*Scientiae Mathematicae Japonicae*

# AN INTELLIGENT MESSAGE AUTHENTICATION SCHEME FOR EMERGENCY AND SAFETY RELATED MESSAGES IN A VEHICULAR NETWORK

Prakash Veeraraghavan and Dalal Hanna
Department of Computer Science and Information Technology
La Trobe University, Victoria 3086, Australia

Abstract. Road safety and traffic efficiency are two important applications of a Vehicular Ad-hoc Network (VANET). In VANET, safety and emergency messages are broadcasted to all vehicles in a risk zone before the validity of the message expires. Emergency and safety-related communications have a very strict real-time requirement of 100ms latency from an originating host's application layer to destination host's application layer and a Packet Delivery Ratio (PDR) of 90% and above. Due to one-to-many nature of these emergency messages, public-key encryptions may not be employed. Furthermore, vehicles on the road have no constant access to the Roadside infrastructure. Thus, access to a Public-key Infrastructure or a Certificate Authority is not always guaranteed. Exploiting this weakness, any attacker with malicious intention can broadcast falsified emergency messages with spoofed identity to disrupt the normal operation. They may also do in order to launch a terror-like attack. Since the identity of the originating malicious vehicle cannot be established, it is not possible to take any legal action against the owner of these vehicles.

In this paper, we propose a smart digital certificate mechanism using a modified threshold cryptography scheme, that we call it as a pseudo-identity based encryption to identify the origin of every emergency message. Since the keys are not forgeable, any such malicious activities are immediately known to the receiving host vehicles and vehicle registration authorities, thus facilitating legal action. The main advantage of our proposed scheme is that it can work without constant access to a Public-key Infrastructure or a Certificate Authority. Our scheme satisfies the identical security requirements as that of the underlying public-key cryptography and incurs the same memory and run-time complexity.

The proposed scheme can also be implemented in a Mobile Ad hoc environment or a distributed environment, where source authentication is an important factor, and there is no constant access to the backbone of the network.