© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Secure Authentication for Vehicle-To-Vehicle Communication Using VANET

M. Vetriselvan, V. RajaRam
Department of Information Technology. Sri Venkateswara College of Engineering .Chennai, TamilNadu, India

ABSTRACT

Intelligent Transportation Systems (ITS) has gain a lot of popularity due to much technological advancement in Vehicular Ad hoc Networks (VANETs). VANET provides safety and entertainment services to vehicle users. Therefore, constrained safety is a prominent feature for VANETs. Since the vehicular nodes typically moves fast than the nodes movement in other network such as Mobile Ad hoc Networks (MANETs), it is of great importance to design an efficient routing protocol to provide safety and comfort services to the passengers on the roads. Recently efforts have been put to use the concepts of fuzzy logic to help in the decision making process in VANETs. Fuzzy logic deals with reasoning that is approximate rather than fixed and exact. The fuzzy logic inference system became important and useful when the values of the decision criteria are not only vague but uncertain in nature. In this work, based on analysis of greedy routing for packet forwarding, we have proposed a Fuzzy Logic based Greedy Routing (FLGR) protocol. FLGR is a multi- hop routing protocol which is used to select the best next-hop node in multi-hop VANETs using fuzzy logic concept. We have considered two characteristics of a vehicle as an input metrics to fuzzy decision making systems. Based on the optimum function of simulation results, the FLGR effectively select the best next-hop node for further packet transmission in the network.

Keywords : VANETs, broadcast communication, signatures, DoS attacks, prediction-based authentication

I. INTRODUCTION

Vehicular adhoc 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, e.g., Road-Side Units (RSUs), located at critical points of the road. Therefore, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are regarded as two basic types of communications in VANETs. 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.

VANETs allow vehicles to broadcast messages to other vehicles in the vicinity. It is suggested that each vehicle periodically send messages over a single hop every 300ms within a distance of 10s travel time (which is a distance range between 10 m and 300 m). This mechanism can be used to improve safety and optimize trac. However, malicious vehicles can also make use of this mechanism by sending fraudulent messages for their own profit or just to jeopardize the trac system. Hence, the system must be designed to ensure that the transmission comes from a trusted source and has not been tampered with since transmission.

Another critical concern in VANETs is driving privacy or vehicle anonymity. As noted in, a lot can be inferred on the driver's privacy if the whereabouts and the driving pattern of a car can be tracked. However, it is possible for attackers to trace vehicles by using cameras or physical tracking. But such physical attacks can only

trace specific targets and are much more expensive than monitoring the communication in VANETs. This paper addresses the latter attacks.

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure. Examples of wireless networks include cell phone networks, Wireless local networks, wireless sensor networks, satellite communication networks, and terrestrial microwave networks.

During past decades WSNs have witnessed a relentless research activity to leverage the deployment of low cost, easy to maintain and energy efficient solutions to monitor natural phenomena and men-made activities. Recently, the surge of packet data traffic over the cellular network has leveraged IoT and Machine-Type Communications, thus making sensors part of an omnipresent communication network. Standardization bodies started several activities on WSN technology and its subsequent amendments at both PHY and Medium Access Control (MAC) layers is one exemplary case of such ongoing effort We consider in this work the latest for professionally installed star topology WSNs (STP-WSN).

In STP-WSNs temporary obstructions might clutter the LOS connection between sensors deployed over a wide survey area and the central coordination point or AP. When this occurs, sensors will be unable to report sensed data although they function properly. Depending on the particular monitored phenomena, faulty sensors might trigger unnecessary human intervention or safety alarms. Network connectivity is an important topic, by the critical transmission radius of a node The NACRP developed for the first time in this work tackles the same general context of but it provides a completely different solution since NACRP is a new protocol solving lack of connectivity under the centralized control of the AP.

II. SYSTEM DESIGN

The major motivation of the fuzzy logic system is to accomplish considerable improvement in the performance of the original greedy routing protocol through the improvement of selecting the next-hop forwarding node from a small subset of neighbor nodes for further transmission. In this paper, we use two metrics for selecting the best next-hop node, namely, distance metric which specifies the distance of a neighboring vehicle from source node/current forwarding node (CFN) and position metric which tells how far the neighboring vehicle is from the source/CFN on a straight line joining source/CFN and destination by projecting a projection on this straight line. The vehicles in VANETs are aware of the network information from the GPS device in the vehicle. A detail of these metrics is explained in the next section. It becomes difficult to decide the best next-hop node by using network information for the following reasons. First, the network information can be imprecise. Secondly, as these multiple metrics can conflict with each other, therefore it results in uncertainty. As fuzzy logic can deal with uncertain and imprecise information, we use a fuzzy logic based method to discover the neighbor node which can give the best results. The two metrics stated above serves as an input to fuzzy decision making system that helps in identifying the approximate best next-hop node for forwarding the packets.

A. VANET Setting

PBA with an objective of providing effective, efficient, scalable broadcast authentication and also non-repudiation in VANETs. To the best of our knowledge, prior authentication schemes for V2V communications either lack non-repudiation or fail to operate in high packet loss or high-density traffic scenarios. The main contributions of this work are First, we analyze the security requirements for broadcast authentication in VANETs and design a lightweight authentication scheme called PBA for V2V communications. 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. Signature verification can be instantly performed based on prediction outcomes from MHTs integrated into beacons in advance.

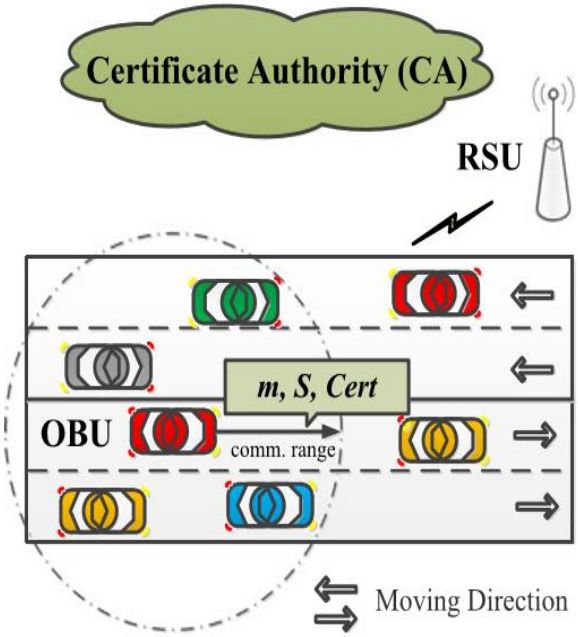

Figure 1. Architecture of V2V communication process

III. DESIGN AND IMPLEMENTATION

A. Elliptic Curve Digital Signature Algorithm

RSU will verify multiple received signatures at the same time such that the total verification time could be reduced. In their schemes, the computational cost is mainly dominated by a few operations of pairing and a number of operations of point multiplication over the elliptic curve. It is affordable for RSUs but expensive for OBUs to verify the messages. If attackers inject false beacons, it is so hard for the receiver to locate them that these schemes are also vulnerable to computation-based DoS attacks. In addition there are some works that rely on RSUs or other vehicles to achieve the authentication for vehicular communication.

B. Reed-Solomon Coding and Public Key Rebinding

A one-time signature scheme named FastAuth to provide lightweight timely and non repudiation authentication for vehicle-to-vehicle communications. They use chained Huffman hash trees to generate a common public key and minimize the signature size for beacons sent during one prediction interval As first exploits the predictability of future beacons to achieve the instant authentication in VANETs. One drawback in FastAuth: once the receiver misses a beacon, it cannot work in the rest of the current prediction interval. To deal with packet losses, they add the schemes of Reed-Solomon Coding and Public Key Rebinding, communication overhead is required in wireless lossy environments, as well as the computational overhead. is required in wireless lossy environments, as well as the computational overhead.

C. Prediction-based Authentication Scheme

1) ECDSA signatures and TESLA-based scheme to authenticate beacons. TESLA scheme, PBA also requires loose time synchronization Chained Keys Generation: At the beginning of a time frame, each vehicle generates n chained private keys for the next 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.vehicles model all the possible results of movements between two consecutive beacons based on information of the past trajectory.

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.

IV. CONCLUSION AND FUTURE ENHANCEMENT

This system propose an effective, efficient and scalable broadcast authentication scheme to provide both computation-based DoS attacks re- silient and packet losses resilient in VANETs. More- over, 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.

V2V communications, 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.

The proposed protocol FLGR is used to select the next-hop forwarding nodes on the routing path through V2V communication processes. In FLGR, all the nodes in the network periodically broadcast the Hello packets. A sender node on receiving the Hello packet from the nodes in its transmission range R gets aware of its neighbors. Next, the current forwarding node (CFN) transmits a packet to a destination via intermediate nodes. Therefore, the CFN selects the best next-hop node among various other neighboring nodes from the right half of the circular region by employing the concept of fuzzy logic.

During next-hop node selection process we consider two routing metrics such as distance of neighbor node from source, and position towards destination from source/CFN for each of the candidate neighbor nodes. These routing metrics are considered as an input of the fuzzy decision making system through which fuzzy output is calculated for each neighbours.

The neighbour node with the maximum value of fuzzy output is selected as the best preferable next-hop neighbor node around a source/CFN. FLGR selects the node from the neighboring nodes as the next-hop node which is at maximum distance from the source node and closer to destination node. PBA is secure and robust in the context of VANETs.

V. REFERENCES

[1] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, "An Efficient Message Authentication Scheme for Vehicular Communications", IEEE transactions on vehicular technology, vol. 57, no. 6, November 2008.

[2] Yixin Jiang, Minghui Shi, Xuemin (Sherman) Shen, and Chuang Lin, "BAT: A Robust Signature Scheme for Vehicular Networks Using Binary Authentication Tree", IEEE transactions on wireless communications, vol. 8, no. 4, April 2009.

[3] Nikita Lyamin, Alexey Vinel, Magnus Jonsson, and Jonathan Loo, "Real-Time Detection of Denial-of Service Attacks inIEEE 802.11p Vehicular Networks", IEEE communications letters, vol. 18, no. 1, January 2014.

[4] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, "An Identity-Based Security System forUser Privacy in Vehicular Ad Hoc Networks", IEEE transactions on parallel and distributed systems, vol. 21, no. 9, September 2010.

[5] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu 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, January 2011.

[6] Yong Hao, Yu Cheng, Chi Zhou, Wei Song, "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs", IEEE journal on selected areas in communications, vol. 29, no. 3, March 2011.

[7] 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, January 2013

[8] Suk-Bok Lee, Joon-Sang Park, Mario Gerla, Songwu Lu, "Secure Incentives for Commercial Ad Dissemination in Vehicular Networks", IEEE transactions on vehicular technology, vol. 61, no. 6, July 2012.

[9] Xiaodong Lin, and Xu Li, "Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks", IEEE transactions on vehicular technology, vol. 62, no. 7, September 2013.

[10] Kyung -Ah 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, November 2013.