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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Study of Prediction Based Authentication for Vehicle to Vehicle Communication

Jayshri A. Marathe, Satpalsing D. Rajput

M.E Student, Department of Computer Engineering, SSBT COET, North Maharashtra University, Jalgaon, Maharashtra, India

Asst. Professor, Department of Computer Engineering, SSBT COET, North Maharashtra University, Jalgaon,Maharashtra, India

ABSTRACT: Broadcast communications are critically important, as many safety-related applications rely on single-hop beacon messages broadcast to neighbor vehicles. 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 attacks that excessive signature verification exhausts their computational resources. Here 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. In contrast to most existing authentication schemes, 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 exploit the sender vehicles ability to predict future beacons in advance. In addition, to prevent memory-based DoS attacks, PBA only stores shortened re-keyed Message Authentication Codes (MACs) of signatures without decreasing security .

KEYWORDS: VANETs; broadcast communication; signatures; DoS attacks; prediction-based authentication

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) have emerged as a distinguished technology that facilitates the exciting analysis and application space for current era of transport system. As a sub category of Mobile Ad Hoc Networks (MANETs),VANETs give communication by redirecting datagram over multi hop wireless links. It helps the communication among Vehicle To Vehicle (V2V) and Vehicle To Infrastructure (V2I) in wireless setting with none underlying network infrastructure.

VANET: VANET are constructed to manage the communication between the vehicles. VANETs, is a form of Mobile Ad-Hoc Network, to provide communications among nearby vehicles and between vehicle and nearby fixed equipment, usually described as roadside equipment. It enhance driver safety and reduce traffic deaths and injuries. Vehicle to Vehicle and Vehicle to Infrastructure communications are regarded as two basic types of communications in VANETs. By using a dedicated Short-Range communications technique, vehicles equipped with wireless On-Board Units can communicate with other vehicles and fixed infrastructure. On Board Unit and Road Side Infrastructure (RSI) are used to carry out the communication process.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

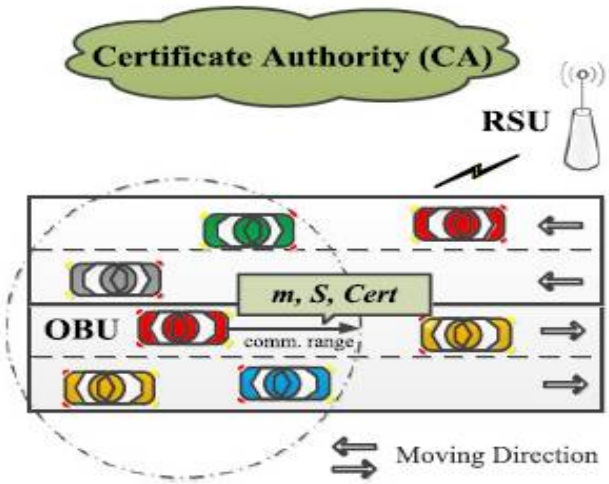


Fig1.1.Typical VANET scenario.

II. WORKING OF VANET

VANET is a technology that uses moving vehicles as nodes in a network to create a mobile network. VANET turns every participating vehicle into a wireless router or node, allowing vehicles approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created. VANET is a subgroup of MANET where the nodes refer to vehicles. Since the movement of Vehicles are restricted by roads, traffic regulations we can deploy fixed infrastructure at critical locations. The primary goal of VANET is to provide road safety measures where information about vehicle's current speed, location coordinates are passed with or without the deployment of Infrastructure. Apart from safety measures, VANET also provides value added services like email, audio/video sharing etc,.

Classes of Information:

- Movement Related – speed, velocity, acceleration, etc
- Traffic Related – number of vehicles, traffic volume, density, congestion
- Passenger Related – weather related information

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). 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 OBU in the network. So that communication overheads and consumes delay in message authentication. 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.

The Road side unit plays a vital role in identifying the malicious node packets and clears those packets with correct packets with respect to all the vehicles in the scenario. Figure 1.2shows Presence of RSU, malicious node and other vehicles in the Highway.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

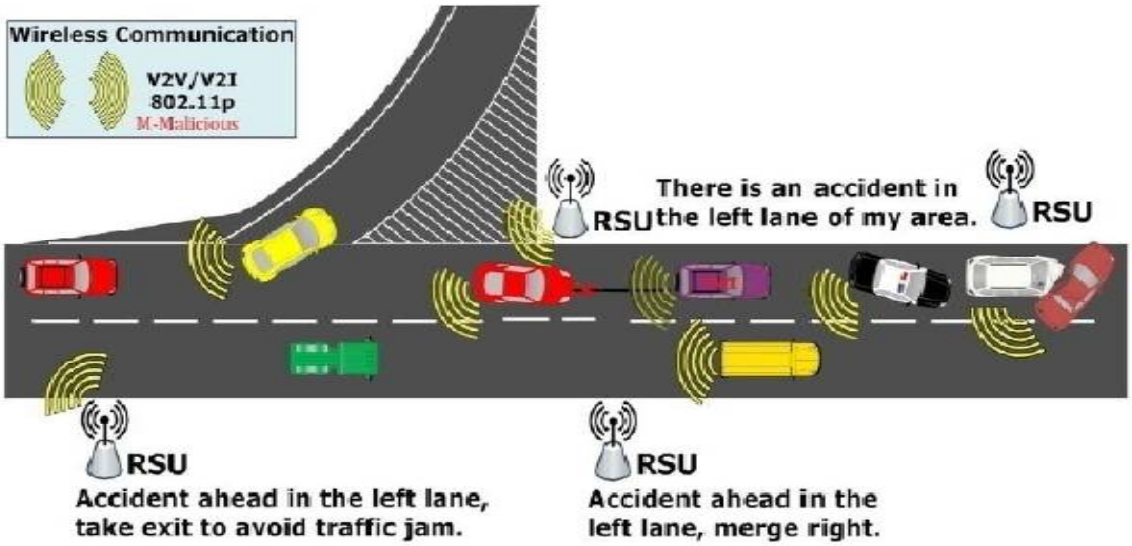


Figure1.2: The Presence of RSU, malicious node and other vehicles in the Highway.

VANET Simulators:

Vehicular mobility generators are needed to increase the level of realism in VANET simulations. Network simulators perform detailed packet-level simulation of source, destinations, data traffic transmission, reception, background load, route, links, and channels. VANET simulators provide both traffic flow simulation and network simulation.

The simulation results indicate that the integrated approach provides higher throughput and reduces the end to end delay, when compared to that of the existing method. It also achieves the high packet delivery ratio and minimizes the delay overhead.

III. 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. Discussing each of these properties in detail.

- Timely authentication: With the authentication mechanism receivers can ensure that a message was sent by a valid vehicle and it has not been modified during the transmission. 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 accountable 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.
- Packet losses resistant:Packet losses are common in wireless networks, specially in VANETs. When a packet is lost during the transmission, it should have little inuence for the receiver to verify other subsequent 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 receiver's computational resources. If an authentication scheme brings large storage overhead, attackers may initiate memory-based DoS attacks which overwhelm the receivers memory resources

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

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 VANETs.

Components of Security Architecture:

- Event Data Recorder: The EDR will be responsible for recording the vehicles critical data such as position, time, speed etc. EDR will also record all the received safety messages.
- Tamper Proof Device: The TPD will store all the cryptographic materials and perform cryptographic operations like signing and verifying safety messages.
- Vehicular Public Key Infrastructure:- In VPKI infrastructure Certificate Authorities will issue certified public/private key pairs to vehicles.
- Authentication: Vehicles will sign each message with their private key and attach corresponding certificate. Thus when another vehicle receives the message it verifies key used to sign the message and then it verifies the message.
- Privacy: To conceal vehicles identity , set of anonymous keys that changes frequently can be used. This keys are preloaded into vehicles Tamper Proof Device for long duration.

IV. LITERATURE SURVEY

SYSTEM DESIGN:

Fast Auth Scheme:

One-time signature scheme named Fast Auth is used to provide lightweight, timely and nonrepudiation authentication for vehicle-to-vehicle communications. Chained Huffman hash trees is use to generate a common public key and minimize the signature size for beacons sent during one prediction interval. Exploits the predictability of future beacons to achieve the instant authentication in VANETs.

Shortcomings:

- If the receiver misses a beacon, it cannot work in the rest of the current prediction interval.
- It cannot accurately collect the entire beacon message
- Also, it cannot increase the packet delivery ratio.

Prediction Based Authentication System Module:

The following are the details in the sender side and receiver side details involved in the communication.

Sender

- Chained keys generation
- Position prediction
- Merkle hash tree construction
- Signature generation

Receiver

- Attack packet detection
- Signature Verification

Overview of Prediction Based Authentication Scheme:

Prediction based authentication is used in the sender side to detect Denial-of-Service attacks before the signature verification. Enhanced attacked packet detection algorithm is used at the receiver side to detect malicious node. To reduce the verification delay, PBA is designed to exploit the sender vehicles ability to predict future beacons in

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

advance. Applications rely on vehicles OBUs to broadcast outgoing beacon messages and to validate incoming ones. The broadcast beacons often contain information about position, current time, speed, direction, driving status, etc.
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. PBA 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. PROTOCOL OVERVIEW: PBA includes the process of generating a signature by a sender and verifying the signature by a receiver. 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.

Sender Side Process:

- 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. MHT structure is proposed to 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 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. It contains public keys, time stamp T0, and other important parameters.

Receiver Side Process:

Attack packet detection:

It is based on the position changing requirements. Attacked packets are identified by the following parameters Frequency (f), Velocity (v), is Coefficient which is determined by the road characteristics and (VMax) is the maximum speed.

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

a) Selfgenerated 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.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

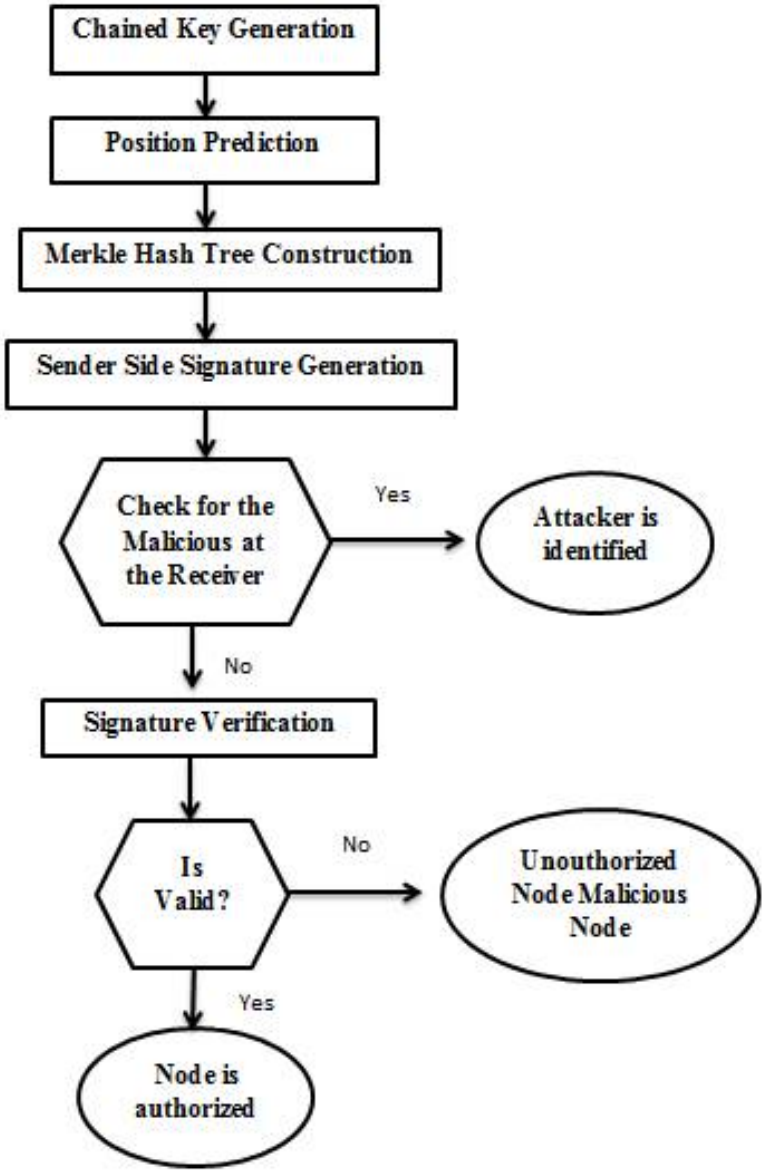
Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

b) Signature verification:

For the first beacon, the receiver veryfies the ECDSA signature. To verify the following signed Bi, 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.

V. SYSTEM FLOW



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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

VI. CONCLUSION

For virtual networks communications, here an effective, efficient and scalable prediction based algorithm is used to resist the computation-based DoS attacks and packet losses in virtual networks. These technology can greatly enhance the infotainment, safety, comfort, communication and convenience value of new vehicles. As vehicles become "smarter", security and privacy gain importance. 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, enhanced PBA protocol 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.

REFERENCES

1. 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 Proc. IEEE Workshop Automotive Netw. Appl., pp. 125, 2006.
2. H. C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Floodingresilient broadcast authentication for vanets," in Proc. ACM Mobicom, pp. 193204, Sep. 2011.
3. 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 Trans. Vehicular Technol., vol. 60, no. 1, pp. 248262, Jan. 2011.
4. T. Unterluggauer and E. Wenger, "Efficient pairings and ecc for embedded systems," in Proc. Cryptographic Hardware Embedded Syst., pp. 298315, 2014.
5. X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," IEEE Trans. Vehicular Technol., vol. 62, no. 7, pp. 33393348, Sep. 2013.
6. R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. IEEE INFOCOM, pp. 19031911, 2008.
7. C. Zhang, X. Lun, R. Lu, P. Ho, and X. Shen, "An efficient message authentication scheme for vehicular communications," IEEE Trans. Vehicular Technol., vol. 57, no. 6, pp. 33573368, Nov. 2008.
8. Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," IEEE Trans. Wireless Commun., vol. 8, no. 4, pp. 19741983, Apr. 2009.
9. ASTM 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.
10. 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.
11. M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Secur., vol. 15, no. 1, pp. 39–68, 2007.
12. K. Shim, "Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree," IEEE Trans. Wireless Commun., vol. 12, no. 11, pp. 5586–5393,Nov. 2013.
13. M. Bellare, J. A. Garay, and T. Rabin, "Fast batch verification for modular exponentiation and digital signatures, " in Proc. EUROCRYPT, pp. 236–250, 1998.
14. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Proc. EUROCRYPT, pp. 416–432, 2003.
15. J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 9, pp. 1227–1239,Sep. 2010.