Future Generation Computer Systems 56 (2016) 476–492

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Secure clustering for efficient data dissemination in vehicular cyber–physical systems

Rasmeet S. Bali, Neeraj Kumar *

Department of Computer Science and Engineering, Thapar University, Patiala, India

HIGHLIGHTS

- A new secure clustering for efficient data dissemination in vehicular environment is proposed.
- A new secure trust metric is evaluated for cooperation among the nodes.
- Performance of the proposed scheme is found satisfactory with respect to various metrics.

ARTICLE INFO

Article history:
Received 30 June 2015
Received in revised form
3 September 2015
Accepted 6 September 2015
Available online 30 September 2015

Keywords:
Secure clustering
VANETs
Vehicular cloud
Trustworthiness
Vehicular cyber–physical systems
Trust computation

ABSTRACT

From the past few years, there has been tremendous growth with respect to the usage of Internet-enabled devices for computing and storage across the globe. These devices have the capabilities of computing as well as communication facilities for smooth execution of various applications. The significance of this type of environment where variety of Internet-enabled devices are interconnected is known as Internet of Things (IoT). Objects/things in IoT may be considered as vehicles and this type of environment is called as Vehicular Cyber–Physical Systems (VCPS). In VCPS environment, there are two planes-physical and cyber. On physical plane, all types of computing and communication devices reside while at the cyber plane service providers such as cloud may exist. However, in VCPS environment, security is one of the major concerns as devices communicate with one another using different protocols which are susceptible to various types of attacks. To address these issues, we propose a novel secure clustering for efficient data dissemination between different devices in VCPS environment. A new trust metric based on varying transmission characteristics of vehicles is defined for trust computation among the different devices which is evaluated both at local, and global levels. This trust metric is used to establish the current security level of vehicles and is the key parameter for creating secure clusters. Algorithms for secure clustering and trust establishment are also designed in the proposed scheme. The performance of the proposed scheme is evaluated with respect to different evaluation metrics in various network scenarios. The results obtained clearly depicts the satisfactory performance of the proposed scheme in VCPS environment.

1. Introduction

Vehicular adhoc network (VANET) is a specialized type of network used for providing seamless services to the onboard passengers such as—safety alerts, ease of driving, and entertainment. Broadly, there are two types of communications used in this environment vehicle-to-vehicle (V2V), and Vehicle-to-Infrastructure (V2I) [1,2]. As communication among the vehicles is mainly done using wireless communication so there is a need to design an efficient secure communication among different components in this environment. VANETs provide base for a large number of applications in different domains related to the intelligent transportation such as vehicular security, brake warning, an enhanced navigation, and road traffic management [3,4]. This necessitates the requirement for inter-vehicular communication to create a reliable transportation system that allows secure broadcasting and collection of various type of information related to entertainment, and safety. There have been several efforts for standardizing the deployment of vehicular network. In USA, IEEE proposed a set of standard for describing the architecture of vehicular network. This standard is called as Wireless Access Vehicular Environment (WAVE) or IEEE 802.11p [5] that describes the requirement and specification of Message Authentication Code

* Corresponding author.
E-mail addresses: nehra04@yahoo.co.in, neeraj.kumar@thapar.edu (N. Kumar).

http://dx.doi.org/10.1016/j.future.2015.09.004

layers to support WAVE communication. Additionally, IEEE 1609 family of standards [6–9] describes higher layers in WAVE architecture.

However, the design and development of various solutions for secure communication in VANET's have various challenges keeping in view of the high mobility and varying density of the vehicles on the road [10]. So, it is essential to ensure that the critical information should not be captured by different attackers in the network. Moreover, the system should be able to establish the identity of the drivers and at the same time must protect the privacy of drivers, and passengers. The IEEE 1609.2 standard is focused on available security services for vehicles to authenticate other neighboring vehicles using certificates managed by a centralized Certification Authority (CA) within a public key infrastructure (PKI). However, deployment of PKI is difficult in VANET as these are designed for networks that have a centralized controlled, and ubiquitous connectivity. VANETs on the other hand are characterized by relatively high velocity with constrained mobility pattern which result in frequent changes in network topology [11]. Moreover, deploying PKI in VANET's with an architecture designed for centralized networks has a large number of challenges pertaining to scalability as CAs cannot be made accessible to all vehicles due to their high mobility [12].

Also, having limited CA for the whole network may create a single point of failure while multiple CA's may enhance the overhead of the network. Some existing solutions [13,14] have considered Road Side Unit (RSU) as CA. However, their density needs to be sufficiently high so that a vehicle need not have to wait a long period outside the RSU transmission range [13].

To resolve the above defined challenges and issues of VANET's, Vehicular Cloud Computing (VCC) has emerged as one of the leading technologies for next generation vehicular networks [14]. VCC is a hybrid technology that provides various solutions for road and traffic management by providing quick response using instant decisions by accessing vehicles resources such as—storage, communication, and computation. VCC takes advantage of cloud-based computing resources for enhancing applications for driver convenience. The main objectives of VCC are to provide fast computational services at a comparatively lower cost thus enhancing the applicability of VANETs for applications such as reducing traffic congestion, and accidents on the road.

VCC provides an integration of Wireless Networks, Intelligent Transportation System (ITS) and Cloud Computing for better road safety to achieve secure modern ITS [15]. In modern ITS, the end users are provided a large number of facilities for their convenience by VCC. By leveraging the communication, storage and computing resources available in the vehicles, the Cloud-based infrastructure can result an efficient resource management at various levels in this environment [16,17]. Combining all these resources in an efficient manner has a significant impact on various vehicular applications. The underutilized vehicular resources including computing power, communication and storage facilities can be pooled with other vehicles on the road or rented to customers, similar to the way in which the resources of the present conventional cloud are provided to the end users (see Fig. 1).

With the evolution of IoT and need for information retrieval from various objects distributed across the globe, VCC has gained momentum to provide seamless services to the end users [18]. The proposed clustering scheme forms the basis for a large number of applications in VANET's. In this environment, we have studied the communication issues and parameters of vehicular dynamics to support secure vehicle-to-vehicle (V2V) cloud-based clustering for efficient communication. Most of the existing proposals in literature depend upon the vehicle-to-roadside (V2R) communication using roadside infrastructure to provide security. Therefore, we propose a distributed and dynamic clustering scheme for VANET's to fulfill the requirement of security in cloud-based infrastructure for generating high security clusters among the vehicles.

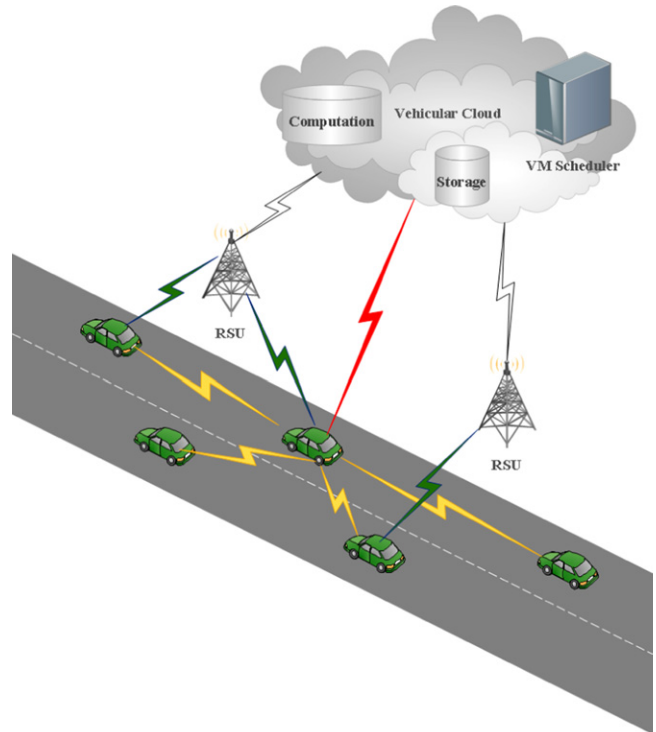

Fig. 1. Vehicular cloud environment for information dissemination.

The proposed scheme is distributed because a set of elected vehicles in a cluster become cluster head's (CH's) having the responsibility of monitoring the neighboring vehicles. The presence of infrastructure on the road is optional and it is dynamic because the election of CH's depends on the topological changes using the parameter based on vehicular mobility. Unlike existing clustering schemes in literature, the election of CH's is based on two parameters based on vehicular dynamics and trustworthiness behavior. The trustworthiness weight of a vehicle depends on its own trust level as compared to average trust levels of all the vehicles within the network.

The proposed scheme uses a vehicular framework for sensing and broadcasting the current vehicular parameters such as velocity, density, and location of each vehicle on the road. To account for the high speed of vehicles and vehicular mobility patterns, the proposed scheme considered different values of clustering durations to construct optimized clusters. The clustering duration are varied between 10 and 140 s by taking into account varying speed of vehicles on urban roads. The variation in clustering duration is estimated using simulations. The clustering duration helps in attaining optimal cluster stability in the proposed scheme. It consists of a module for sensing vehicular parameters and a cloud-based module for computing trustworthiness values. The sensing module is deployed with on-board vehicles which provides information about the vehicles traffic and security characteristics. It broadcasts this information periodically to the vehicular cloud using various short, medium, and long range communication protocols such as—RFID, Bluetooth, WiFi, WIMAX, and LTE. The centralized cloud-based computing module helps to evaluate the security behavior of every vehicle in immediate vicinity and then uses the past behavior characteristics of the vehicle to modify its trustworthiness level with respect to other vehicles.