MESSAGE AUTHENTICATION USING PROXY VEHICLES IN VEHICULAR AD HOC NETWORKS

SHAIK SUMREEN¹, SHAIK KARIMULLA²

¹ PG Scholar, Dept of CSE, QCET, Nellore, Andhra Pradesh, India
² Associate professor, Dept of CSE, QCET, Nellore Andhra Pradesh, India

ABSTRACT: Normally, authentication in vehicular ad-hoc networks (VANETs) uses Public Key Infrastructure (PKI) to verify the integrity 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. Most existing schemes focus mainly on assuring the security and privacy of VANET information. 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. To reduce the computational overhead of RSUs, we propose a Proxy Based Authentication Scheme (PBAS) using distributed computing. In PBAS, proxy vehicles are used to authenticate multiple messages with a verification function at the same time. In addition, RSU is able to independently verify the outputs from the verification function of the proxy vehicles. We also design an expedite key negotiation scheme for transmitting sensitive messages. It is shown from the analysis and simulations that an RSU can verify 26500 signatures per second simultaneously with the help of the proxy vehicles. The time needed to verify 3000 signatures in PBAS can be reduced by 88% if compared to existing batch-based authentication schemes.

EXISING SYSTEM

In Existing System, a security attack on VANETs can have severe harmful or fatal consequences to legitimate users. Consequently, ensuring secure vehicular communications is a must before any VANET application can be put into practice the CRL size in VANETs is expected to be large for the following reasons:

To preserve the privacy of the drivers, i.e., to abstain the leakage of the real identities and location information of the drivers from any external eavesdropper should be preloaded with a set of anonymous digital certificate, where the OBU has to periodically change its anonymous certificate to mislead attackers. Consequently, a revocation of an OBU results in revoking all the certificate carried by that OBU leading to a large increase in the CRL size.

OBU - On-Board Units

Disadvantage

In Existing system, vehicles communicate through wireless channels, a variety of attacks such as

- Injecting false information,
- Modifying and
- Replaying the disseminated messages can be easily launched.

PROPOSED SYSTEM

In this proposed scheme, each proxy vehicle plays an important role, which is adopted to authenticate multiple messages with the help of a verification function at the same time. In this way, the distributed computing can be used to shed the time-consuming centralized computing loads at RSUs. We also design a systematic and independent mechanism for RSUs to verify the output of the verification function from different proxy vehicles, by which an RSU can evaluate the validity levels of different messages in the same way as done in separate verification schemes. In addition, batch key negotiations can also be accomplished in the proposed scheme, in which an RSU can complete the batch process of vehicles’ key negotiations by broadcasting a single message.

It shows the main characteristic features of the proposed PBAS scheme. Specifically, the design requirements of the proposed PBAS can be summarized as follows:
1) The scheme should be designed to meet the computational efficiency requirements of VANETs.
2) The scheme should be designed to meet the general security requirements of VANETs, such as message integrity and authentication, privacy preservation, etc.
3) The scheme has the property that enables the verification process to continue even in the event that a small number of proxy vehicles have been compromised in VANETs.

ADVANTAGES

✓ Safety-related VANETs applications

MODULES

1. Conventional & Batch authentication
2. Certificate Revocation
3. Security model
   a) Message integrity & Authentication
   b) Identity privacy preserving and trace ability
   c) Resisting signature replay attacks
   d) Confidentiality
   e)

MODULES DESCRIPTION

1. CONVENTIONAL & BATCH AUTHENTICATION

   In this module, it shows and relationship between the integrity of messages and the validity of sender’s identities that a VANET user needs to verify the validity of the identity of a message sender before verifying the integrity of the messages it sends out. If the system designers focus only on the mechanisms to verify messages and ignore the importance associated with the verification of valid entities, a malicious participant could exploit many forged identities to disable VANET communications.

   Each message before its transmission, which is to perform the identity authentication that provides on-repudiation of attribution in multi-hop communications. Any receiver can use the signer’s public key to verify the identity of the message. To verify the messages from the vehicles outside the coverage of an RSU that the neighboring vehicles could work cooperatively to probabilistically verify only a small percentage of these message signatures.

   Rapid Certification Scheme (RCS), in which a VANET leader is responsible to collect the messages of n distinct vehicles, and then sends them to RSU. The RSU verifies the batch of messages. The RCS is able to reduce the transmission overhead of RSUs by integrating messages into batches.

2. CERTIFICATE REVOCATION

   In this module, approaches for efficient authentication in VANETs, but the revocation list will get very long when it is needed to check the time-consuming Certificate Revocation Lists (CRLs) introduced a protocol for V2V communications, called Expedite Message Authentication Protocol (EMAP), which uses keyed Hash Message Authentication Code (HMAC) technique to replace the CRL checking process. It can help to reduce the computation overhead compared to the conventional schemes employing CRL.

3. Security Model

   a. Message integrity & Authentication

      Messages sent by vehicles can be authenticated to prove that they are indeed sent by authorized entities without being modified or forged. Moreover, RSUs should have an ability to authenticate a large amount of signatures for many vehicles.

   b. Identity privacy preserving and trace ability

      The real identity of a vehicle should be kept anonymous, which is heterogeneous with the other pseudo identities. Any third party should not be able to reveal the real identity of a vehicle by analyzing multiple messages sent from it. However, when the vehicles send malicious
information, TA has an ability to reveal the real identities from the pseudo identities of the misbehaved vehicles.

c. **Resisting signature replay attacks**

Signature replay attack can be prevented by such a carefully designed scheme. The definition of a signature replay attack can be generalized as an attack that replays the signatures from a different vehicle for the intended or expected RSUs, thereby to fool the RSUs to believe that they have successfully completed the verification of the owner of these signatures.

d. **Confidentiality**

A server can establish a secure communication link with a requesting vehicle for subsequent communications. For instance, ISP and parking payments systems require that the session key negotiation process generates the keys for confidentiality of their transmitted messages.

### 3.2 ALGORITHMS AND FLOWCHARTS

#### Algorithm 1: The algorithm to identify malicious proxy vehicles

1. The batch of messages is marked as valid by \( \{ M = a \} \).
2. The batch of messages is marked as invalid by \( \{ M = b \} \).
3. Task (1): verify the message \( M_{proxy} \) from the proxy vehicle:
   - if \( M_{proxy} \) is valid then
   - Task (2): verify the result of the proxy vehicle:
   - if \( M = a \) || Eqn. (3) is held then
   - else if \( M = a \) || Eqn. (3) is not held then
   - if \( M_{proxy} \) is untrusted then
   - TA revokes the proxy vehicle.
   - else if \( M = b \) || Eqn. (3) is held then
   - if \( M_{proxy} \) is untrusted then
   - else
   - TA revokes the proxy vehicle.
4. else
5. TA revokes the proxy vehicle.
6. else
7. TA revokes the proxy vehicle.
8. else
9. TA revokes the proxy vehicle.
10. The result message is not from the authentic proxy vehicle.

#### Algorithm explanation:

RSUs can independently verify the results from the previous verification processes of the proxy vehicles, and then system can exclude false results and revoke malicious proxy vehicles. The verification in an RSU at the outputs from the proxy vehicles includes the following three tasks. Task (1) ensures that the originators of the messages is indeed the real proxy vehicle and there are no forwarding nodes actively modifying messages; Task (2) guarantees that the result from a proxy vehicle contains correct verification output through their batch verification phase; Task (3) revokes the proxy vehicle when RSU finds that it fails the process.

In task 3 the vehicles signatures are verified at RSU. Here it checks for each message with public key and the Identity.

Before the verification process, the proxy vehicle has obtained the public key (PK1, PK2), received the message \( M_i \), the signature \( \sigma_i \) of \( M_i \), and the pseudo identity \( (ID_{i1}, ID_{i2}) \) surrounding vehicle \( V_i \). Then, here we calculate the data of
each message and identity of vehicle can be calculated by the proxy vehicle, respectively. If these two terms are indeed identical, the integrity of all messages and the identities of senders of these messages are verified.

**CONCLUSION & FUTURE ENHANCEMENT**

PBAS makes use of vehicles’ computational capacity to reduce the burden of RSUs, where the proxy vehicles can authenticate multiple messages from the other vehicles. PBAS also provides RSUs with a systematic and independent mechanism to verify the messages from the proxy vehicles. In addition, PBAS can negotiate a session key with every other vehicle for the confidentiality of sensitive information. The evaluation model of PBAS showed that PBAS offers fault tolerance, which enables the scheme to continue operating properly even if a small number of proxy vehicles are compromised in VANETs. Moreover, we analyzed and compared the performance of PBAS with the other authentication schemes in terms of their computation and transmission overheads. We also used simulations to verify the efficiency of PBAS in realistic environments, showing that PBAS is a promising security scheme for efficient VANET authentication. In this work on PBAS,
we focused on cryptography algorithm under an assumption that any vehicle having completed system initialization can act as a proxy vehicle. However, it is crucial to make sure that these vehicles have incentives to serve for the others under the condition of efficient message delivery.

**FUTURE ENHANCEMENT:**

In the future, we will exploit the game theory to study incentives mechanism. The redundant authentication is another issue, in which different proxy vehicles may work on the same message. To minimize the redundant authentication events, we should design a selection strategy that combines extra computation resource utilization optimization and redundant authentication reduction.

**REFERENCES:**