Vehicular Communications ••• (••••) •••–•••

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Secure cooperative communication scheme for vehicular heterogeneous networks

Liangmin Wang [a,b], Xiaolong Liu [a,*]

[a] School of Computer Science and Communication Engineering, Jiangsu University, Jiangsu, China
[b] Laboratory of Security Tech. for Industrial Cyberspace, Jiangsu, China

ARTICLE INFO

Article history:
Received 11 August 2017
Received in revised form 29 November 2017
Accepted 19 January 2018
Available online xxxx

Keywords:
OBU
D2D
Cooperative communication
Stochastic geometry
Physical layer security

ABSTRACT

Vehicular Heterogeneous Network (VHN) is a massive network which contains dedicated short range communication (DSRC) based on IEEE 802.11p, Device-to-Device (D2D) communication and cellular network (e.g., 5G). VHN is supposed to complete the interactions of V2X (where X stands for vehicle, road, pedestrian and Internet) and cooperative communications among multiple networks. However, different networks use different communication protocols so that it is hard to implement cooperative communication. Furthermore, due to the openness of wireless channels, communication links are vulnerable to eavesdroppers and cannot guarantee the confidentiality. To deal with these problems, this paper designs an On Board Unit (OBU) with multi-level security. Meanwhile, we implement cooperative communication using designed OBU, for which OBU performs the vertical handoff and selects best mode with consideration of communication requirements. In VHN, we also consider a network model which contains an eavesdropper, and present formulations to describe its specific security problem by utilizing stochastic geometry theory. Thereafter, we propose a secure cooperative communication scheme which uses physical layer security, and explore secrecy-based successful transmission probability as well as transmission capacity. In addition, we propose mode selection and optimization algorithms to improve security of the proposed cooperative communication. Finally, experimental results show that our proposed scheme is feasible and achieves better security than other communication schemes in comparison.

1. Introduction

VHN fuses multiple heterogeneous networks (e.g., in-vehicle network, vehicular ad-hoc network and 5G cellular network) to facilitate their efforts to better realize V2X interaction and cooperative communication. In general, there are two main solutions for current V2X interaction, including backend-based communication with long term evolution (LTE) cellular standard [1] and DSRC based on IEEE 802.11p standard [2]. However, LTE system cannot satisfy the low latency and high reliability, especially in dynamic network topology. Unfortunately, DSRC based on IEEE 802.11p (short for DSRC) also has some obvious shortcomings, such as deficient delay optimization, limited range of communication and special requirement for a large number of Road Side Units (RSUs) as well as dedicated spectrum resources (i.e., 915 MHz/5.8 GHz/5.9 GHz), which results in untimely handling for security issues. Besides, uncertain evolutionary path of future for DSRC can restrict the development of VHN to intelligent connected vehicle (ICV) [3] in the next period of time. Therefore, cooperative communication with a better solution used to supplement deficiencies is required to be considered.

5G mobile communication technologies provide opportunities for innovation of communication modes in VHN. The remote interaction modes are extended from pure cellular communication to D2D-based intra or out of band communication. D2D, one of the key technologies of 5G, allows direct messages transmission between two adjacent vehicles [4]. It promotes the development of multi-level topologies, including D2D-underlaid device layer and macro cellular layer. In addition, it can significantly decrease communication delay, improve spectral efficiency and expand channel capacity. Cheng et al. [5] and Sun et al. [6] presented that D2D technology has been applied as the supplement to DSRC in cooperative communication of VHN.

Since multiple networks use different communication protocols, cooperative communication among D2D, DSRC and cellular networks cannot be implemented easily. In our consideration, OBU is an essential hub for cooperative communication among these networks. But in security concern, multiple networks access will

* Corresponding author.
E-mail address: liuxl6063@163.com (X. Liu).

https://doi.org/10.1016/j.vehcom.2018.01.001
2214-2096/

threaten OBU and in-vehicle network which is usually assumed to be completely secure. Besides, D2D-based vehicle-to-vehicle (V2V) also brings in security problems such as eavesdropping during message transmission. It is easy for malicious or selfish nodes to obtain legitimate user's privacy (e.g., trajectory, identity and hobby) by eavesdropping.

To enhance security of messages transmission, physical layer security technology based on Shannon theory is considered as an effective method [7,8]. Physical layer security exploits the inherent characteristic of communication channels to prevent message leakage to the eavesdropper. It is applied independently of the higher layers. There are no limitations assumed for the eavesdropper on computational resources. Just because of its low dependence on computational complexity and strong ability of anti-eavesdropping, physical layer security technology can serve as a complement to computation-based encryption security in terms of secure transmission. Therefore, in order to adapt to characteristics of multiple networks communication, and enhance security during multiple networks access and messages transmission, we propose a secure design scheme for OBU. Based on the designed OBU, we provide the cooperative communication scheme combining with physical layer security for VHN, which uses three different communication modes. The main contributions of this paper are summarized as follows:

1) We propose an OBU equipped in vehicle to implement cooperative communications among DSRC, D2D-V and cellular network for VHN.
2) To meet security demands of multiple networks access and cooperative communication, we propose a multi-level security architecture and protection mechanisms for our designed OBU.
3) We consider a VHN communication model with assumption of the presence of an eavesdropper. By utilizing stochastic geometry theory, we provide the analysis of security problem formulations in detail.
4) We explore multiple safety indexes (e.g., secrecy outage probability and secrecy-based transmission capacity), and propose model selection and optimization algorithms to improve the security of messages transmission in cooperative communication scheme.

The rest of this paper is organized as follows. The next Section reviews more related works. In Section 3, we describe the implementation for secure cooperative communication scheme based on designed OBU with multi-level security, and present a VHN communication model. We detailedly analyze security enhancement using cooperative communication scheme with model selection and optimization algorithms in Section 4. In Section 5, we present simulation and evaluation for security performance of our scheme. Finally, we conclude this paper in Section 6.

2. Related works

In vehicular ad-hoc networks (VANETs), IEEE 802.11p-based DSRC has become popular communication mode among vehicles and infrastructure at present [9]. However, the defects such as delay issue and limited range of communication restrict its future development. Meanwhile, D2D-V communication regarded as an appealing solution can assist DSRC, which has been proposed by academic and standardized activities [6,10].

Nevertheless, there are more severe interference and eavesdropping issues D2D-V experienced than that of DSRC. Interference is also one of impact factors for security in scenarios with eavesdropping. For example, from perspective of eavesdroppers, as vehicle density increase, the probability of successful eavesdropping decrease because of interference issue introduced by increase in the number of vehicle nodes. Therefore, related studies have paid attention to alleviating interference caused by reusing spectrum resources using resource allocation or power control [11–14]. For example, Haenggi et al. [14] considered the interference and improvement on performance of Poisson network with a certain communication mode. In this paper, we analyze this issue by considering secure cooperative communication among multiple modes, and obtain better performance.

Remarkably, the key security issue during message transmission for VHN lies in eavesdropping. In this connection, a large number of studies focus on preventing eavesdropping by using physical layer security technology for VHN. For example, Sun et al. [15] studied a new cooperative scheme for source-relay vehicles with capability of anti-eavesdropping to maximize secrecy capacity. Yang et al. [16] proposed a method about appropriately increasing artificial noise (AN) in the course of messages transmission. It can reduce the quality of received signals of an eavesdropping node. Kong et al. [17] presented that reducing transmit power and SINR of eavesdropping vehicles can decrease channel capacity of eavesdropping nodes.

Cooperative communication among multiple networks can achieve complementary advantages, thus significantly improving performance of VHN. For researches of cooperative communication between DSRC and D2D-V in VHN, Mumtaz et al. [18] pointed out that D2D communication technology will assist IEEE 802.11p-based V2V communication using spectrum sensing in VHN. Cao et al. [19] explored the improvement of end-to-end delay in VANETs with the assistance of D2D-V communication link. Abdelrahman et al. [20] studied network blocking and fault recovery of hybrid network model based on D2D and IEEE802.11p standard, and simulation results show better latency than traditional V2V communication. Nevertheless, few researches explore the security improvement of cooperative communication in VHN comprised of D2D-V and DSRC links. To the best of our knowledge, many existing studies in [15, 18,21,22] only consider secrecy transmission with one communication mode (i.e., D2D-V or DSRC).

3. Implementation for secure cooperative communication scheme

3.1. Hardware design of OBU

According to the assessment of security threats based on ISO 13335 Guidelines for the Management of IT Security (GMITS), as shown in Fig. 1, the OBU hardware is designed into four security areas because of different functions and security levels of areas. The description of four security areas are as follows.

Area A, a core security area, is set up in the innermost layer of OBU. It mainly refers to Security Microcontroller Unit (S_MCU) and components connected to in-vehicle Controller Area Network (CAN) such as the ports of automotive electronic control system. Because of direct connection with in-vehicle network, Area A is the most significant area in OBU. We assume that S_MCU is secure and trusted, then it is applied to authenticate data frames and entities that need to communicate with in-vehicle CAN. Thus, Area A can prevent illegal devices and data from accessing in-vehicle network.

Area B, the signal transmitting area, is located in the outer layer of Area A. There are some significant input information that would be transmitted from Area C and Area D to Area A, including vehicle diagnostic data acquired by On-Board Diagnostic (OBD) from Area C, analysis data of driving behavior from Area C, and judgment of traffic conditions from Area D. The input information are main decision-making sources for Area A to control automotive electronic control system.

Area C is the external hardware devices area, including OBD, monitoring equipments, storage devices and other hardware de-

Please cite this article in press as: L. Wang, X. Liu, Secure cooperative communication scheme for vehicular heterogeneous networks, Veh. Commun. (2018), https://doi.org/10.1016/j.vehcom.2018.01.001