Vehicular Communications 7 (2017) 40–50

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

SMMV: Secure multimedia delivery in vehicles using roadside infrastructure

Satya S. Karanki, Mohammad S. Khan *

Department of Electrical Engineering & Computer Science, Texas A&M University, Kingsville, TX 78363, USA

ARTICLE INFO

Article history:
Received 28 September 2016
Received in revised form 30 November 2016
Accepted 18 December 2016
Available online 23 December 2016

Keywords:
VANET
WiMAX
Android
AES
SHA-256

ABSTRACT

Vehicular ad-hoc networks (VANETs) have gain a lot attention from academic and industry in recent years. It is seen as the most promising field to change the automotive industry, specially regarding road safety. The primary objective of this paper is to build an Android-based application that utilizes WiMAX IEEE 802.16 network protocols to send a multimedia message securely from one vehicle to another vehicle using infrastructure like rode side units (RSUs) or base station etc. The proposed protocol combines both AES encryption and SHA-256 hashing algorithms to secure the message. Thus, it enables the vehicle's driver to send multimedia messages securely to other drivers using voice commands without having to reach for a cell phone. We compared our proposed scheme in various car density environments such as urban and high-way scenarios. We justified our proposed scheme with simulation results in the end.

1. Introduction

World Health Organization statistics show that approximately 1.25 million people died globally and 20–50 million people were injured or disabled in road accidents in 2013 [1]. According to the American National Safety Council, 38,300 people lost their lives in traffic accidents, and almost 4.4 million people were injured in auto-related collisions in 2015. These statistics represent a 14% increase when compared to data from 2013 and 2014 [2]. In economic terms, accidents in the US cost almost $242 billion per year [3].

Technology can play a vital role in preventing road accidents while also ensuring safety. Vehicular early warning systems have gained high priority in recent years and are mostly used to recognize and detect the road conditions or accidents for providing safe transportation. Developments in the field of wireless communication and automobile industries made VANET into one of the most promising fields in academic and research sectors. Due to its unique characteristics, such as dynamic topology and predictable mobility, VANET has become more popular as a methodology for preventing accidents [4].

In VANET, each vehicle acts as a wireless node or router and connects to another vehicle in order to create a broad range of the mobile vehicular network (V2V). Any number of vehicles can join or leave the network at any time. This wireless network enables comprehensive communication between the vehicles [5]. When a major accident or obstruction occurs, this strategy helps in terms of communicating the requisite information between the vehicles (V2V).

The primary concern of VANET is the safety of the passengers in the vehicles. However, numerous applications have been proposed which include 'value added' non-safety features. Based on the type, VANET applications are broadly divided into safety and non-safety applications. Applications that convey critical safety information, including but not limited to road conditions, accidents, and traffic related information through the data communication between vehicles, RSU's or roadside infrastructures, come under the heading of safety applications [6].

The secondary purpose of VANET is to enable the multifarious non-safety applications that can provide infotainment to travelers [7]. These are entertainment based applications that provide online connectivity, video or audio streaming, and message communications. Google's 'Android Auto' [8] and Apple's 'Apple Car Play' [9] are examples of car's dashboard projections that provide information and entertainment to the vehicle's travelers. These applications work when mobile devices are connected to the vehicle dashboards. These systems are completely dependent on mobile operating systems.

The Android Compatibility Definition Document released on Oct 2015 refers to a vehicle dashboard display, running on the Android Operating System called Android Automotive. Rather than using previous versions of Android Auto, which required a mobile to function, Android Automotive works independently in order to

* Corresponding author.
E-mail address: adhoc.khan@gmail.com (M.S. Khan).

http://dx.doi.org/10.1016/j.vehcom.2016.12.002
2214-2096/© 2016 Elsevier Inc. All rights reserved.

provide a system with interdisciplinary infotainment functionality [10].

The concept of Android Automotive is still in the budding stage; focus on using Android applications for message communications between vehicles which is fairly a new approach. This paper focuses on the explication of developing an Android application protocol deemed Secure Multimedia Messaging service in Vehicular Ad-Hoc Network (SMMV) that can be used for personal message communications between vehicles using WiMAX network securely.

Considerable research has been done on message communication between vehicles using Road Side Unit (RSU), but little extant research has been conducted on using WiMAX towers. Road Side Units (RSU's) use WAVE (Wireless Access in Vehicular Environment – IEEE 802.11p), which is standard protocol for communication between vehicles and other RSU. These are stationary objects placed on the road side. They operate at 5.9 GHz bands and support short range communications. These units and vehicles have to maintain secure keys or certificates to authenticate the message transmission from each unit or vehicle. This requires storage capacity in both RSU's and vehicles which is very limited [11]. As the number of vehicles and RSU increases, the number of keys and/or certificates needed also increases excluding the maintenance cost of keys or certificate.

The main advantage of using the Android application with WiMAX is that every time the application connects to the server it authenticates itself. Therefore, there is no need for maintaining other vehicle certificates or keys to authenticate for message communication. The Android application uses a secure communication channel (HTTPS) to connect to the application and the server. Additionally, the message is encrypted end-to-end with AES for message authenticity and uses SHA-256 to verify its integrity. For efficient transmission, 'Ad-hoc On-demand Multipath Distance Vector Routing' (AOMDV) protocol is used.

The remainder of the paper is organized as follows. Section 2 summarizes the related work on VANET, security, routing protocols. Section 3 explains our proposed protocol in details. Section 4 discusses the application development. Section 5 describes the security performance evaluation. Section 6 is about performance analysis of message transmission. Section 7 focuses on performance analysis of RSU and WiMAX, and Section 8 concludes the paper.

2. Related work

VANET is becoming one of the most promising emergent technologies as it helps in preventing accidents by alerting the drivers about the incidents or conditions that are ahead on their route while also notifying law enforcement or medical teams about the incidents so that they can prevent further loss. A good amount of research conducted, not only in vehicular safety but in also providing infotainment solutions, has reinforced the robustness of the VANET approach.

As discussed earlier, VANET is a group of mobile nodes moving at variable speeds; each node acting as a host and router that can go out of the network or join in a network. Since these are dynamic topologies, one of the key challenges is to design a dynamic routing protocol. Johnson and Maltz [12] proposed a protocol called "Dynamic Source Routing" (DSR) that adapts to routing changes with little or no overheads. Perkins and Royer [13] introduced a novel algorithm called "Ad hoc On-Demand Distance Vector Routing" (AODV). It considers each vehicle as a router and attains the route on demand. Whenever this protocol initiated, a request sent to the destination through a network and subsequently waiting for a reply, depending on latency and overhead, this may take a longer time for large networks. If it failed to discover a route because of troubleshooting issues, a new request is initiated to find the destination, which may take an even longer time. To overcome these hurdles, Marina and Das [14] have proposed the "Ad hoc On-demand Multipath Distance Vector Routing" (AOMDV) protocol. Instead of utilizing a single path suggested by AODV, AOMDV protocol discovers multiple paths originating from the source to the destination, and the best route is selected amongst them. Moreover, it has to invoke a new path only when all the previous paths fail.

VANET exhibits numerous choices in wireless technologies to communicate with other vehicles. These are divided into three categories: Long range, Medium range and Short range. Anwer and Guy [15] did an extensive survey and compared different wireless technologies and selected WiMAX suits well for wireless communication in VANET. They also stated that since WiMAX provides bandwidth higher than LTE (2.5 GHz), it increases the throughput.

In 2011, IEEE Standard Association approved IEEE 802.16m (WiMAX) [16]. Among emerging broadband technologies that provide high-speed Internet, WiMAX is one of the best compatible wireless technologies for utilizing VANET. Vinoth and Manoreya, in their recent publication, mentioned that WiMAX aimed to provide download rates of 100 mb/sec at a speed of 340 km/h [17].

The performance of AODV, AOMDV, and DSR routing protocols has been analyzed recently by Dorge and Dorle [18] in their published research article. Their design is based on a WiMAX network with Multiple Inputs Multiple Outputs (MIMO) and Adaptive Modulation Coding (ADC) techniques. They have used an NS2 simulator to create realistic scenarios like high-speed highway environments, variable speed vehicle environments, and city environments. They concluded that AOMDV routing protocol is better for WiMAX-based VANET systems than the other two protocols based on the quality of service, maximum throughput, and packet delivery ratio.

In 2005, Google acquired Android Operating System. It developed on Linux and mainly was used as a mobile operating system for cell phones and tablets. The advances in Android technology have grown in such a way that Android open source projects, in their latest upgrades, have embraced a wide variety of devices such as Android Television, Watches, Handheld Devices and Automotive applications [10].

Most of the research in transmitting secure messages is based on RSU's utilization of IEEE 820.11p such as [11,19–22]. However, very little or no research has been initiated pertaining to communicating personal messages based on Android-based applications through VANET between vehicles. Since VANET uses wireless technologies, care has been taken to minimize the risk of security threats.

As discussed earlier, the proposed system uses Android Automotive to send secure multimedia messages from one vehicle to the other. Android features multilayer security that ensures the safety of the users, network, applications, data and the device [23]. This protocol uses the Https connections to connect the server in order to create secure web traffic [24].

Y. Zou et al., [25] in their article "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends", excellently described the WiMAX protocol stack and security sublayers. There are two layers in the protocol stack, Medium Access Control (MAC) layer, and Physical layer. MAC layer constitutes three more sub-layers: Service Specific Convergence Sub-Layer, Common Part Sub-Layer and Security Sub-Layer. All the security-related issues managed under security sub-layer. Additionally, it is responsible for authentication, authorization, and encryption. However, MAC layer is well-protected Physical layer is vulnerable to security threats like eavesdropping, jamming, and scrambling attacks. Eavesdropping constitutes secretly listening to someone's conversation; jamming reduces the channel capacity while scrambling is similar to jamming but with short bursts targeted at specific intervals. Either way, the message transmitted from one person to another is not private anymore.