Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Verifier Approach in VANET

MohanaPriya A
PG Scholar, Department of CSE,
Sri Shakthi Institute of Engineering & Technology,
Anna University, Chennai, India

Dr. Kannammal K E
Professor, Department of CSE,
Sri Shakthi Institute of Engineering & Technology
Anna University, Chennai, India

Abstract -- VANETs are subset of mobile ad hoc networks (MANETs) in which vehicles act as nodes. Vehicles are equipped with wireless On-Board Units (OBUs), to perform communication. In VANET, Message authentication, a fundamental issue, is traditionally defined as the task of authenticating a message in terms of integrity and identification check. To deal with message authentication issue, a cooperative approach, known as cooperative message authentication scheme is introduced. The scheme, however, has been explored to alleviate authentication overhead on individual vehicle and thereby eliminating redundant authentication efforts on the same message by different vehicles. To further resist certain attacks, including Free-riding attacks and linkability attacks, and encourage cooperation among the network, the scheme uses an evidence-token mechanism. In the existing system, Trusted Authority (TA) is responsible for verifying the evidences sent from the vehicles, via the Road-Side Units (RSUs). In this project a Verifier Approach is introduced to remove the direct involvement of Trusted Authority. Among the participating vehicles one vehicle will be acting as a verifier, it performs the role of TA. This highly helps to reduce the authentication overhead and workload. Also this approach overcomes insider and outsider attacks.

Keywords -- Cooperative authentication, free-riding attacks, insider & outsider attacks, vehicular ad hoc networks (VANETs), Verifier.

I. INTRODUCTION

Vehicular Ad-hoc NETworks (VANET) are self-organizing networks established among vehicles equipped with communication facilities. For a rich set of applications implementing Intelligent Highways, like application related to road safety, traffic monitoring and management, road disaster mitigation etc. the road side infrastructure plays a vital role for any VANET. This is the reason that efficient communication between the vehicles and the road side infrastructure is required. VANET is composed of three components wireless On Board units (OBUs), Roadside units (RSUs) and a Trusted Authority (TA). The communication between Vehicles and RSUs is by using a Dedicated Short-Range Communications technique (DSRC). A fundamental security problem in VANET is message authentication. Message authentication is achieved by two security checks, i.e., an integrity check and identification check. Message authentication must be implemented to allow vehicle users to differentiate reliable information from unreliable information. By using digitally sign messages, this problem can be solved. This solution allows the receiver to identify the sender and prevents the message contents from being modified in transit. Without the direct involvement of trusted authority, an efficient cooperative message authentication scheme is adopted. With this scheme, a group of neighboring vehicle users; with minimal inter-vehicle coordination, reduces authentication effort of different vehicles working on the same message. It results in rich cooperation and resists free riding attacks.

II. VANET TECHNOLOGY

VANETs are subgroup of Mobile Ad hoc Networks (MANETs) with the distinguishing property that the nodes are vehicles like cars, trucks, buses and motorcycles. The primary goal of VANETs is to increase road safety. To achieve this, the vehicles act as sensors and exchange warnings**.** A VANET uses moving cars as nodes in a network to create a transportation network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. In VANET, rather than moving at random, vehicles tend to move in an organized fashion.

III. RELATED WORK

A. Privacy Preserving Protocol

X. Lin, X. Sun, P.-H. Ho, and X. Shen, has presented a secure and privacy-preserving protocol for vehicular communications called Group Signature and Identity (ID)- based Signature (GSIS) [2]. According to them, security problems are divided into two fold: Security and Privacy Preservation between the OBUs and OBUs and between the OBUs and the RSUs. Group signature was used to secure the communication between the OBUs and OBUs, whereas, a signature scheme using ID-Based Cryptography (IBC) was adopted in the RSUs to digitally sign each message launched

by the RSU to ensure its authenticity. With group signature, security, privacy and efficient traceability can be achieved. On the other hand, the management complexity on the public key and the certificate can be reduced with the ID- based signature. To enhance the performance and to reduce the communication overhead, an efficient broadcast authentication protocol called TESLA (Timed Efficient Stream Loss- Tolerant Authentication) has proposed.

B. RSU-Aided Message Authentication Scheme

A novel RSU- aided message authentication scheme [5] was presented in the year 2008 by C. Zhang to reduce the communication overhead imposed by the previous paper. When the traffic density becomes larger, a vehicle cannot verify all signatures of the messages sent by its neighbors in a timely manner, which results in message loss. A novel RSU-aided messages authentication scheme, called RAISE was introduced. With RAISE, roadside units (RSUs) are responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles. In VANETs, vehicles are equipped with wireless On-Board Units (OBUs), which communicate with each other or with Roadside Units (RSUs) with a Dedicated Short Range Communications (DSRC) protocol. According to DSRC, each vehicle periodically broadcast its routine traffic-related information containing its current speed, location, deceleration/acceleration, etc. With the received information, other drivers can make an early response in case of exceptional situations such as accidents, emergent braking, and traffic jams. RAISE explores the unique features of VANETs by employing RSUs to assist vehicles in authenticating messages. Each IVC message will be attached with a short keyed Hash Message Authentication (HMAC) code generated by the vehicle, and the corresponding RSU in the range will verify these HMACs and disseminate the notice of authenticity to each vehicle.

IV. EXISTING SYSTEM

In the existing work, all vehicles relied on a Trusted Authority (TA) for controlling the overall network which leads to the need of a centralized authority. It is infeasible for any attacker to compromise. Thus, creates a burden to message authentication scheme and overload to Trusted Authority. Since TA acts as administrator that maintains message authentication and management of network, TA load increases due to large number of received messages.

V. PROPOSED SYSTEM

In the proposed work, Verifier is a device that handles the role of Trusted Authority. One of the vehicle inside the VANET acts as verifier for every token change. Selecting verifier is one of the complex tasks in this process. Verifiers are chosen in such a way by calculating the rank of each participating vehicles in the current time slot. This method uses efficient encryption methods and some features of Token. The main concept in Verifier mechanism is to remove the direct involvement of Trusted Authority and distribute the work among the vehicle users. Verifier approach maintains a list which comprises the authorized nodes that currently participating in the VANET network. But the previous studies focus mainly on security concerns, not to reduce workload. So to reduce the authentication overhead on individual vehicles and shorten the authentication delay, the cooperative authentication scheme is used. It maximally eliminates redundant authentication effort on the same message by different vehicles. To enhance this scheme and to reduce the authentication effort by a central authority with the help of evidence token mechanism, Verifier approach is introduced. But here the evidence report is sent to Verifier vehicle instead of Trusted Authority.

A. Evidence Token Mechanism

A vehicle authenticates some of the original signatures that are received and generates an integrated signature at a time slot. It then creates an evidence for its authentication effort, which includes the time slot, the number of cooperative vehicles x, the number of original signatures y, and the number of original signatures $v_{x,y}$ that have been included in the integrated signature. It transmits the integrated signature and the evidence to others though verifier vehicle. Fig. 1 explains evidence token mechanism.

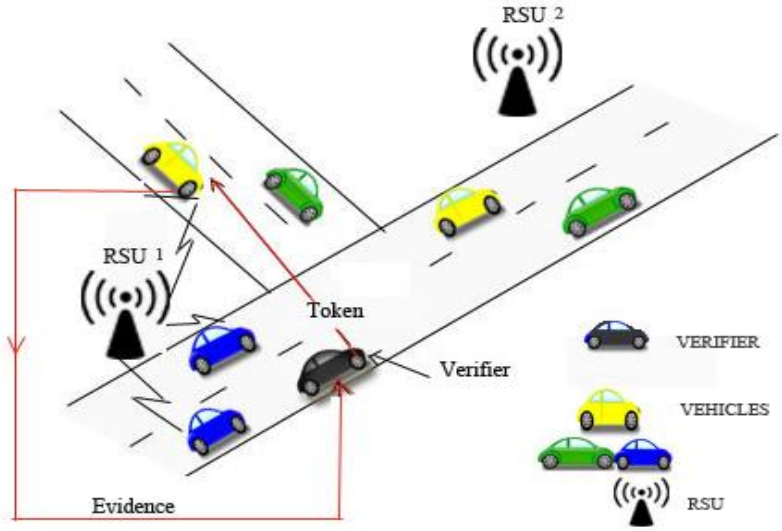

Fig.1 Evidence Token Mechanism

B. Security Threats

This Mechanism resists five different types of security threats.

*1) Insider Threat***:** This type of attackers is an authentic user of the network and have detailed knowledge of network. Insider attacker might have access to insider knowledge and this knowledge will be used for understanding the design and configuration of network. When they have all information about the configuration then it's easy for them to launch attacks and create more problem as compare to outsider attacker. It can create problem in the network by changing the certificate keys. In general, insider attacker is the right man doing the wrong job in the network.

2) Outsider Threat: In general, external attackers (outsider) are mainly outside the VANET who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network.

3) Linkability attack: Authentication linkability helps the TA to identify misbehaving users. In the linkability attack, a malicious user falsely claims that it has verified multiple message–signature pairs, and it also disables the Verifier to trace its unique identifier to avoid being punished.

4) Free-riding attack without authentication effort (or passive free-riding attack: Passive free-riding attack is launched by a malicious user who aims to enjoy the authentication efforts of other users at no cost, for e.g., by passively listening to the information sent from nearby users. It reduces the attacker's authentication overhead and breaks the fairness among users.

5) Free-riding attack with fake authentication effort (or active free-riding attack: Active free-riding attack is launched by an active malicious user who participates in the cooperative authentication protocol by generating fake authentication efforts. In a cooperative authentication environment, the attacker checks the authentication effort of other users and combines them to forge an authentication effort for itself. By doing so, it does not authenticate any original message but provide valid verification efforts because these signatures have been checked by others. The active attack is more intelligent than the passive attack. It can be hardly detected by nearby users or the TA.

VI. VERIFIER APPROACH

The proposed approach abolishes the role of TA and it focuses on the vehicles for all tasks. Vehicles acts as verifier and selecting verifier is a complex task. The verifier is selected according to the highest rank calculation. Each vehicle should have a verifier. Initially, set rank for all nodes as zero and generally first node in the network is chosen as the verifier for the first time.

Consider a network with three nodes "A", "B", "C". So, first node "A" is set as verifier initially. If "B" sends a message to "C" and "C" verifies the message for authorization, if the result is correct, then increment the rank of "B" by 1. Otherwise, decrement the rank by 1 or remove from the buddy list and mark as unauthorized node. Similarly, check for all other nodes and calculate the highest rank for the particular slot. At each time verifier will be different. The highest rank node will be the verifier for the other nodes and also for itself. The following algorithm is used for Verifier selection approach.

```
Verifier_Selector()
{
start
initially verifier->node list->first node
    1. Each node in network checks
  a. Each evidence in nodes' evidence list
      {
        if(evidence->checked result is true)
                evidence->node->rank=evidence->node->rank+1
                 this->node->buddyList->add(evidence->node)
         else
                evidence->node->rank=evidence->node->rank-1
                    this->node->buddyList->remove(evidence->node)
      }
    2. at next time interval
     a. Each node generates a key
  b. create a verifierpacket with generated key+node->rank
     c. broadcast this packet to all trusted nodes.
    3. at each node
     a. checks all the verifierpackets
     b. find out the largest ranked packet
            node->verifier=verifierpacket->node
            encryption key->verifierpacket->key
    4. at verifier
       a. Verifies all the evidences
       b. Provide trusted certification for nodes
end }
```


VII. SIMULATION RESULTS

In Fig. 2, the authentication effort per vehicle is reduced upon increase in number of vehicle. In case, if the number of vehicle is 5 then, every user can verify 2 messages each. In case of 10 vehicles, each user verifies one message at a time. As the total number of users' increases, the effort per vehicle gradually decreases. The line shows the performance of the cooperative authentication scheme.

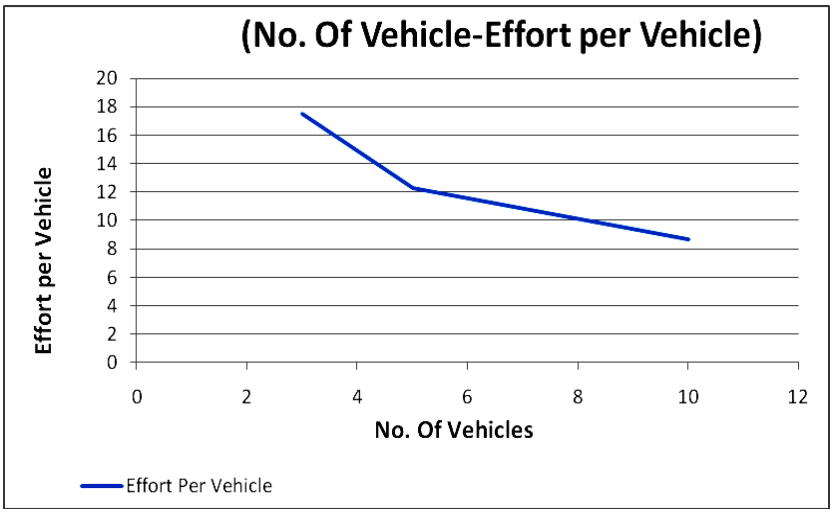

Fig. 2: No. of Vehicle Vs Effort per Vehicle (Units in Secs)

In Fig. 3, it clearly shows that the overhead is reduced compare to the existing system. Because the involvement of Trusted Authority is completely removed by introducing verifier among the vehicles.

.

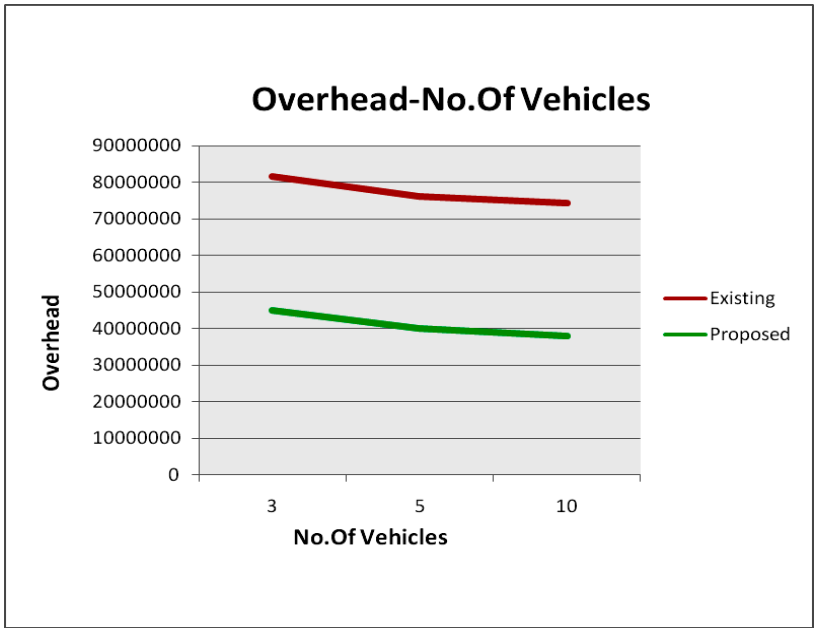

Fig. 3: Overhead (Units in ns) Vs No.of.Vehicles

VIII. CONCLUSION

In this paper, we have presented a novel cooperative message authentication scheme for VANETs. Through the proposed scheme, vehicle users can cooperatively authenticate a bunch of message–signature pairs with the Removal of a TA. In addition, the linkability attack, the free-riding attacks without authentication efforts (or passive free-riding attack), the free-riding attacks with fake authentication efforts (or active free-riding attack), insider threat, outsider threat. The Verifier strategically adjusts the valid period (lifetime) of tokens for each vehicle user based on the collected evidence, thereby periodically controlling vehicle users' cooperation capabilities. The simulation results have confirmed that the proposed scheme can significantly reduce the computational overhead on vehicle users for authenticating signatures and enable the Verifier to flexibly balance the advantages that a vehicle user takes from others and the efforts it offers to others during cooperative authentication.

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers, whose insightful comments helped us to improve the quality of the paper.

REFERENCES

[1] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "*Efficient and robust pseudonymous authentication in vanet,*" in Proceedings of VANET‟ 07, Montreal, Quebec,Canada, pp. 19–28, September 2007.

[2] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "*GSIS: A secure and privacy preserving protocol for vehicular communications*," IEEE Transformation Vehicular Technology, vol. 56, no. 6, pp.3442–3456, Nov. 2007.

[3] H. Zhu, X. Lin, R. Lu, Pin-Han Ho, X. Shen "*AEMA: An Aggregated Emergency Message Authentication Scheme for Enhancing the Security of Vehicular Ad HocNetworks*", IEEE Trans, pp. 1436-1440, May 2008.

[4] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," in Proc. 27th IEEE INFOCOM, Phoenix, AZ, USA, pp. 246–250, 2008.

[5] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "*RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks*," in Proc. IEEE ICC, Beijing, China, pp. 1451–1457, May 2008.

[6] C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen, "*An efficient message authentication scheme for vehicular communications*," IEEE Trans. Vehicle Technology, vol. 57, no. 6, pp. 3357-3368, 2008.

[7] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "*A distributed key management framework with cooperative message authentication in VANETs*," IEEE J. Sel. Areas Communication, vol. 29, no. 3, pp. 616–629, Mar. 2011.

[8] X. Lin, R. Lu, X. Liang, and X. Shen, "*STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs*," in Proc. 30th IEEE INFOCOM, Shanghai, China, pp. 2147–2155, 2011.

[9] R-X Lu, X-D Lin, T-H Luan, "*Pseudonym changing at social spots: an effective strategy for location privacy in VANET*", IEEE Transaction on Vehicular Technology, vol.61, no. 1, pp.86-96, Jan, 2012.

[10] X Jia, X. Yuan, L. Meng, L. Wang, "*EPAS: Efficient Privacy-preserving Authentication Scheme for VANETs-based Emergency Communication*", journal of software, vol. 8, no. 8, august 2013.

[11] X. Liang, R. Lu, X. Lin, and X. Shen, "*PPC: Privacy-preserving chatting in vehicular peer-to-peer networks*," in Proc. 72nd IEEE VTC, Ottawa, ON, Canada, pp. 1–5, 2010.

[12] M. Raya and J. P. Hubaux, "*Securing vehicular ad hoc networks*," J. Computer Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[13] "Vehicle safety communication project final report. Appendix H: WAVE/DSRC security," Nat. Highway Traffic Safety Admin., Washington, DC, USA, Apr. 2006.

[14] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "*TSVC: Timed efficient and secure vehicular communications with privacy preserving*," IEEE Trans. Wireless Communication., vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

