Article

Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET

Adnan Shahid Khan [1,*], Kuhanraj Balan [1], Yasir Javed [1,2], Seleviawati Tarmizi [1] and Johari Abdullah [1]

[1] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia; 17020126@siswa.unimas.my (K.B.); yjaved@psu.edu.sa (Y.J.); swati@unimas.my (S.T.); ajohari@unimas.my (J.A.)

[2] Department of Computer Science, Prince Sultan University, Riyadh 11586, Saudi Arabia

* Correspondence: skadnan@unimas.my

Received: 9 September 2019; Accepted: 8 November 2019; Published: 14 November 2019

Abstract: Vehicular ad hoc networks (VANET) are also known as intelligent transportation systems. VANET ensures timely and accurate communications between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) to improve road safety and enhance the efficiency of traffic flow. Due to its open wireless boundary and high mobility, VANET is vulnerable to malicious nodes that could gain access into the network and carry out serious medium access control (MAC) layer threats, such as denial of service (DoS) attacks, data modification attacks, impersonation attacks, Sybil attacks, and replay attacks. This could affect the network security and privacy, causing harm to the information exchange within the network by genuine nodes and increase fatal impacts on the road. Therefore, a novel secure trust-based architecture that utilizes blockchain technology has been proposed to increase security and privacy to mitigate the aforementioned MAC layer attacks. A series of experiment has been conducted using the Veins simulation tool to assess the performance of the proposed solution in the terms of packet delivery ratio (PDR), end-to-end delay, packet loss, transmission overhead, and computational cost.

Keywords: VANET; trust model; blockchain; architecture; privacy; authentication; security

1. Introduction

Vehicle ad hoc networks (VANET) emerged as a subset of a mobile ad hoc network (MANET) [1] application. VANET is considered a substantial approach for intelligent transportation systems (ITS) [2]. VANET has recently been the focus of various researchers in the wireless mobile communication field. The aim of VANET is to provide inter-vehicle communication and roadside units to vehicle communication to increase road safety and improve local traffic flow and the efficiency of road traffic by providing accurate and timely information to road users [3]. In VANET, vehicles are used as network nodes, as seen in Figure 1.

There are two types of communications in VANET, which are vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications [4]. The on-board units (OBUs) and road side units (RSUs) in VANET establish a connection among themselves with the help of dedicated short-range communication (DSRC) in a single or multi-hop communication [5–7].

VANET offers various services and applications to the users, most of which are concerned with the safety of the drivers, infotainment, and navigational aid [8]. There are two types of information shared in VANET: safety (vehicle speed warning, curve warning) and non-safety information (value-added comfort application) [9]. By default, safety information is given a higher priority in VANET as compared to non-safety information, since safety information notifies drivers of expected dangers to allow an