AUTHENTICATION PROTOCOL USING EXPEDITE MESSAGE

SOWJANYA REDDY MALLREDDY,
Associate Professor,
Department of Computer Science and Engineering,

VARIKUPPALA GANESH,
Assistant Professor,
Department of Computer Science and Engineering,

Siddhartha Institute of Technology and Sciences,
Narapally, Hyderabad, Telangana – 500 088.

ABSTRACT

To secure vehicle ad hoc networks, the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) are utilised (VANETs). Checking if the sender's certificate is included in the current CRL and evaluating the authenticity of the sender's certificate and signature is how every PKI system authenticates a received message. In this research, we propose an Authentication Protocol Using Expedite Message for VANETs that replaces the time-consuming CRL checking method with an efficient revocation checking technique. Authentication Protocol Using Expedite Message also uses a new probabilistic key distribution that allows non-revoked OBUs to share and update a secret key safely. Authentication Protocol Using Expedite Message can drastically lower the message loss ratio owing to message verification latency when compared to typical authentication systems that use CRL. Through security research and performance assessment, Authentication Protocol Using Expedite Message has been demonstrated to be secure and efficient.

INTRODUCTION

Vehicle-based ad hoc networks (VANETs) are a subset of mobile ad hoc networks (MANETs) with the distinct feature that the nodes are vehicles such as cars, trucks, buses, and motorcycles. This means that node movement is limited by factors such as the road route, which includes traffic and traffic restrictions. Because node movement is restricted, it is logical to expect that the VANET will be supported by some fixed infrastructure that can provide access to stationary networks and aid with various functions. Slip roads, service stations, problematic junctions, and regions known for extreme weather will all have fixed infrastructure installed.

The IEEE 802.11p wireless communication standard is used in the North American DSRC standard to link nodes together. Messages must be transmitted through other nodes to communicate

with participants who are not within radio range (multi-hop communication). MANETs are constrained in terms of energy, space, and computation, whereas vehicles are not. The vast size of the VANET, as well as the possibility of very high node speeds (up to 250 km/h), make it far more complicated. The major purpose of the VANET is to improve road safety.

LITERATURE SURVEY

Vehicular communications (VC), as a new technology, poses a number of challenges that must be addressed. Security and privacy concerns are among them, and they are important for VC's mainstream acceptance. In this position paper, we are concerned about privacy and identity management in the context of new technologies. We highlight VC-specific difficulties and obstacles by taking into account the essential aspects of these systems. We regard them as part of a broader set of privacy protection measures, as well as ongoing development on VC standards and other mobile wireless communication technologies.

On a vehicular ad hoc network (VANET), a car's broadcasts during communication with other vehicles or roadside devices can be used to locate and track it. This type of tracking jeopardises the privacy of the vehicle's owner's whereabouts. We look at how to provide location privacy in the VANET by allowing vehicles to avoid being tracked through their broadcast emissions in this paper. We begin by outlining the unique characteristics of VANET that must be considered while creating location privacy solutions.

METHODOLOGY

We provide an expedite message authentication protocol Authentication Protocol Using Expedite Message that replaces the CRL checking technique with an efficient revocation checking mechanism using a fast and secure HMAC function. Authentication Protocol Using Expedite Message is suitable for VANETs and any network that employs a PKI system. To our knowledge, this is the first method for decreasing authentication latency on VANETs caused by CRL checks.

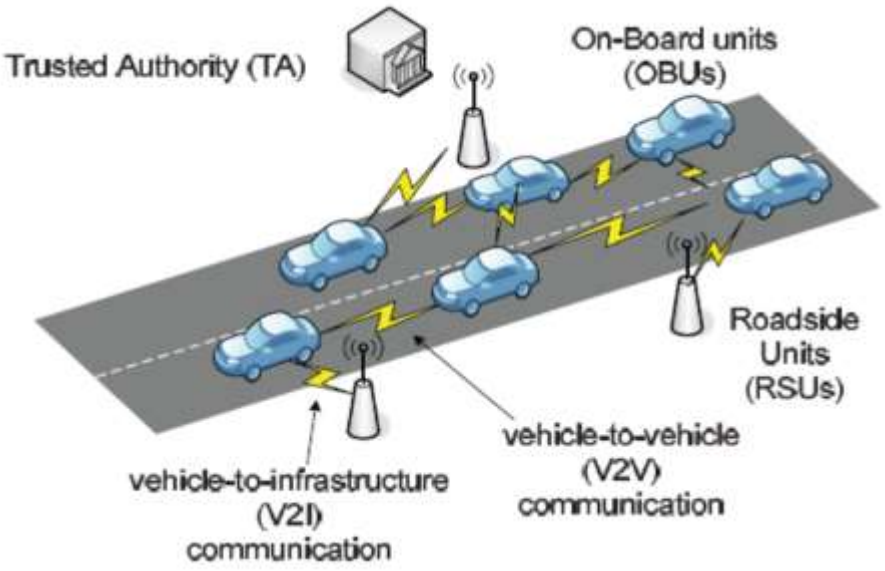

FIGURE 1: The proposed system architecture

ADVANTAGES OF THE PROPOSED SYSTEM:

• Authentication Protocol Using Expedite Message has the simplest computing complexity when compared to CRL checking methods that use linear and binary search algorithms.

• The number of messages confirmed using Authentication Protocol Using Expedite Message in less than 300 milliseconds is 88.7% more than the number of messages validated using linear and binary CRL checking, respectively.

• The suggested Authentication Protocol Using Expedite Message in authentication minimizes the end-to-end delay when compared to the linear or binary CRL checking techniques.

RESULT AND DISCUSSION

Authentication Protocol Using Expedite Message uses a probabilistic key distribution that allows non-revoked OBUs to securely communicate and update a secret key. AUTHENTICATION Protocol Using Expedite Message can drastically lower the message loss ratio owing to message verification latency when compared to typical authentication systems that use CRL. Through security analysis and performance evaluation, Authentication Protocol Using Expedite Message 's security and efficiency are demonstrated.

FIGURE 2: PAGE OF REGISTRATION

CONCLUSION

We suggested Authentication Protocol Using Expedite Message for VANETs, which replaces the time-consuming CRL checking method with a rapid revocation checking process using the HMAC function, which speeds up message authentication. The proposed Authentication Protocol Using Expedite Message employs a new key sharing technique that allows an OBU to update its compromised keys even if certain revocation messages were previously missed. Authentication Protocol Using Expedite Message also has a modular feature that enables it to work with any PKI system. It's also resistant to common attacks and outperforms traditional CRL-based authentication methods.

REFERENCES

1. M. Arjomandi, S. Agostino, M. Mammone, M. Nelson, and T. Zhou, "Classification of unmanned aerial vehicles," Mech Eng, vol. 3016, 2006.
2. L. Brooke-Holland, "Unmanned Aerial Vehicles (drones): an introduction," UK House of Commons Library Report, Standard Note SN06493 (25 April 2013), 2012.
3. R. Weibel and R. J. Hansman, "Safety considerations for operation of different classes of UAVs in the NAS," in AIAA 4th Aviation Technology, Integration and Operations (ATIO) Forum, 2004, p. 6244.
4. Colomina and P. Molina, "Unmanned aerial systems for photogrammetry and remote sensing: A review," ISPRS Journal of Photogrammetry and Remote Sensing, vol. 92, pp. 79-97, 2014.

5. J. William, "BEST LIST OF TOP 26 DRONE WITH CAMERA FOR 2018," in Drones Globe vol. 2018, ed, 2018.
6. E. Torun, "UAV Requirements and design consideration," Turkish Land Forces Command Ankara (Turkey)2000.
7. C. Soutis, "Fibre-reinforced composites in aircraft construction," Progress in Aerospace Sciences, vol. 41, pp. 143-151, 2005.