A Distributed Secure Architecture for Vehicular Ad Hoc Networks

Tahani Gazdar, University of Manouba, Tunisia
Abdelfettah Belghith, University of Manouba, Tunisia
Abderrahim Benslimane, University of Avignon, France

ABSTRACT

In this paper, the authors propose a dynamic Public Key Infrastructure (PKI) for vehicular ad hoc networks to distribute the role of the central certification authority (CA) among a set of dynamically elected CAs. The election process is based on a clustering algorithm relying on trust levels and relative mobility. Furthermore, the authors have adapted the Dynamic Demilitarized Zones to protect the elected CAs from malicious nodes and enable them to act as registration authorities (RA). Extensive simulations are conducted to evaluate the performance of the clustering algorithm and investigate the impact of the vehicle speed, the vehicle average arrival rate, and the percentage of confident vehicles on the stability and efficiency of the security infrastructure. The authors demonstrate the percentage of confident nodes has a little impact on these performance metrics and that the minimum number of CAs to cover the entire platoon.

Keywords: Clustering, Registration Authorities, Security, Stability, Vehicular Networks

INTRODUCTION

A Vehicular ad hoc network (VANET) is an important and a special instantiation of Mobile ad hoc Networks (MANET) aiming essentially to increase road safety, yet it enables vehicles to share pertinent information on the road. To this end, vehicles must be able to route information and inform each other about potential ongoing events on the road. The inherent open architecture of VANETs, however, raises several network vulnerability and security issues. Unlike wired networks which can be protected by several layers of defense such as firewalls, attacks on vehicular networks emanate from different and various sources due to the constraints and requirements imposed on such networks. In particular, nodes or vehicles in VANETs are subject to a high mobility, the trajectories can be predictable and the environment is known as it can either be urban, rural or prescribed highways. Furthermore, obstacles and radio interference are predominant and affect the pattern of mobility and the quality of radio transmissions.
Communication security in VANETs has to take into account several stringent requirements (GWoch et al., 2006; Hubaux et al., 2006; Parno & Perrig, 2005). Firstly, vehicles must authenticate each others, so each driver must have a unique identity. The privacy and anonymity of drivers should, however, be preserved. For example, trying to prevent spoofing in a way that reveals the permanent identity of each vehicle violates privacy requirements and could not be tolerated. Secondly, security solutions in VANETs must insure non repudiation; namely a sender of a message cannot deny having sent such a message. The drivers responsible for an event occurring on the network, an accident for instance, should certainly be identified. Non repudiation is a stringent requirement that enables retracing events in case of an investigation for example. Thirdly, the security in VANETs requires data consistency. Data sent in similar messages should be consistent. The legitimacy of messages requires consistency with other similar messages.

Given that the characteristics of VANETs are different from those of MANETs, security solutions proposed for MANETs cannot be simply and directly transposed to VANETs. They need to be adapted to the nature of this type of networks. In this paper, we propose a secure architecture for VANETs based on previous works proposed for MANETs. Our solution consists on establishing a secure architecture based on an efficient trust model and a distributed clustering algorithm for designing a specific key management system properly adapted to VANETs. The distributed clustering algorithm uses, in particular, two metrics to select a cluster head: security and relative mobility. Furthermore, in order to enhance the security of a cluster, we propose a novel entity called the VANET Dynamic Demilitarized Zone (VDDZ) which is formed by a set of trusted nodes located at 1-hop from the CA in each cluster. The role of this set of nodes is to filter and pre-treat certification requests from unknown nodes thus shielding the CA.

The remainder of the paper is organized as follows. We discuss the related work on current security solutions proposed for VANETs. We then describe our network model, the trust model and the proposed distributed clustering algorithm and present simulation results of the proposed clustering algorithm.

RELATED WORK

PKI in VANET

The significant number of vehicles registered in different countries and their long distance routes, even beyond their regions of recording and licensing, requires a strong and an evolutionary structure for securing communications in VANETs. Therefore, the participation of the authorities in the recording phase of vehicles implies the need of certain level of centralization. Indeed, the communication via base stations is not sufficient for vehicular communications, because vehicles need to communicate with each other (without calling any server). As such, vehicles have to authenticate not only to base stations but also, to one another, which creates a problem of scalability. Hence, given the properties of a large scale and initially low penetration of vehicular communications infrastructure, Public Key infrastructure (PKI), is a good promising choice for enabling V2V security. In fact, PKI ensures secure communications by providing data integrity, confidentiality, strong authentication and non repudiation. It is based on asymmetric cryptography algorithms and Trust Third Parties (TTPs) called Certification Authorities (CA) which is responsible for certifying nodes’ public keys. However, PKI cannot be applied directly in VANETs because it was intended for centralized networks. CAs must be continually available within the network and must be reachable by all nodes on the road. Another challenge in deploying a PKI in MANETs and particularly in VANETs amounts to the open nature of these networks which increases the risk of a single point of
A Novel Approach for Supplying Wireless Energy to Multiple Devices Simultaneously Using Sweeping Effect
www.igi-global.com/chapter/a-novel-approach-for-supplying-wireless-energy-to-multiple-devices-simultaneously-using-sweeping-effect/105671?camid=4v1a