Vehicular Communications 5 (2016) 9–17

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET

Raghad Baiad [b], Omar Alhussein [a], Hadi Otrok [b,*], Sami Muhaidat [b]

[a] School of Engineering Science, Simon Fraser University, Burnaby, Canada
[b] Department of ECE, Khalifa University, Abu Dhabi, United Arab Emirates

ARTICLE INFO

Article history:
Received 20 February 2016
Received in revised form 10 July 2016
Accepted 1 September 2016
Available online 13 September 2016

Keywords:
Cross layer
VANET
QoS-OLSR
Watchdog
Blackhole attack

ABSTRACT

In this paper, we propose novel cross-layer cooperative schemes for detecting blackhole attack that commonly targets the quality of service secure optimized link state routing protocol (QoS-OLSR) in vehicular ad-hoc networks (VANETs). The QoS-OLSR relies mainly on the multi-point relays (MPRs) that are responsible for establishing the routing among the nodes in the network. Such nodes are victims of the well known attack named as blackhole where packets are intentionally dropped to cause a denial of service. In the literature, watchdogs are used to detect such an attack by utilizing the captured network layer information. Improving the detection performance of such a technique and minimizing the drawbacks due to the high channel collision are the main goals of this work. As a solution, we propose two detection schemes that allow the information to be exchanged across two and three layers respectively. The first scheme utilizes the information among physical and network layers, while the second one relies on the physical, MAC and network layers to enable an efficient and reliable detection. In the physical layer detection technique, each legitimate user is assigned a signature key that is multiplied by the message, and each monitoring node uses the maximum likelihood approach to determine whether the message is legitimate or not. On the other hand, the MAC detection technique monitors the number of RTS/CTS (request to send/clear to send) requests among all the neighbors while the cooperative watchdog technique is implemented at the network layer to overhear the transmitted exchanged packets among the neighbors. Simulation results are conducted to show that utilizing a cooperative cross layer design enhances the detection rate and minimizes the false alarm rate compared to other contemporary state-of-the-art detection schemes.

1. Introduction

Recent research advances in information and wireless technologies have led to growing interests in the development of intelligent transportation systems (ITSs). These systems promise significant improvements in road safety and traffic flow, and shall enable new data services. As being a key component of ITS, vehicular ad-hoc networks (VANETs), including inter-vehicular communications and vehicle to infrastructure communications, are attracting attention in both industrial and academic communities [1,2]; due to its huge commercial potential. Yet, VANETs present several challenges, particularly in aspects related to security and privacy. Therefore, many works have been proposed to address these issues. In [3] Georgios et al. indicate that most recent promising applications in vehicular networks are the security concepts. In [1], the authors propose a security technique that depends on cryptographic primitives and plausibility checks to mitigate false position injection. However, these schemes suffer from a huge distinction between efficiency and security, where one is implemented in account of the other. In [4], Raya et al. propose an algorithm to balance between efficiency and security. Their algorithm depends on relaying the information among vehicles. Thus, the focus is on message aggregation, in which there are three main major classes, namely combined signatures, overlapping groups, and dynamic group key creation. In this paper, we take this existing compromise between security and efficiency into account.

VANET's quality of service optimized link state routing (QoS)-OLSR [5] protocol is proposed to form a stable vehicular network. It is taken from the classical OLSR protocol [6], where the multi-point relays (MPRs) are selected by the normal nodes to broadcast the network topology information. The idea behind this protocol is to divide the network into clusters, where each cluster is com-

* Corresponding author. Fax: +971 (0)2 447 2441.
E-mail addresses: raghad.baiad.ae@ieee.org (R. Baiad), oalhusse@sfu.ca (O. Alhussein), hadi.otrok@kustar.ac.ae (H. Otrok), sami.muhaidat@kustar.ac.ae (S. Muhaidat).

http://dx.doi.org/10.1016/j.vehcom.2016.09.001
2214-2096/

posed of a cluster head (CH) for each group of neighbor nodes located in the same transmission range called voters. To partition the network into clusters and elect a set of optimal cluster heads, each node votes for its neighbor which has the highest QoS value. A node can also vote for itself, if it has the maximal QoS value. The nodes use their Hello messages to broadcast their votes. This solution yields a one-hop clustering model. Each node is one-hop away from its designated cluster head. Once the election algorithm is performed, the CHs select a set of multi-point relays (MPRs) that connect various clusters together and reduce the overhead messages by minimizing the number of transmissions. In this protocol, there exists a tradeoff between QoS requirements and high speed mobility constraints.

In this work, we assume the VANET QoS-OLSR protocol [5] which although provides efficiency in terms of connection, still vulnerable to several types of attacks, such as wormhole and blackhole attacks. A blackhole attack [7] is categorized as a packet drop attack, where the attacker node exploits the routing protocol and advertises itself as a legitimate relay to the destination node. Once it receives the data packets, it starts discarding them without necessarily informing the source [8], thus compromise the security of the network routing. To that end, various techniques are proposed to detect blackhole attacks. They can be classified based on the nature of their operation into three main categories, namely acknowledgment (ACK)-based [9], reputation-based [5,10], and detection-based [11,12] schemes. It is worth mentioning that most of the works proposed in the literature adopt the third category.

Watchdog monitoring technique is widely implemented due to the fact that it is independent on the utilized routing protocol or technology. There, the monitoring nodes maintain a buffer of recently sent packets and compare each incoming overhead packet with the ones in the buffer to validate if a match exists [11]. However, watchdog provides detection only at the routing level which puts limitations on this technique and leads to high probability of false positives, mainly due to: (1) Watchdogs at the routing level are not able to determine whether a packet dropping event is due to packet collisions or an attack; and (2) They are not able to detect accurately if the watchdogs themselves have problems. With the aforementioned limitations of the watchdog technique, our main dilemma in blackhole detection is that one needs to determine whether packet drops are due to an attack or just a mere collision. Therefore, further techniques should be proposed to fix the aforementioned network layer detection technique limitations.

Many solutions in recent works consider the joint optimization of important system parameters residing in different IOS layers systematically to achieve the best detection capability. For instance, in [13], the authors propose a modular cross layer intrusion detection which makes use of the context information from different layers and sources. On every node, different modules are in charge of collecting audit data from different layers, namely the network and application layers. At the network level, the nodes are responsible for collecting data from neighboring nodes for forwarding attitudes, whereas at the application layer level, they are responsible on receiving warning messages. Subsequently, a local decision is made with the aid of additional information available from other devices, such as the GPS system. Moving to [14], IEEE wireless access in vehicular communication (WAVE) cross-layer message verification scheme is proposed to verify the safety application on the received message. The verification mechanism consists of signature generation, transmission of a periodic safety message, and verification of the received message. In [15], a novel detection system is designed to perform two levels of detection by analyzing the pattern of trace files. However, to the best of our knowledge, none of the mentioned schemes provide a real evaluation in detecting real attack. Also, there is no cross layer scheme proposed in the literature that takes the trade-off between network connectivity and security.

In this paper, we propose novel cooperative cross layer based intrusion detection schemes (IDSs) to enhance the performance of the watchdog detection technique in tackling blackhole attack. It is noted that in the literature, the terms *cooperative* and *cross layer* are sometimes used interchangeably. Here cooperative refers to the cooperation between nodes in the network, while cross layer refers to the information exchange that occurs between the three different layers. Our main focus is on the development of detection techniques designed for assisting watchdog monitoring in blackhole attack, whereby the cooperative and cross layer approach shall enable us to further minimize the intrinsic increase in the false-alarm rate, and thus, enhance the overall detection performance. We approach this by introducing the individual intrusion detectors for each layer, and then, we propose two cross layers detection schemes, and lastly integrate them together to build a reliable and efficient IDS scheme.

In what follows, we briefly describe each local detector. First, for the physical layer, we propose a signature key based detector, where each legitimate user is provided with a signature key. Then, by utilizing the maximum likelihood test and based on the signature key, a monitoring node decides whether a received signal is from a legitimate user or an intruder. If the signal is determined to be from an intruder, then the signal is dropped. Otherwise, the signal is passed to the next layer of defense, namely the network layer. It is worth noting that depending solely on the physical layer detector would not be sufficient since high noise levels or physical channel interference may lead to a detection error. As a second layer of defense, in the network layer, we implement the aforementioned watchdog technique to further decide the authenticity of the received signal. Lastly, in the MAC layer, we count and compare the number of sent RTS packets to the number of received CTS packets. If a discrepancy is detected, we indicate that the packet loss is due to collision and not an intrusion. The proposed ID schemes also utilize cooperation between watchdogs located at the same cluster and monitoring nodes from other layers. This is achieved by allowing the monitoring nodes to overhear the communications between other nodes, and therefore, build a final unified decision. The main contribution of this work is a novel cross layer detection framework that can improve the detection against Blackhole attack targeting QoS-OLSR protocol. Such a cooperative framework will be able to reduce the false alarm rate generated due to collisions and falsely reported detection. Our schemes are able to increase the detection rate and minimize the false alarm rate compared to the work proposed in the literature. Simulations are conducted, using Matlab, to evaluate the performance and robustness of the proposed schemes.

The rest of this paper is organized as follows: Section 2 demonstrates the problem statement which identifies the need to develop novel cooperative cross layer based approaches. While the proposed cooperative cross layer techniques are introduced in Section 3. Finally, simulation results are shown in Section 4, while Section 5 concludes this work.

2. Problem statement

One of the foremost challenges in VANETs is to design routing protocols that can handle the high mobility of vehicles and constant changes in the underlying topology [16]. In the proposed schemes, we adopt the VANET QoS-OLSR protocol which is proposed in [5]. However, in addition to that model we take into account the direction of the node during the cluster head selection process which provides a more realistic scenario. Cluster head selection process is based on the maximum quality of service value, where each node votes for itself and the nodes in its transmission