Computers and Electrical Engineering 43 (2015) 33–47

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

An accurate and efficient collaborative intrusion detection framework to secure vehicular networks ☆

Hichem Sedjelmaci *, Sidi Mohammed Senouci

University of Burgundy, DRIVE Lab, 49 Rue Mademoiselle Bourgeois, 58000 Nevers, France

ARTICLE INFO

Article history:
Received 13 October 2014
Received in revised form 24 February 2015
Accepted 27 February 2015
Available online 19 March 2015

Keywords:
Vehicular ad hoc networks
Intrusion detection system
Detection rate
False positive rate
Detection time
Overhead

ABSTRACT

The advancement of wireless communication leads researchers to develop and conceive the idea of vehicular networks, also known as vehicular ad hoc networks (VANETs). Security in such network is mandatory due to a vital information that are managed by the vehicle. Therefore, in this paper we design and implement an accurate and lightweight intrusion detection framework, called AECFV, that aims to protect the network against the most dangerous attacks that could occur on such network. AECFV is suitable for VANET's characteristics such as high node's mobility and rapid topology change. This is achieved with a help of the proposed secured clustering algorithm that considers both node's mobility and network vulnerability during cluster formation. Clusters are constructed with a high stability and good connectivity. Cluster-Heads (CHs) are elected based on both node's mobility and the vehicle's trust-level. The simulation performed using NS-3 simulator shows, AECFV exhibits a high detection rate, low false positive rate, faster attack detection, and lower communication overhead compared to current detection frameworks.

1. Introduction

Vehicle ad hoc networks (VANETs) are attracting much attention from both academia and industry. They are considered as the main system for the deployment of Intelligent Transportation Systems (ITS) based applications. These networks rely on a various types of data collected and/or disseminated from/to vehicles to provide multiple services, which can be sorted in three classes: (i) Road traffic management application such as driver assistance, management of traffic signals, providing information about road and traffic conditions, and route planning. (ii) Traffic safety applications such as self-driving (or autonomous car), prevention and warning of accidents, and emergency management (e-Call for Emergency-Call). (iii) Mobility and comfort application such as point of interest services for vehicles, eco-driving services, management of vehicle fleets services and machine to machine (M2M) services. Securing these networks is an important challenge, especially when traffic-safety applications are deployed. In fact, with these applications, vehicles manage vital and sensitive information that are attractive for attackers. A security mechanism is mandatory to protect VANETs against attacks.

The intrusion detection systems (IDSs) have shown their efficiency to detect internal and external attacks with a high accuracy [1–5]. These systems use special agent nodes to monitor the behavior of a target node and trigger an alarm when a malicious behavior is detected. This paper describes the design and implementation of an accurate and lightweight

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Ayaz Isazadeh.

* Corresponding author.

E-mail addresses: Sid-Ahmed-Hichem.Sedjelmaci@u-bourgogne.fr (H. Sedjelmaci), Sidi-Mohammed.Senouci@u-bourgogne.fr (S.M. Senouci).

http://dx.doi.org/10.1016/j.compeleceng.2015.02.018
0045-7906/© 2015 Elsevier Ltd. All rights reserved.

intrusion detection framework for vehicular networks (AECFV) that takes into account the VANET's characteristics such as high node's mobility and rapid topology change. To handle these characteristics an effective secured clustering[1] algorithm is proposed. This algorithm considers node's mobility during cluster formation, produces clusters with high stability, assures more connectivity between cluster members and elects Cluster-Heads (CHs) based on the vehicles' trust-level. Choosing a cluster-based topology lies in the fact that it is the most appropriate structure for large-scale networks since it allows reducing the broadcast storm and hence decrease the communication overhead [2,6,7].

AECFV aims to secure traffic-safety applications, where the focus is to detect and prevent dangerous attacks that could occur in this application, such as: selective forwarding, black hole, packet duplication, resource exhaustion, wormhole and Sybil attacks. It uses three intrusion detection agents: Local Intrusion Detection System (LIDS) running at cluster member level, Global Intrusion Detection System (GIDS) running at CH level and Global Decision System (GDS) running at Road Side Unit (RSU) level. To detect the malicious vehicle with a high accuracy (i.e. high detection and low false positive rates), the LIDS uses a rules-based detection and GIDS uses a hybrid detection technique (i.e. rules-based detection and anomaly detection based on Support Vector Machine – SVM). The rules based detection relies on a certain rules related to each attack to model a normal behavior and anomaly detection is based on a learning algorithm to model a normal behavior. The combination of these both techniques (i.e. hybrid detection) allow a high detection and low false positive rates [1]. Furthermore, with a help of the proposed detection techniques, a new reputation mechanism is developed that evaluates the trustworthiness level of vehicles according to their behaviors and the information they provide. AECFV suits the following requirements: fast in terms of attacks detection, lightweight in terms of communication overhead, and scalable.

The rest of the paper is organized as follows: In Section 2, we underline previous related work and describe their main shortcomings. In Section 3, we describe our secured vehicular clustering algorithm. Section 4 presents details about our intrusion detection framework AECFV and Section 5 provides NS3 simulation results. In Section 6, we analyze various security aspects of the AECFV. Finally, we conclude the paper and give some perspectives that we envisage to carry out in Section 7.

2. Related work

The intrusion detection system is the most reliable technique to protect vehicular networks against the malicious nodes since it has the ability to detect internal and external attacks with a high accuracy (i.e. high detection and low false positive rates), unlike cryptography mechanisms that prevent only from external attackers to penetrate the network [1,8]. Furthermore, the proposed detection system should take into account the node's high- mobility and frequent network topology change.

Recently, some intrusion detection frameworks have been proposed to address security issues in vehicular networks [2,3,9–13]. In [9], the authors aim to identify the vehicle that provides a false location by applying a set of detection rules. In this scheme, a cooperative detection is applied between intrusion detection agents to identify the malicious vehicle with a high accuracy. To check the claimed position of a monitored vehicle, a packet's Time-of-Flight (ToF) technique proposed by the authors in [10] is used. ToF is defined as the time taken by the packet to arrive at the destination and return back. In their simulations results, their scheme exhibits a high detection rate, high delivery ratio and low packet loss when the number of malicious nodes is large (60 intruders). However, the authors did not take into account collusion issues that can occur in such wireless networks. In fact, when collusions occurred, ToF value computed by the intrusion detection agents will be incorrect. In [11], the authors propose a detection framework to identify the malicious vehicle that provides a false position coordinates. The detection policy proposed by the authors rely on comparing the claimed position of a monitored node and the expected position computed by this IDS, which is based on plausibility model [14]. This latter relies on the vehicle position and movement verification. In this research work, the authors aim to detect two attacks, which are fake congestion and denial of congestion. According to the simulation results, their framework exhibits a high detection rate. In [3], an intrusion detection schema against selective forwarding and false information dissemination attacks is proposed. The detection policy used by this schema relies on *anomaly detection* technique based on a entropy method, which aims to model a normal behavior of a monitored vehicle and any deviation from this model is detected as an attack. According to their simulation results, these attacks were detected with a high accuracy. Furthermore, when the number of attackers increases the performance of the detection frameworks [11,3] degrade significantly (i.e. high false positive rate and low detection rates). In [12], the authors propose a detection framework for VANET called T-CLAIDS that uses an *anomaly based detection technique* to identify the malicious vehicle. This technique uses a learning automat and Markov Chain Model (MCM) approaches to model a normal behavior of node. Combining between these two approaches, the authors prove in the simulation that their approach allows detecting the attacks with a high accuracy. Nevertheless, embedding these both algorithms in a vehicular network could generate a high computation and communication overheads, specifically when the number of vehicles increase. Furthermore, the authors did not define the kind of attacks that were detected.

Recently in [2,7,13], the authors develop a secure cluster-based vehicular network (i.e. the most trusted node at each cluster is elected as a Cluster-Head, CH). Specifically, in [2] the authors propose a detection framework called VWCA to secure a

[1] Clustering architecture aims to group vehicles into a set of clusters, where cluster members communicate with a special node called Cluster-Head (CH).