EXPEDITE MESSAGE AUTHENTICATION PROTOCOL FOR VEHICULAR AD HOC NETWORKS

GANESH NOMULA,
Associate Professor,
Department of Electrical & Electronics Engineering,

BOMMA GOPI,
Assistant Professor,
Department of Electrical & Electronics Engineering,

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

ABSTRACT

The Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) are used to secure vehicular ad hoc networks (VANETs). The authentication of a received message is performed in any PKI system by checking if the sender's certificate is included in the current CRL and validating the authenticity of the sender's certificate and signature. In this paper, we propose an Expedite Message Authentication Protocol (EMAP) for VANETs that uses an efficient revocation checking mechanism to replace the time-consuming CRL checking process. Furthermore, EMAP employs a new probabilistic key distribution that allows non-revoked OBUs to safely share and update a secret key. When compared to traditional authentication systems that use CRL, EMAP can dramatically reduce the message loss ratio due to the message verification latency. EMAP has been proven to be secure and efficient through security analysis and performance measurement.

INTRODUCTION

Vehicular ad hoc networks (VANETs) are a subclass of mobile ad hoc networks (MANETs) with the distinguishing attribute that the nodes are vehicles such automobiles, lorries, buses and motorbikes. This means that variables such as the road course, which includes traffic and traffic laws, limit node movement. Because of the limited node movement, it is reasonable to assume that the VANET will be backed by some fixed infrastructure that can offer access to stationary networks and assist with various functions. The fixed infrastructure will be placed at high-risk areas such as slip roads, service stations, dangerous crossroads, and areas known for severe weather.

The North American DSRC standard, which uses the IEEE 802.11p standard for wireless communication, is intended to be used to connect nodes. Messages must be passed by other nodes to allow communication with participants who are not within radio range (multi-hop communication). Vehicles are not constrained by the same rigorous energy, space, or computing limitations as MANETs are. The potential for very high node speeds (up to 250 km/h) and the VANET's huge size make it much more difficult. The major purpose of the VANET is to improve road safety. To do this, the vehicles operate as sensors, exchanging warnings or telematics data (such as current speed, location, or ESP activity) that allows drivers to react quickly to unusual and possibly dangerous conditions such as accidents, traffic jams, or glaze.

LITERATURE SURVEY

Vehicular communications (VC), an emerging technology, involves a variety of technological issues that must be solved. Among them, security and privacy concerns are critical for VC's widespread acceptance. We are concerned with privacy and identity management in the context of these technologies in this position paper. Taking into account the key elements of these systems, we highlight VC-specific concerns and obstacles. We see them in the context of broader privacy protection measures, as well as ongoing work on VC standards and other mobile wireless communication technologies.

It is feasible to find and track a car on a vehicular ad hoc network (VANET) based on its broadcasts during communication with other vehicles or roadside equipment. This form of tracking puts the vehicle's user's location privacy at risk. In this work, we look at how to provide location privacy in the VANET by allowing vehicles to avoid their broadcast transmissions from being tracked. We begin by identifying the distinct properties of VANET that must be taken into account while developing appropriate location privacy solutions. We present CARAVAN, a location privacy strategy based on these insights, and evaluate the privacy enhancement achieved in the face of a global adversary and some existing standard VANET application limitations.

METHODOLOGY

In this research, we provide an expedite message authentication protocol (EMAP), which uses a fast and secure HMAC function to replace the CRL checking procedure with an efficient revocation checking mechanism. EMAP is appropriate for VANETs as well as any network that uses a PKI scheme. This is, to our knowledge, the first approach for reducing the authentication latency caused by CRL checks on VANETs.

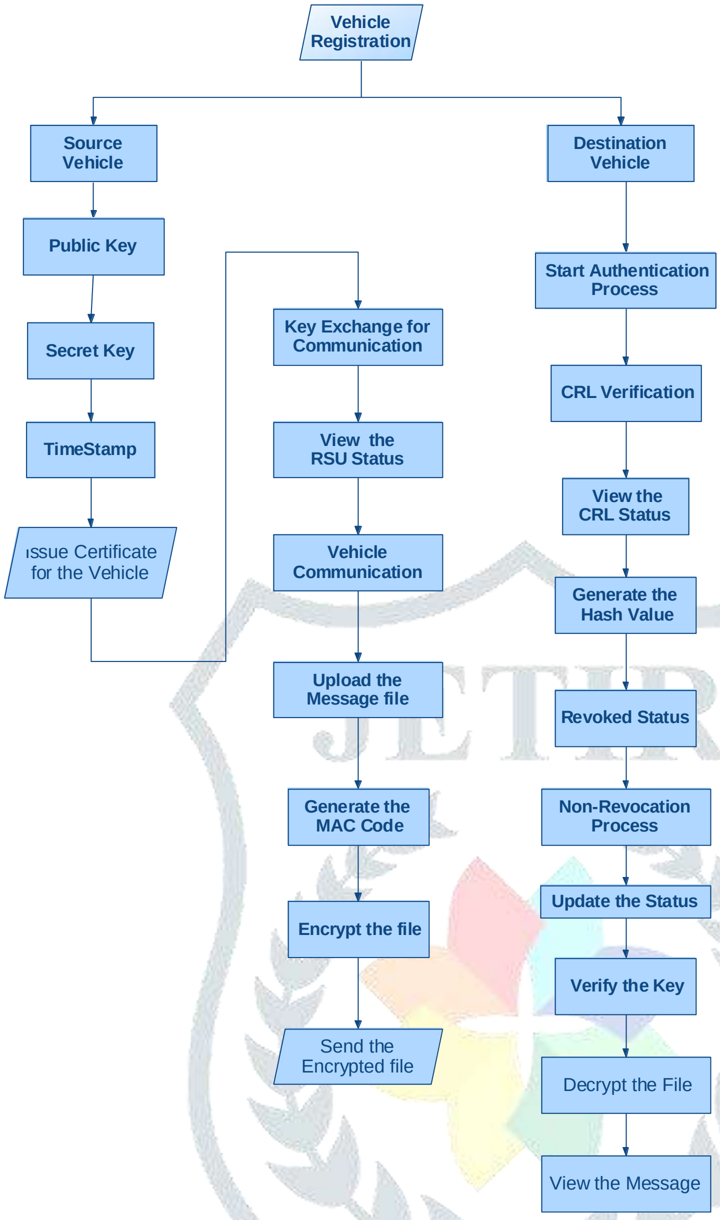

FIGURE 1: PROPOSED SYSTEM WORK FLOW

ADVANTAGES OF THE PROPOSED SYSTEM:

- When compared to CRL checking methods that use linear and binary search algorithms, EMAP has the simplest computing complexity.
- The number of messages that can be confirmed using EMAP within 300 milliseconds is 88.7% higher than the number of messages that can be validated using linear and binary CRL checking, respectively.
- When compared to the linear or binary CRL checking processes, the suggested EMAP in authentication reduces the end-to-end delay.

RESULT AND DISCUSSION

EMAP employs a unique probabilistic key distribution that allows non-revoked OBUs to share and update a secret key in a secure manner. When compared to traditional authentication systems that use CRL, EMAP can dramatically reduce the message loss ratio due to the message verification latency. EMAP's security and efficiency are demonstrated through security analysis and performance evaluation.

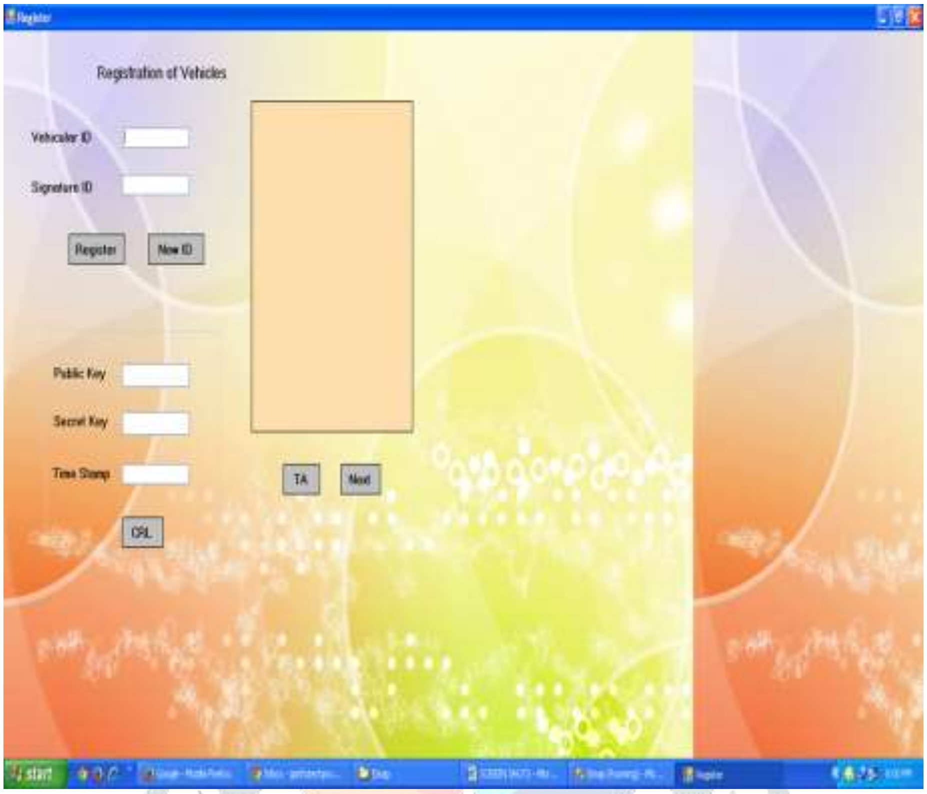

FIGURE 2: REGISTRATION PAGE

CONCLUSION

We have proposed EMAP for VANETs, which expedites message authentication by replacing the time-consuming CRL checking process with a fast revocation checking process employing HMAC function. The proposed EMAP uses a novel key sharing mechanism which allows an OBU to update its compromised keys even if it previously missed some revocation messages. EMAP also includes a modular feature that allows it to be integrated with any PKI system. Furthermore, it is immune to common assaults while outperforming traditional CRL-based authentication solutions.

REFERENCES

1. M. Kihl, M. L. Sichitiu, and H. P. Joshi, “Design and Evaluation of two Geocast Protocols for Vehicular Ad-hoc Networks,” Swedish Governmental Agency for Innovation Systems (Vinnova), 2007.
2. H. Rahbar, K. Naik, and A. Nayak, “DTSG: Dynamic time-stable geocast routing in vehicular ad hoc networks,” in Ad Hoc Networking Workshop (Med-Hoc-Net), 2010 The 9th IFIP Annual Mediterranean, 2010, pp. 1–7.

3. Y. B. Ko and N. H. Vaidya, “Location-Aided Routing (LAR) in mobile ad hoc networks ,” ACM journal of Wireless Networks, vol. 6, pp. 307–321, 2000.
4. D. Akhtar Husain, Brajesh Kumar, “A study of location aided routing (LAR) protocol for vehicular ad hoc networks in highway scenario,” International Journal of Information Technology and Web Engineering, vol. 2, no. 2, pp. 118–124, 2010.
5. S. K. Dhurandher, M. S. Obaidat, D. Bhardwaj, and A. Garg, “GROOV: A geographic routing over vanets and its performance evaluation,” in Global Communications Conference (GLOBECOM), 2012 IEEE, 2012, pp. 1670–1675.
6. Yan-Bo Wang; Tin-Yu Wu; Wei-Tsong Lee; Chih-Heng Ke, "A Novel Geographic Routing Strategy over VANET," Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on , vol., no., pp.873,879, 20-23 April 2010