RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks

K. Balan[1], A. S. Khan[3], A. A. Julaihi[4], S. Tarmizi[5], K. S. Pillay[6]
Faculty of Computer Science and Information Technology
University Malaysia Sarawak
Kota Samarahan, Sarawak, Malaysia

L. F. Abdulrazak[2]
Research Management Center
Computer Science Department,
Cihan University Sulaimani, Iraq

H. Sallehudin[7]
Faculty of Information Science and Technology
University Kebangsaan Malaysia
UKM Bangi, Selangor, Malaysia

***Abstract*—Autonomous Vehicular Ad hoc Networks (A-VANET) is also known as intelligent transportation systems. A-VANET ensures timely and accurate communications between vehicle to vehicle and Vehicle to Roadside Unit (RSU) to improve road safety and enhance the efficiency of traffic flow. Due to open wireless boundary and high mobility, A-VANET is vulnerable to several security threats especially impersonation, denial of service, pollution attacks. This paper presents a novel Received Signal Strength Indicator (RSSI) based public key infrastructure (PKI) to address the above-mentioned attacks. Each incoming signal will be authenticated based on RSSI value and digital signal (obtained using PKI) is utilized for cryptography and communication within the insecure channel. The proposed solution is verified with and without the presence of attacker by evaluating the packet delivery ratio and packet overhead.**

Keywords*—Autonomous; vehicular ad hoc networks; public key infrastructure; received signal strength indicator

I. Introduction

Vehicular Ad Hoc Networks is also known as intelligent transportation systems. The aim is to provide inter-vehicle communication and roadside to vehicle communication to increasing road safety, improving local traffic flow and the efficiency of road traffic by providing accurate and timely information to road users [1], [2]. In VANET, vehicles are used as network nodes as seen in Figure 1. Security necessities are imperative to provide safe communication in VANET. Due to high mobility, security is more challenging because nodes constantly change network topology. Due to its open-access nature, additionally, VANET is powerless against pollution, Denial of Service (DoS), impersonation, and message fabrication attacks. Thought process of the attackers is to alter the message content, to occupy from different malicious attack, to get the information required, send false message and make network resources become unavailable to others. The various security attacks adopted by an attacker such as pollution attack, impersonation attack, DoS attack and fabrication attack do not only invade driver's confidentiality but also pose risks to the driver, which can cause serious harms/injuries or, worse, loss of lives.

Autonomous vehicles are a type of self-driving car in this current technology of world [3]. The number of autonomous vehicles being used on the road is increasing day by day. Self-driving car, driver-less car or robotic cars are capable to perform an action and navigate without human input or driver responsibility. The autonomous car will have its own GPS (Global Positioning System) as function to locate the user destinations [4]. Alongside other technology that has emerged during this time, the idea of autonomous car can be categorized as an excellent idea, however there are still draw back happened. As the autonomous car is wireless, it depends on a system for exchanging data or information between other vehicles in order to avoid collision on the road [5], [6]. The use of wireless sensor network (WSN) system creates an opportunity to the attacker such as hacker to attack the car system and function of the autonomous car.

An attacker could launch pollution attack by sending malicious or useless data to the target vehicles in order to reduce the vehicles performance. The attacker also created a great number of fake messages to interrupt the vehicle and make it malfunction. In addition, some attackers will distract those good vehicles from malicious attacks in order for other attackers to attack successfully.

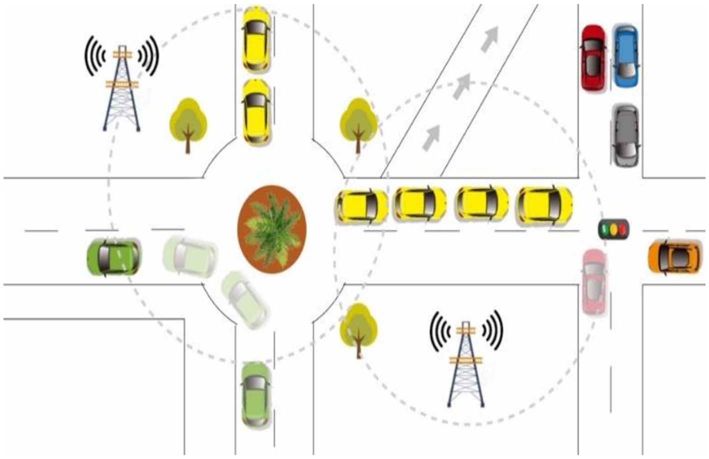

Fig. 1. Basic VANET Structure.