EMFU COMBINED WITH AUTHENTICATION PROTOCAL

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

VNS MANSWINI,
Assistant Professor,
Department of Computer Science and 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 protect vehicle ad hoc networks (VANETs). Every PKI system authenticates a received message by checking if the sender's certificate is included in the current CRL and evaluating the authenticity of the sender's certificate and signature. We propose an (EMFU) Expenditure Message for UAV in this paper, which replaces the time-consuming CRL checking approach with a fast revocation checking methodology. EMFU also employs a new probabilistic key distribution, which enables non-revoked OBUs to safely share and update a secret key. When compared to traditional authentication systems that employ CRL, EMFU can dramatically reduce the message loss ratio due to message verification latency. EMFU has been shown to be secure and efficient through security research and performance evaluation.

INTRODUCTION

VANETs are a subtype of mobile ad hoc networks (MANETs) in which the nodes are vehicles such as automobiles, trucks, buses, and motorbikes. This means that variables like the road route, which includes traffic and traffic limits, limit node movement. Because node movement is limited, it is reasonable to assume that the VANET will be supported by some fixed infrastructure that can offer access to stationary networks and assist with a variety of operations. Fixed infrastructure will be placed on slip roads, service stations, troublesome junctions, and places notorious for extreme weather. The North American DSRC standard uses the IEEE 802.11p wireless communication standard to connect nodes. To communicate with individuals who are not within radio range, messages must be sent through other nodes (multi-hop communication). In terms of energy, space, and compute, MANETs are confined, whereas vehicles are not. The VANET's huge scale, along

with the prospect of extremely high node speeds (up to 250 km/h), makes it significantly more challenging. The VANET's primary goal is to increase road safety.

LITERATURE SURVEY

As a novel technology, vehicular communications (VC) presents a number of issues that must be solved. Among these are security and privacy concerns, both of which are critical for VC's general acceptability. We are worried about privacy and identity management in the context of emerging technologies in this position paper. Taking into account the basic elements of these systems, we highlight VC-specific challenges and limitations. We see them as part of a larger set of privacy safeguards, as well as ongoing work on VC standards and other mobile wireless communication technologies. A car's broadcasts during communication with other vehicles or roadside devices can be used to find and track it on a vehicular ad hoc network (VANET). The privacy of the vehicle's owner's location is jeopardised by this form of tracking. In this study, we examine ways to provide location privacy in the VANET by allowing vehicles to avoid being tracked via broadcast emissions. We begin by describing the VANET's distinct properties that must be taken into account while developing location privacy solutions.

METHODOLOGY

EMFU is an expedite message authentication protocol that replaces the CRL checking technique with an efficient revocation checking mechanism based on a quick and secure HMAC function. VANETs and any network that uses a PKI system will benefit from EMFU. This is the first approach that we are aware of for reducing authentication latency on VANETs caused by CRL checks.

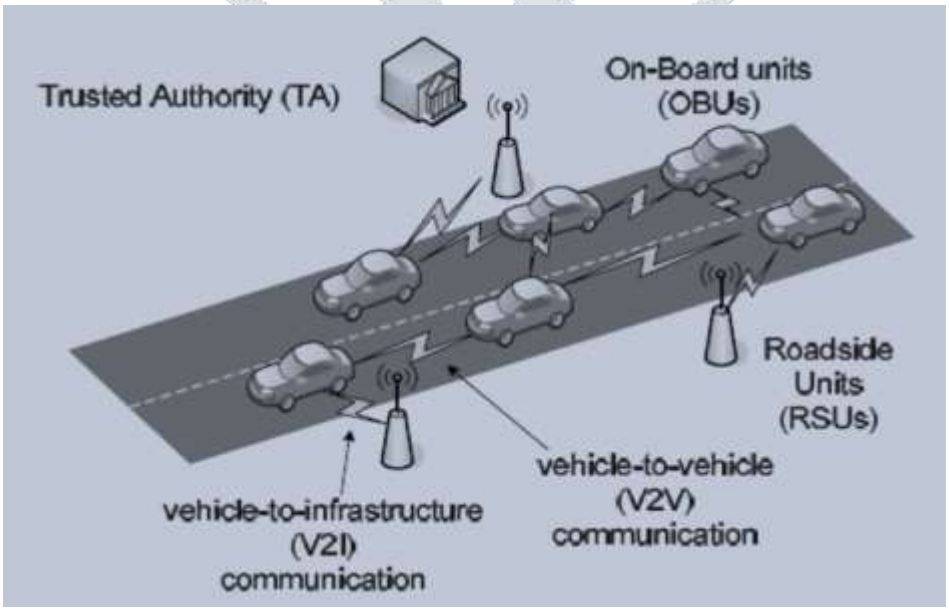

FIGURE 1: The Architecture of the proposed Work

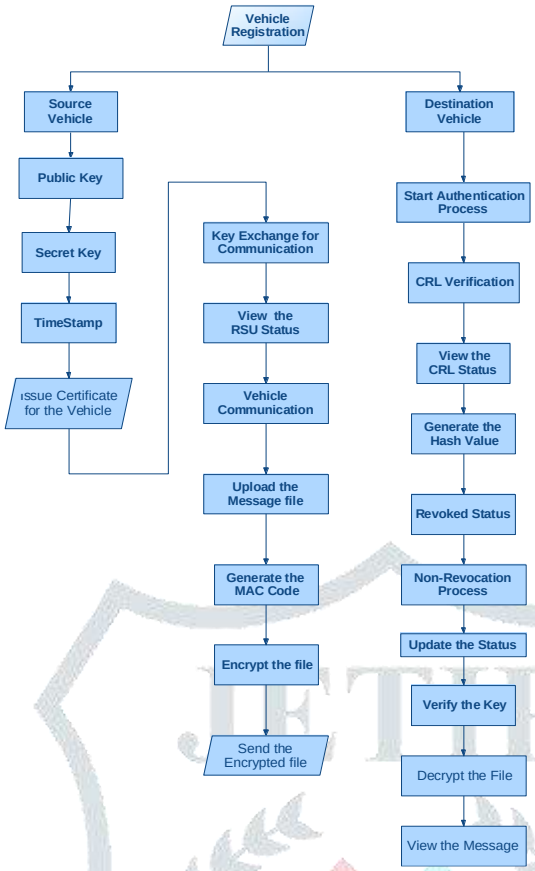

FIGURE 2: WORK FLOW

ADVANTAGES OF THE PROPOSED SYSTEM:

• When compared to CRL checking methods that use linear and binary search algorithms, the EMFU has the simplest processing complexity.

• The number of communications confirmed in less than 300 milliseconds utilising EMFU is 88.7% higher than the number of messages validated using linear and binary CRL checking, respectively.

• When compared to linear or binary CRL checking procedures, the recommended EMFU in authentication minimises the end-to-end delay.

RESULT AND DISCUSSION

Non-revoked OBUs can securely communicate and update a secret key using the EMFU, which uses a probabilistic key distribution. When compared to traditional authentication systems that employ CRL, the EMFU can dramatically reduce the message loss ratio due to message verification latency. The security and efficiency of EMFU are shown through security analysis and performance measurement.

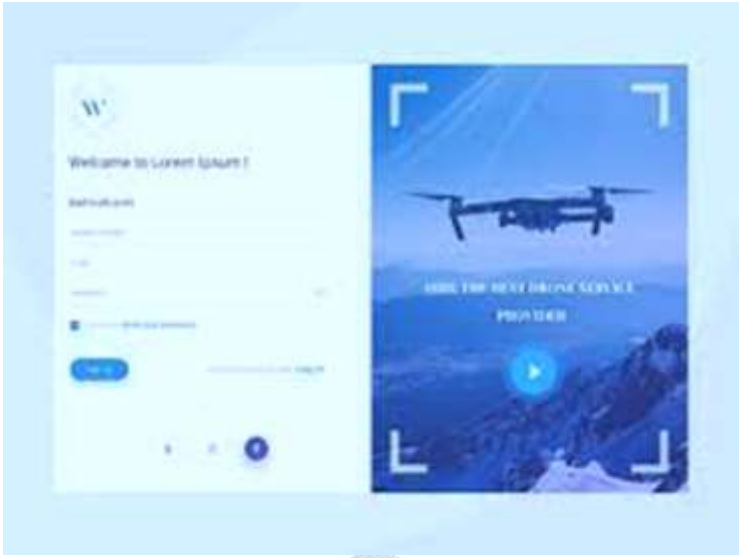

FIGURE 3: Registration Page

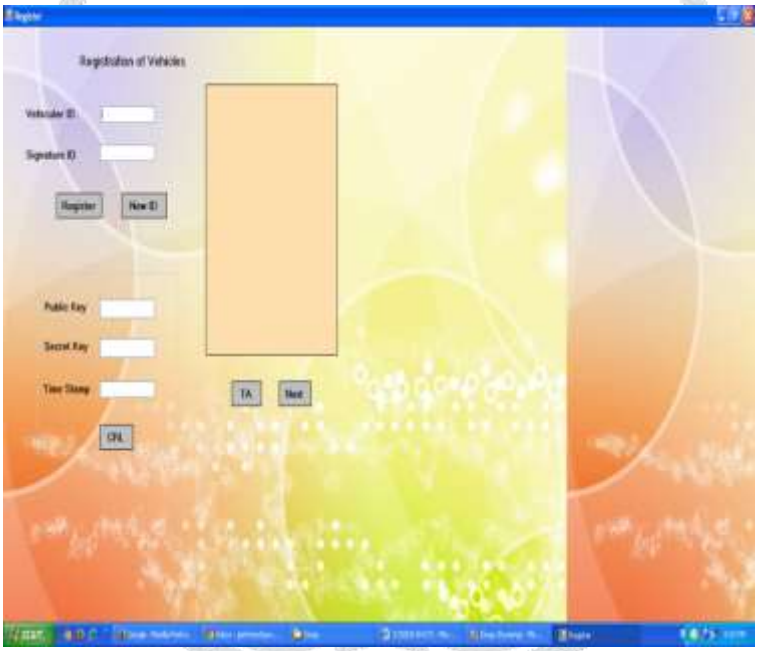

FIGURE 5: LOGIN PAGE

CONCLUSION

For VANETs, we proposed EMFU, which replaces the time-consuming CRL checking method with a quick revocation checking process based on the HMAC function, which speeds up message authentication. The proposed EMFU uses a new key sharing approach that allows an OBU to update its compromised keys even if certain revocation notifications have been missed earlier. A modular feature of EMFU allows it to work with any PKI system. It also outperforms traditional CRL-based authentication systems and is resistant to typical assaults.

REFERENCES

1. 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.
2. J. William, "BEST LIST OF TOP 26 DRONE WITH CAMERA FOR 2018," in Drones Globe vol. 2018, ed, 2018.
3. E. Torun, "UAV Requirements and design consideration," Turkish Land Forces Command Ankara (Turkey)2000.
4. 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.
5. 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.
6. 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.