IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Simulation and Analysis of PBA under Vehicular Networks

S. Anugraha[1], K. Bhuvaneswari[2], J. Indumathi[3], S. Sona[4], S. Sivanesskumar M.E., Ph.D.,[5]

UG Student, Electronics and Communication Engineering, A.V.C College of Engineering, Mannampandal[1]

HOD, Electronics and Communication Engineering, A.V.C College of Engineering, Mannampandal[2]

Abstract: In this paper, we propose an efficient broadcast authentication scheme called Prediction-Based Authentication (PBA) to not only defend against computation-based DOS attacks, but also resist packet losses caused by high mobility of vehicles. Our PBA is an efficient and lightweight scheme since it is primarily built on symmetric cryptography. To further reduce the verification delay for some emergency applications, PBA is designed to to predict future beacons in advance. In addition, to prevent memory-based DS attacks, PBA only stores shortened re-keyed Message Authentication Codes (MACs) of signatures without decreasing security. We analyze the security of our scheme and simulate PBA under varying vehicular network scenarios.

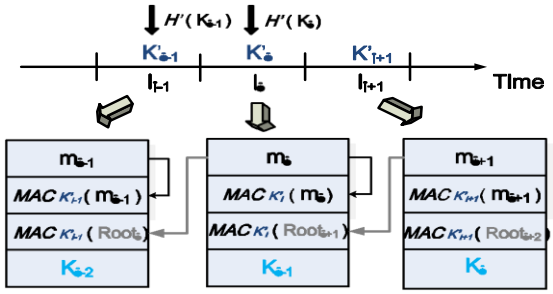
Keywords: cryptography; denial of service attacks; PBA scheme; tesla scheme; VANET.

1. INTRODUCTION

Vehicular ad hoc networks (VANETs) have recently attracted extensive attentions as a promising approach to enhancing road safety, as well as improving driving experience. By using a Dedicated Short-Range Communications (DSRC) technique, vehicles equipped with wireless On-Board Units (OBUs) can communicate with other vehicles and fixed infrastructure. Once VANETs become available, numerous safe, commercial and convenient services can be deployed through a variety of vehicular applications. These applications mostly rely on vehicles' OBUs to broadcast outgoing beacon messages and validate incoming ones. 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. 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. However, the current VANET signature standard using Elliptic Curve Digital Signature Algorithm (ECDSA). In this paper, we define this attack as computation-based DOS attacks. Even without any malice, the computation-based DOS attacks can be easily initiated in a high-density traffic scenario. To defend against DOS attacks, most existing schemes make use of the technology of identity-based batch verification or aggregate signature built on asymmetric cryptography to improve the efficiency of verification. In this paper, we propose an effective broadcast authentication scheme: Prediction-Based Authentication (PBA) to defend against computation-based DOS attacks for V2V communications. Unlike most of existing schemes based on asymmetric cryptography our PBA is primarily implemented on symmetric cryptography, whose verification is more than 22 times faster than ECDSA. In addition, PBA resists packet losses naturally. Similar to mobile wireless networks, packet losses are common in VANETs. We design our PBA on the TESLA scheme, which is proposed to secure loss multicast streams with hash chains. With TESLA signatures piggyback, PBA operates smoothly even when the packet loss rate is high. Extensive simulations also indicate that PBA achieves excellent performance while incurring low delay and storage cost.

2. TESLA SHEME

TESLA is an efficient scheme based on symmetric cryptography 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. TESLA can guarantee the receiver never accepts a message as an authentic message unless it was actually sent by the sender.



DOI 10.17148/IJARCCE.2017.62113

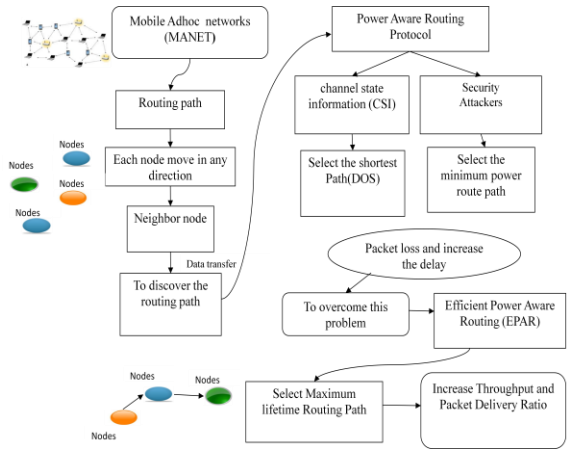
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

As a lightweight authentication scheme, TESLA also tolerates arbitrary packet loss. Drawback of TESLA is that the receiver has to buffer packets one disclosure delay before it can authenticate them. More- over, TESLA does not provide non-repudiation, since the receiver cannot convince a third party that the message arrived from the claimed sender.

3. BLOCK DAIGRAM



Nodes in an ad hoc wireless network are powered by batteries. It is expected that battery technology is unlikely to advance as rapidly as computing or communication technology. Traditional routing protocols tend to use shortest path algorithms (minimum hop count) with-out any consideration of energy consumption, often resulting in rapid energy exhaustion for the small subset of nodes in the network that experience heavy traffic loads. A power-aware routing protocol addresses the issues associated with energy consumption and conservation. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure fewer networks of mobile devices connected wirelessly. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Routing is the process of selecting a path for traffic in a Network, or between or across multiple networks. Routing is performed for many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), computer networks, such as the Internet, as well as in networks used in public and private transportation, such as the system of streets, roads, and highways in national infrastructure. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. A distributed denial-of-service (DDOS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example, a botnet) flooding the targeted system with traffic.

4. SIGNATURE GENERATION

After generating the commitment K0, constructing the prediction table with a local coordinate, and producing the MHT's root Root1 for the next beacon B1, the sender broadcasts the first beacon in a time frame. It contains public keys, time stamp T0, and other important parameters (such as, its local coordinate system). We format the first beacon as B0 ¼ fm0; S0; Cert where m0 ¼ fT0; I0; ~P0;K0;~x;~y;Root1g is signed by ECDSA, and a Cert is issued by a CA. For Ii, being at the position ~Pi and time Ti, the vehicle will locate the leaf node corresponding to ~Pi in the MHT, and broadcast the necessary values and off-path nodes of this leaf in mi. We define off-path nodes are the siblings of the nodes on the path from one leaf to the root of MHT. the car shows the leaf associated with the current location and time. At T1, the sender moves to ~P1 ¼ ~P0 þ ~ M2, associated with L2. Hence, m1 includes the random value and off-path nodes: fR12; L1; L10; L14g.

5. SECURITY REQUIREMENT

An efficient authentication scheme should guarantee timely message authenticity and non-repudiation. Meanwhile, it should resist packet losses and DOS attacks for relevant applications in VANETs. Here, we discuss each of these properties in detail. Timely authentication refers the receivers can ensure that a message was sent by a valid vehicle and it has not been modified during the trans- mission. Furthermore, timely signature verification is essential since each message has an expiration time by which the receiver should verify it. In VANETs, single-hop relevant applications usually have a shorter deadline. Non-repudiation, the property of non-repudiation allows a receiver to prove to a third party that the sender is account- able for generating the message. If the broadcast mechanism lacks non-repudiation, an adversary can claim it to be another party that created the message. Non-repudiation usually implies authentication, so the receiver can identify the sender and detect the manipulation of bogus packets. DOS attacks resistant. Given the relatively expensive Nature of signature verification, attackers may initiate computation-based DOS attacks that broadcasting a number of invalid signatures overwhelms the receivers' computational resources. If an authentication scheme brings large storage overhead, attackers may initiate memory-based DOS attacks which overwhelm the receivers' memory resources by broadcasting a number of invalid malicious messages. An authentication mechanism should have low computational and memory cost such that other applications can be operated normally in VANET.

5.1. CRYPTOGRAPHY

When a message is sent using cryptography, it is changed (or) encrypted before it is sent. The method of changing text is called a "code" or, more precisely, a "cipher". The changed text is called "cipher text". The change makes the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

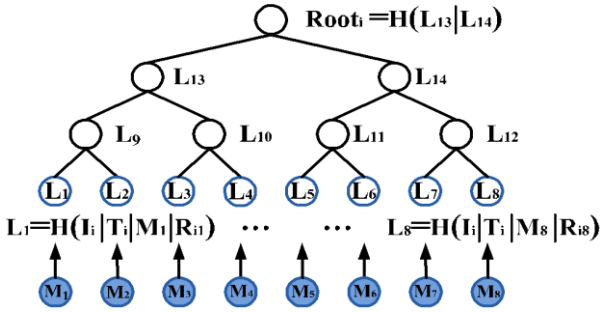
message hard to read. Someone who wants to read it must change it back . How to change it back is a secret. Both the person that sends the message and the one that gets it should know the secret way to change it, but other people should not be able to. Studying the cipher text to discover the secret is called "cryptanalysis" or "cracking" or sometimes "code breaking"

6. THE PBA 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 GPS-equipped vehicles are time- stamped 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. Our PBA includes the process of generating a signature by a sender and verifying the signature by a receiver. We intro- duce them separately.

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, as shown in Fig b
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 pro- pose a MHT, which ties these pre-computed keys together and then generates a single public key or prediction outcome for all the possible movements.

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 B0 in the time frame. For the rest of beacons such as B1 ; B2 ; ... ; Bn , the vehicle signs the message and the prediction outcome from MHT using the TESLA keys assigned in the intervals I1 ; I2 ; ... ; In .
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 net- work bandwidth.

Self-Generate MAC Storage
In a time frame, as the first beacon B0 is signed by ECDSA, a receiver will directly store K0, Root1 and other local parameters if it passes the verification. Except B0, when the receiver gets the signature of a beacon Bi, it will store a self- generated MAC to reduce memory cost.

Algorithm 1 depicts the operations of the receiver.

Require: Beacon Bi, Local secret key SKloc
1: Check the security condition;
2: if not satisfied then
3: Drop the beacon
4: else
5: Compute
MACRSiþ1 ¼ MACSKloc ðMACK0i
ðRootiþ1ÞÞ
6: Store MACRSiþ1
7: if Ki_1 is valid then
8: Reconstruct the MHT's root node Root0i
9: Recompute
MAC0RSi ¼ MACSKloc ðMACK0i
_1 ðRoot0iÞÞ
10: if Search ðMAC0RSiÞ ¼¼ 1 then
11: Accept mi
12: Free memory for MACRSi
13: else
14: Compute
MACMSi ¼ MACSKloc ðMACK0i
ðmiÞÞ
15: Store mi and MACMSi
16: end if
17: Verify previously received messages
Free memory for mg and MACMSg (g < i)
18: end if
19: end if

6.1Wireless lossy environment
In this section, we first prove that PBA is secure. Then, we discuss the performance of PBA in wireless loss environment .Finally, we analyze the storage requirements of PBA. We assume the packet loss rate is p, and a beacon's lifetime is N (N _ 1) intervals from the time that a sender generates the beacon.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Security Proof

PBA relies on the symmetric cryptographic functions (hashes and MACs) and the basic TESLA scheme. We begin by assuming these cryptographic functions are secure. The security of the TESLA scheme has been proved in previous work [24]. Besides the basic TESLA scheme, new mechanisms are proposed in PBA to provide more properties. On one hand, a sender broadcasts a MAC before it sends the beacon to support instant authentication. On the other hand, by using a secret key on the received MAC, the receiver generates a shortened MAC to reduce the possibility of memory-based DOS attacks. However, these new mechanisms will become useless if they enable adversaries to spoof other vehicles. Here, we show a detailed security proof of PBA.

Theorem 1.

If the underlying MAC algorithms and hash chains are secure, given a receiver vehicle's key is securely kept, PBA provides a negligible probability that an attacker could forge a legitimately authenticated message in the context of VANETs, independent of the attacker's computational capability.

7. SIMULATION RESULTS

To evaluate the performance of PBA, we use NS-2 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. Then, we simulate PBA together with ECDSA, TESLA and VAST in more real road situations, with more sources sending beacons. The parameters commonly used in VANETs are listed in Table 1. Moreover, a prediction table is required to model the vehicle's future positions.

7.1Single-Neighbor Case

We first discuss the impact of the time frame n, the packet loss rate p, and the lifetime of beacons N on our PBA scheme. We will evaluate PBA based on these four metrics: Sender's computational overhead, which is expressed by the average time for a beacon's signature generation; Receiver's computational overhead, which is expressed by the average time for a beacon's signature verification; Packet processing rate of a receiver, to wireless losses or highly dynamic environments, some beacons are lost so that the incoming beacons will be not verified instantly and buffered in the queue. If N is large enough, the receiver can verify the beacons even under high packet loss rate (e.g., p ¼ 0:6). In this case, PBA can still maintain almost 100 percent packet processing rate. Otherwise, the curve of packet processing rate declines when beacons are out of date and then dropped. On the storage overhead, we compare the simulation results with theoretical analysis obtained by Equation .We find the theoretical analysis predicts the performance very accurately

$$ES=XS.\pi 0+(xm+|mc|).(\sum_{i=1}^{N-1}(i)\pi^{N}(N-1).\pi N)$$

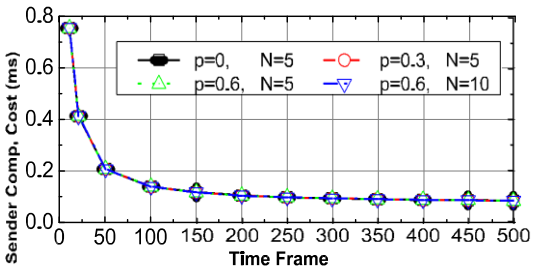


Figure 1time frame against number sender comp

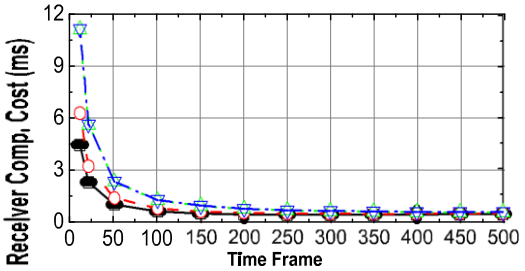


Figure 2 time frame against receiver comp.cost

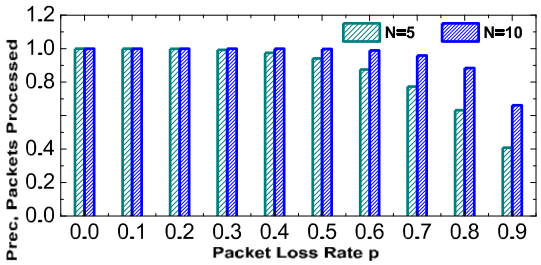


Figure3 packet loss against proceed packets processed

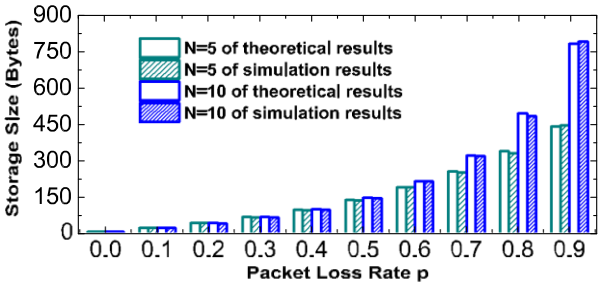


Figure4 packet loss rate against storage size

8. CONCLUSION

For V2V communications, we propose an effective, efficient and scalable broadcast authentication scheme to provide both computation-based DOS attacks resilient and packet losses resilient in VANETs. Moreover, PBA has the advantage of fast verification by leveraging the predictability of beacons 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 VANETs. Through a range of

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

evaluations, PBA has been demonstrated to perform well even under high-density traffic scenarios and loss wireless scenarios.. For some vehicular applications, it is also important to consider the privacy issues

REFERENCES

[1] TM E2213-03-Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems-5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Sep. 2003

[2] F. Bai, H. Krishnan, V. Sadekar, G. Holland, and T. Elbatt, "Toward characterizing and classifying communication-based automotive applications from a wireless networking perspective," in Proc. IEEE Workshop Automotive Netw. Appl., pp. 1–25, 2006.

[3] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proc. Fourth Workshop Hot Topics Netw., Nov. 2005.

[4] S. B. Lee, G. Pan, J. S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in Proc. ACM Mobihoc, pp. 150–159, 2007

[5] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Secur., vol. 15, no. 1, pp. 39–68, 2007

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

[7] D. Hankerson, J. L. Hernandez, and A. Menezes, "Software implementation of elliptic cryptography over binary fields," in Proc. Cryptographic Hardware Embedded Syst., pp. 1–24, 2000.