Privacy Preserving Authentication Framework for VANET using PCREF

Humashameen. C
Department of Computer Science and Engineering
Saveetha Engineering College/ PG Scholar
Chennai, Tamil Nadu/India

Saravanan. R
Department of Computer Science and Engineering
Saveetha Engineering College/Head of the Department
Chennai, Tamil Nadu/India

***Abstract*— A vehicular Ad hoc Network (VANET) is a technology that employs moving vehicles as nodes in a network to create a mobile network to provide communication among vehicles and nearby fixed Road Side Units (RSU). In Vehicular Ad hoc Networks (VANET) authentication is a crucial security service for both inter-vehicle and vehicle-roadside communications. Therefore, vehicles have to be protected from the misuse of their private data and the attacks on their privacy as well as to be capable of being investigated for accidents or liabilities from non-repudiation. In this paper, a security mechanism has been incorporated in the AODV protocol to provide secure transmission among the vehicles. The detection, prevention and reactive AODV scheme (DPRAODV) is developed with control packet to detect the attack and remove the malicious node in the environment. Thus the control packet will notify the vehicle which are active in the communication and broadcast the black listed vehicle ids to the neighborhood nodes. It also provides integrity, confidentiality, non-repudiation, anonymity and traceability for VANET communications. The developed framework has been applied in a simulated environment using NS-2 package.**

Keywords— ***Ad hoc, VANET, Attacks, Security mechanism, AODV, DPRAODV,NS-2***

I. Introduction

VANET is an application of mobile ad hoc network. More precisely a VANET is self-organized network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers. Two types of communication are provided in the VANET. First a pure wireless ad hoc network where vehicle to vehicle without any support of infrastructure. Second is communication between the road side units (RSU), a fixed infrastructure, and vehicle. Each node in VANET is equipped with two types of unit such as On Board Unit and Application Unit (AU). OBU has the communicational capability whereas AU executes the program making OBU‘s communicational capabilities. An RSU can be attached to the infrastructure network which is connected to the Internet.

In VANETs the user authentication is a crucial security service for access control in both inter-vehicle and vehicle-roadside communication. On the other hand vehicles have to be protected from the misuse of their private data and the attacks on their privacy, and meanwhile, be capable of being investigated from accidents or liabilities for non-repudiation. Peculiarly safety applications require a strong mutual authentication, because most of the safety-related messages may contain life-critical information. Traditional mechanisms cannot deal with the vulnerabilities discussed of the new challenges in VANETs. Such challenge is the high network volatility caused by the highly mobile very large scale network. Another challenge is that the network must offer liability and privacy at the same time in an efficient way, as the applications are delay sensitive. To make things even worse the network are very heterogeneous different vehicles can have different equipment and abilities, so no unique solution can solve every problem. When defining the key vulnerabilities and challenges of vehicular ad hoc networks, it is crucial to first define and characterize the possible attackers.

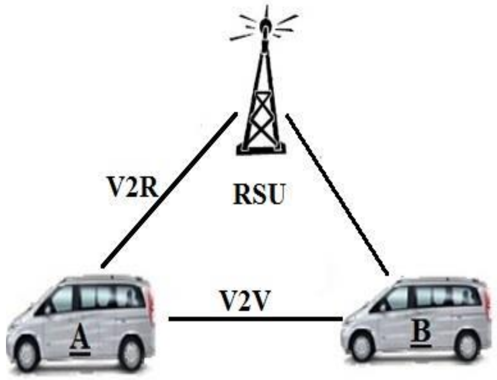

Fig 1: Types of Communication of Vanet

Each solution must preserve the security requirements like authentication, integrity, and privacy which are more targeted. Since vehicular network is managed by the different operators hence authentication must be required not only for Vehicle to Vehicle (V-V) communication but also in Vehicle to Infrastructure (V-I) and administrative domain. Solutions also used the different cryptographic algorithms broadly categorised into Symmetric and Asymmetric. In networked Systems attackers could inject false measurements to the controller through compromised sensor nodes which not only threaten the security of the system but also consumes network resources. To deal with this issue an en-route filtering schemes have been designed for wireless sensor networks.

The main vulnerabilities in VANETs come from the wireless nature of the communication, and the sensitive information, such as location of users, used by the network. One major vulnerability comes from the wireless nature of the system the Communication can be jammed easily, the messages can be forged. Another problem related to the wireless communication is that while the nodes are relaying messages, they can modify them. This is called In-Transit

Traffic Tampering. Another kind of problem, that the vehicles can impersonate other vehicles with higher privileges such as emergency vehicles to gain extra privileges. The most relevant problem to this dissertation is that the privacy of the drivers of the vehicles can be violated. The proposed framework provides the conditional vehicle anonymity for privacy preservation with traceability for the non-repudiation, in case that malicious vehicles abuse anonymous authentication techniques to achieve malicious attacks. The mechanism such as the public-key cryptography (PKC) to the pseudonym generation, which ensures a legitimate third party to achieve non-repudiation of vehicles by obtaining vehicle real IDs.

1.1 System Architecture

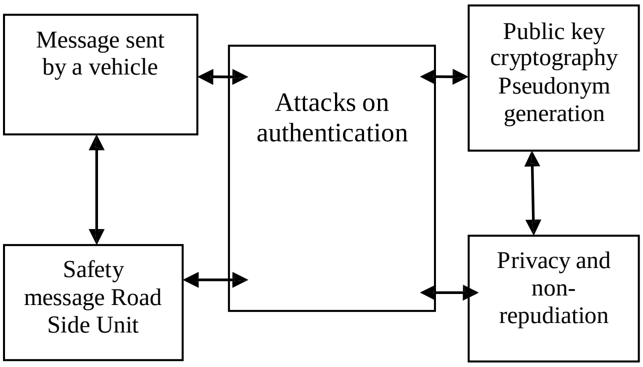
Message sent by a vehicle
Attacks on authentication
Public key cryptography Pseudonym generation
Safety message Road Side Unit
Privacy and non-repudiation

Fig 2: Architecture of VANET with Privacy Preservation

The communication in VANET is established between V2V and V2R. The message send between vehicle to vehicle compromised with various types of attack such as Sybil, black hole, impersonate and so on. The attack on authentication is protected by digital signature with encrypt the message with vehicle real id and pseudonym generation. The privacy and non-repudiation is achieved by trusted third party can link pseudonym with message. Thus the safety of message is achieved with schema to detection, prevention and reactive AODV called DPRAODV is implemented. Adoptions of alarm packet are used to notify the attack in the communication. The Black hole attack in VANET communication is mainly discarded with the help of neighborhood based routing and distributed cooperative mechanism. This mechanism helps in detecting and preventing attacks in the VANET environment.

II. RELATED WORK

Jie Li, Huang Lu, Mohsen Guizani [1] proposed "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs" Public-key cryptography (PKC) to the pseudonym generation ensures legitimate third parties to achieve the non-repudiation of vehicles by obtaining vehicle's real IDs. The self-generated PKC-based pseudonyms are also used as identifiers instead of vehicle IDs. The update of the pseudonyms depends on vehicular demands for the privacy preserving authentication in nodes. ACPN provides the conditional vehicle anonymity for privacy preservation with traceability. Malicious vehicles abuse anonymous authentication techniques to achieve malicious attacks.

Qingzi Liu, Qiwu Wu, Li Yong [2] proposed " A hierarchical security architecture of vanet " ID-based security system architecture cancels the extra expenditure for CRL and evades use of the public key in traditional PKI. The process involves generating irreversible algorithm for pseudonyms based on ID with firm confirmation that only one pseudonym is available within the same entity to prevent from Sybil attack.

Ren-Junn Hwang, Yu-Kai Hsiao and Yen-Fu Liu proposed [3] "Secure Communication Scheme of VANET with Privacy Preserving",Identity-Based Encryption (IBE) to provide privacy preservation in VANET environment. Two types of role such as the trusted third party named Authorization server (AS) in the VANET and VANET user. Each vehicle registers at AS before joining the network. If there is malicious vehicle broadcasting wrong messages then the validity of the vehicle is broken immediately. Efficient and scalable information dissemination is a major challenge due to the changes in network topology.

Xi Yu , Huaqun Guo and Wai-Choong Wong [4] proposed "A Reliable Routing Protocol for VANET Communications" AODV Routing Protocol for VANET Communications transforms the vehicles movement information into the route discovery process. A Total Weight of the Route is introduced to choose the best route together with an expiration time estimation to minimize the link breakages. With the weight prediction method the system is able to achieve better routing performance by sending TCP packets with a lower packets drop rate. TCP connection may not be the best transport layer protocol for the simulation of ad hoc network protocols due to the high bit error characteristics of an ad hoc network like VANET.

Jan Janech, Stefan Toth [5] proposed "Communication in distributed database System in the vanet environment", in safety applications and comfort applications. System focusing on the best way to distribute information to all nodes that are interested. The database system is designed to be used in VANET environment and so its basic principles had to be altered for such usage.

Song Haibin, Meng Qi, Men Aidong [6] proposed "P2P Computing in Design of VANET Routing Protocol" Peer computing based Ad hoc On Demand Vector (PAV) combine the functions of p2p overlay routing protocols operating in a logical namespace with those of VANET routing protocols operating in a physical namespace. By this means, PAV has inherited all the advantages of P2P networking technology in sustaining highly dynamic networks and maintaining network scalability. Also introduces a series of optimizing mechanisms to solve the detouring problem of structured P2P overlay network and to further improve routing efficiency. The issue is in state-efficiency" trade-off between routing table and network parameters.

Victor Cabrera, Francisco J. Ros, Pedro M. Ruiz [7] proposed "Simulation-based Study of Common Issues in VANET Routing Protocols" The method forwarding loop ratio (FLR) was used to route data messages with the temporary loops. DTN is adopted by some vehicular routing protocols uses simulation based analysis. T-seconds-wait-rule to find expressions for the exact delay time and delivery ratio. The issue is that it is possible to calculate the delay time and delivery ratio when a car sends a packet to a location k-1 instead of k cars ahead.

III. PROPOSED WORK

The proposed DPRAODV scheme provides the conditional vehicle anonymity for privacy preservation with traceability for the non-repudiation in case that malicious vehicles abuse anonymous authentication techniques to achieve malicious attacks. The method includes encrypting public-key cryptography (PKC) to the pseudonym generation, which ensures a legitimate third party to achieve non-repudiation of vehicles by obtaining vehicle real IDs. The PKC-based adaptive pseudonym scheme by using self-generated pseudonyms instead of real-world IDs in authentication for privacy preservation and non-repudiation, in which the update of the pseudonyms depends on vehicular demands. The scheme shows the feasibility of ACPN with respect to the system analysis on the objectives, such as authentication,non-repudiation,time constraint, independency, availability and integration.

A. V2V authentication

Vehicular network within a radio frequency form a group. They elect their leader based on some criteria who is then responsible for generating a group public and private key pair. Each vehicle is equipped with a tamper resistant OBU which is capable of generating public/private keys pairs and also self-certifies the generated keys based on one way hash chaining technique. Any vehicle joins the group communicates the group leader, authenticates itself to obtain the group key. Later, the vehicle uses the group key to send traffic related messages to the group leader who is responsible for batch verifying the authenticity of the message from different sources and one hop broadcast them to reduce the computation overhead on message verification in each vehicle. In addition the proposed scheme adopts the k-anonymity approach to protect user identity privacy, where an attacker cannot associate a message with the sending vehicle. Extensive analysis and simulations show that the proposed architecture provides an efficient and fully self-organized system management for car-to-car communication without the need of any external infrastructure. The communication between vehicle to infrastructure is possible either with or without road side unit.

$$SD = 1 - \frac{\mathrm{De}}{\mathrm{Df}}$$

To find shorter distance between source and destination node for transmission,

Here,

SD : Shorter Distance.
D$_e$: Distance from edge to target node.
D$_f$: Distance from source to target node.
$\frac{\mathrm{De}}{\mathrm{Df}}$: Adjacency of next hop.

B. PKC based pseudonym generation

When a vehicle needs to report an event, it randomly picks one pseudonym and signs the message with it, using public key cryptography (PKC). This makes it difficult to track a vehicle simply by observing the pseudonym it uses; thus privacy is preserved. In trying to preserve privacy, these schemes have been shown to be susceptible to attacks. This is because a malicious vehicle may broadcast multiple messages, each signed with a different pseudonym selected from the given pool. Since other vehicles and RSBs should not know the pseudonym-pool for each vehicle, they will be unable to recognize that the messages are from one vehicle solves this problem by preloading vehicles with temporary pseudonyms, each having an "expiry time". Vehicles are expected to obtain new pseudonyms from an RSB right before its current pseudonyms expire. This can be a strong assumption since vehicles may not be near an RSB (to download new pseudonyms) when its current pseudonym is about to expire.

C. Cross RSU V2V authentication

The cross-RSU V2V authentication is required when a vehicle receives an authentication message from another vehicle, whose pseudonym does not appear in its storage. In this case, the vehicle can query the RSU, which consists of the following steps. We take an example to illustrate this approach, where vehicle w is aiming to authenticate with vehicle u with its online SIG wonline. On the receiving authentication message from w, the vehicle u checks its storage for the pseudonym and the POI set of w. If the information does not appear in vehicle u's storage, vehicle u transmits its query message q.y. of authenticity to the nearest RSU, which includes the POI set of vehicle w in the form of (PSw/SIGw offline(PSw)/IDr), signed with the IBS SIGu. After receiving the queried message, the current RSU queries other RSUs or the RTA via secure channels to check if the POI set is authenticated. Afterwards, the current RSU replies the query result q.r. back to the querying vehicle u, whether or not the POI set is authenticated. When a vehicle enters a new region, first it has to go to the current RTA for registration. At a RTA, a vehicle can update or replenish its RSU pool and the certified domain parameters for authentication.

D. Attack on authentication

In the proposed ACPN, authentication is guaranteed by digital signatures, which bound messages to vehicular pseudonyms and consequently the corresponding identities. The signature verification and the query process in the peer vehicles (sometimes via the RSUs) for the paired digital signatures and vehicular pseudonyms protect the vehicles from the adversaries pretending other entities in ACPN. Since the acceptable digital signatures are specifically bounded to the PKC-based vehicular pseudonyms, the adversaries cannot trigger either the impersonation attacks or the Sybil attacks without obtaining the corresponding vehicular pseudonyms of the digital signatures.

E. Attacks on privacy and non-repudiation

The adoption of pseudonyms in VANET communications conceals real world identities of vehicles such that peer vehicles and RSUs cannot reveal the sender's real-world identity of a specific message; however, it is still able to authenticate the sender. By frequently updating the pseudonyms during communication in the general UVC of VANETs, the proposed ACPN defends legitimate vehicles against density revealing and location tracing. In ACPN, the message non-repudiation is achieved from the decrypted value of the vehicle pseudonyms by the private key of the PKC scheme. Since the secure interactions with the RTA or RSUs are proposed in ACPN, we can claim that the authorized third parties (e.g., the police) can link pseudonyms with the identity of a vehicle with the validated digital signature at any time on demand, which protect the authorized parties from the repudiation attacks. That has a long duration and minimal power consumption.

1. Detection, Prevention and Reactive AODV (DPRAODV) Scheme:

In this scheme used a new control packet called ALARM is used, while other concepts are the dynamic threshold value. Unlike normal AODV, the RREP Sequence Number is also checked whether it is higher than the entrance value or not. If the value of RREP sequence Number is higher than the entrance value, the sender is said to be as an attacker and is updated it to the black list. The ALARM is sent to its neighbors who has the black list, thus the RREP from the malicious node is blocked but is not processed. On the other hand, the dynamic entrance value is changed by finding the average of destination sequence number between the sequence number and RREP packet in each time slot. According to this technique, the black hole attacks not only can be detected but also prevented by updating the entrance value which responses the pragmatic network atmosphere. The pros of DPRAODV scheme is that it achieves an obviously higher packet delivery ratio than the actual AODV, except for it takes a little bit higher routing overhead and end to end delay. But DPRAODV simply finds the multiple black holes rather than cooperative black hole attack.

2. Neighborhood based Routing Recovery Scheme (NBRRS)

In this detection technique uses a neighborhood-based method to identify the black hole attack, and a routing recovery protocol to construct the accurate path. This technique is used to identify the nodes which are unproven. In this technique, source node sends a Modify Route Entry control packet to destination node to restore (renew) routing path in the recovery protocol. In this technique, not only a higher throughput and lower detection time are achieved, but the accurate detection probability is also acquired. The main constraint of this scheme is that it becomes ineffective when the attacker agrees to counterfeit the forged reply packets.

3. Distributed Cooperative Mechanism (DCM)

DCM is used to resolve the collaborative black hole attacks in AODV routing protocol. The DCM consists of four steps includes

Step 1: Data gathering phase

An inference table is constructed and maintained by each node in the network. The condition to be evaluated in this phase includes each node checks the information of overhearing packets to determine whether there is any malicious node or not. If there is one mistrustful node, the detected node begins the local detection phase.

Step 2: Local detection phase

To identify whether there is a probable black hole. The initial detected node sends a check packet to inquire the cooperative node. The packet sends to all active communication noode in the environment. If the examination value is found positive, the doubtful node is regarded as a normal node. Else the initial detection node initiates the co-operative detection phase.

Step 3: Co-operative detection phase

Deals with the broadcasting and notifying all one-hop neighbours to participate in the decision making. An inhibited broadcasting algorithm is used to confine the warning range within a fixed hop count. The neighbourhood based routing mechanism helps to construct the path with the hop count measurements as one and combine nodes for detection phase.

Step 4: Global reaction phase

To set up a notification structure, and sends warning messages to the whole network. This mode will react to incorrect data and to malicious node included in communication. There are reaction modes in global reaction phase. There is a lot of communication overhead wasted. Thus the DCM is incorporated to provide better communication range. Each node is only concerned about its own black hole list and organizes its transmission route in other mode. DCM has a higher data delivery ratio and detection rate even if there are various black hole nodes which is the main advantage of this technique.

IV. CONCLUSION

Security and privacy are two important issues in VANETs. In this paper DPRAODV scheme has been developed to provide secure communication between V2V and V2R. The process includes a control packet called alarm in the AODV scheme to add additional security features. The packet will detect and prevent the malicious node and react to the incorrect data and notify it to the whole network. This scheme helps in the high packet delivery ratio with the secure and fast transmission as per the requirement of low latency safety application.

REFERENCES

[1] Jie Li, Huang Lu, Mohsen Guizani “ACPN: A Novel Authentication Framework with Conditional Privacy- Preservation and Non-Repudiation for VANETs” in Parallel and Distributed Systems, IEEE Transactions on (Volume:PP , Issue: 99) 25 February 2014.

[2] Qingzi Liu, Qiwu Wu, Li Yong "A hierarchical security architecture of VANET” Cyberspace Technology (CCT 2013), International Conference on 23-23 Nov. 2013.

[3] Ren-Junn Hwang, Yu-Kai Hsiao and Yen-Fu Liu “Secure communication scheme of VANET with privacy preserving" in parallel and distributed systems (ICPADS), IEEE 17th International Conference on 2011.

[4] Xi Yu , Huaqun Guo and Wai-Choong Wong “A reliable routing protocol for VANET communications"in Wireless Communications and Mobile Computing, 7th International Conference (IWCMC)on 4-8 July 2011.

[5] Jan Janech, Stefan Toth “Communication in distributed database system in the VANET Environment" in Computer Science and Information Systems (FedCSIS), Federated Conference on 8-11 Sept. 2013.

[6] Song Haibin, Meng Qi, Men Aidong “P2P computing in design of VANET routing protocol" in Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on 21-25 Sept. 2007.

[7] Victor Cabrera, Francisco J. Ros, Pedro M. Ruiz “Simulation-based study of common issues in VANET routing protocols” in Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th 26-29 April 2009