, pp. 416-432, 2003.

[10] D. Hankerson, J. L. Hernandez, and A. Menezes, "Software implementation of elliptic curve cryptography over binary fields, " in Proceedings of CHES, pp. 1-24, 2000.

[11] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," IEEE Transactionson Vehicular Technology, vol. 62, no. 7, pp. 3339-3348, Sep. 2013.

[12] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sep. 2010.

BIOGRAPHY

P.SheelaRani , is anAssistant Professor, in Department of Information Technology at Panimalar Institute of Technology , Chennai, India . She received M.E degree in Computer Science & Engineering dept in 2011 at Anna University, Trichy, India. She has 7 years experience in Teaching. The article title of " Implementation of Customized Green call Algorithm for Energy efficient of Wireless Lan" was published in international research journal (ACST) by her. She is the Life ember of ISTE. She has attemded 3 international conference. Area of Interest are Network Security, Computer Networks, Cryptography & Security.

Mr.R.Vinston Raja receivedM.Tech in SathyaBama University Chennai, B.Tech Information Technology in Noorul Islam College of Engineering Anna University Chennai. He is working as an Assistant professor in Department of Information Technology at Panimalar Institute of Technology Chennai.

10.15680/ijircce.2015.0302043