A Secure and Efficient Vehicle Communication Scheme Using FP Tree Algorithm in Vehicular Ad Hoc Network

Punam R. Sathe\textsuperscript{1}, Ganesh N. Dhanokar\textsuperscript{2}

M. E Student, Department of Computer, G.H.Raisoni College of Engineering, Jalgaon, 
North Maharashtra University India\textsuperscript{1}

Department of Information Technology, G.H.Raisoni College of Engineering, Jalgaon, 
North Maharashtra University India\textsuperscript{2}

ABSTRACT: Ordinarily, authentication in vehicular ad-hoc networks (VANETs) customs Public Key Infrastructure (PKI) to verify the truth of messages and the identity of message senders. The issues considered in the authentication schemes include the level of security and computational efficiency in verification processes. However, these schemes may not work well in VANET scenarios. For instance, it is difficult for a Roadside Unit (RSU) to verify each vehicle’s signature sequentially when a large number of vehicles emerge in the coverage areas of an RSU. In proposed system we prefer Frequent Pattern Tree Algorithm for communication In VANET, algorithm is less time consuming. Mostly proposed schemes focus on guarantee the security and privacy of VANET information.

KEYWORDS: Message Authentication; Proxy Vehicle; Vehicular adhoc network(VANET).

I. INTRODUCTION

VANET (Vehicular Ad-hoc Network) may be a form of Eduard MANET (Mobile Ad-hoc Network), that may be a next-generation networking technology that has communication between vehicles or between a vehicle associate decreed an RSU (Road aspect Unit) victimization wireless communication. Transport ad-hoc networks (VANETs) have attracted intensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. VANETs include entities together with On-Board Units (OBUs) infrastructure Road-Side Units (RSUs). Since vehicles communicate through wireless channels, a range of attacks like injecting false data, modifying and replaying the disseminated messages may be simply launched. A security attack on VANETs will have severe harmful or fatal consequences to legitimate users. Consequently, making certain secure transport communications may be a should before any VANET application may be place into apply.

II. RELATED WORK

An Expedite Message Authentication Protocol (EMAP) for VANETs, which exchanges the inefficient CRL check technique by an effective revocation checking process. Single-hop broadcast, multiple forwarding of packets, store the message in different RSU areas\textsuperscript{[14]}. EMAP customs a profligate HMAC function and novel key circulation scheme paying probabilistic arbitrary key supply \textsuperscript{[1]}. Based on decentralized CA, 2FLIP only needs numerous dangerous lightweight hashing methods and a fast MAC action for message signing and verification among vehicles \textsuperscript{[2]}. EMAP can reduction the message damage percentage due to the message confirmation interruption associated with the predictable authentication approaches using CRL\textsuperscript{[3]}. In addition, the RSU is able to autonomously prove the outputs since the verification function of the proxy vehicles \textsuperscript{[4]}. To check the message validity at RSU, a batch verification of all signed messages is being performed by RSU, which is known as Identity-based batch verification (IBV)\textsuperscript{[5]}. ID based signature scheme which consists of four algorithms namely setup, extract, sign and verify \textsuperscript{[6]}. The other vehicles can also make the message...
authentication and identity verification based on the techniques of chameleon hash, HMAC and Diffie-Hellman key exchange [13].

III. PROPOSED ALGORITHM

1 Trusted Authority:
- All works are simply distributed by Trusted Authority.
- Dynamic Keys are distributed by TA to all vehicles.
- Trace the both Identity (real, hateful) of Vehicle.

2 Dynamic Keys:
- 32 bit Dynamic keys.
- Assign to the vehicle.
- All vehicles having unique key.

3 Node (vehicle) link:
- Node is link with each other.
- Select the shortest path logically.

4 Attach Path:
- Physical path established.
- Path is ready to send the data.

5 Proxy Vehicle:
- Verify signature of vehicle
- After verification process data will be forwarded to RSU.
- Proxy vehicles which achieves batch authentication of communication and sends the outcome to RSU[22].

6 Road Side Units
- Accept data from proxy vehicle.
- All verified data will be forward to the trusted authority.

a) System parameter generation:
- The TA stores \( UV = \{ \text{RID}_i | 1 \leq i \leq n \} \). \text{RID}_i = \text{Real identity of the vehicle } \text{Vi}, \text{ where } \text{RID}_i \in G
- Given the bilinear limitations (\( P, q, G_1, G_2, e \)), the TA selects four unplanned numbers, i.e., \( s_1, s_2, s_3, s_r \in \mathbb{Z}_q^* \).
- The TA adds \( \text{PK}_1 = s_1P, \text{PK}_2 = s_2P, \text{ and } \text{SK}_r = s_3P. \text{SK}_r = \text{Key of RSU}. \)
- The tamper-proof device of each vehicle is in secret preloaded with the parameters \( \{ s_1, s_2, s_3 \} \).
- The RSUs are secretly preloaded with the parameters \( \{ \text{SK}_1r, \text{SK}_2r \} \).

b) Pseudonym and key generation:
1) The RSU computes \( \text{SK}_r = s_rRr \text{PRand PKr} = srP. \) Therefore, the private key of the RSU can be modeled as \( (\text{SK}_1r, \text{SK}_2r) \).
2) A vehicle, which is denoted by \( \text{Vi} \), chooses a random number \( \text{ri} \in \mathbb{Z}_q^* \).
3) Vi computes \( \text{ID}_1i = \text{riP} \text{and ID}_2i = \text{RID}_i \oplus H(\text{riPK}_1) \).
4) Vi computes \( \text{SK}_1i = s_1\text{ID}_1i \text{ and SK}_2i = s_2H(\text{ID}_1i\text{ID}_2i) \).

c) Publishing the system parameters:
The system parameters \( (P, q, G_1, G_2, e, PK_1, PK_2, PKr) \) are preloaded by each VANET member. The system initialization phase should keep private material confidentiality. First, the private master keys \( \{ s_1, s_2, s_3 \} \) are loaded into the vehicle’s tamper-proof device in the system parameter generation process. The tamper-proof device on vehicles, an adversary cannot extract any data stored in the device including key material, data, and code [12]. Second, the tamper-proof device is responsible for generating the identity \( (ID_1i, ID_2i) \) and the corresponding privacy key \( (SK_1i, SK_2i) \) in the pseudonym and key generation process.
IV. RESULTS

- **Network Module**

- **Dynamic Key Distribution**

---

**Fig. 1 Network**

**Fig. 2 Dynamic Key Distribution**
• Avoid Redundant Authentication

Fig.3 Avoid redundant Authentication

• Guest Proxy Handover details

Vehical 3 Key b5bf9545-fddc-4715-9b29-ef0dd010d08d - Assigned by Proxy Guest Proxy and same reported to RSU
Vehical 3 Handed over to Proxy Vehical 1.
VANET communication is one of most important communication media which is also important for our modern life. The working of Frequent Pattern Tree Algorithm is successfully completed with the help of the properties, those properties are first one is node link property and the another one is attach path property are useful in the data transmission. We successfully completed the proposed system over VANET with following results:

1) Avoid Redundant Authentication of Message.
2) Guest Proxy vehicles are easily handover Record to Regular Proxy.
3) Reuse of Dynamic key are avoided

REFERENCES


