Journal of Network and Computer Applications 35 (2012) 1130–1139

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

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

Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks

Abderrahmane Baadache *, Ali Belmehdi

Laboratory of Industrial Technology and Information, University of A. Mira, Targua Ouzemour, Bejaia 06000, Algeria

ARTICLE INFO

Article history:
Received 7 March 2011
Received in revised form
4 November 2011
Accepted 29 December 2011
Available online 14 January 2012

Keywords:
Wireless ad hoc network
Packet droppers
Selfish
Black hole
Cooperative black hole

ABSTRACT

In multi-hop wireless ad hoc networks, the packets are forwarded through intermediate nodes along the source–destination path. Without having any control on packets forwarding, an intermediate node can behave selfishly or maliciously to drop packets going through it. The dropper motivation is the preservation of its resources, like its limited energy (selfish behavior) or the launch of denial of service attack (malicious behavior). In this paper, we propose an approach to verify the correct forwarding of packets by an intermediate node. The Merkle tree principle has been used for implementation in justification of our proposed approach. Through simulation, we have shown our approach efficiency, and we have evaluated its performance in both proactive and reactive routing protocol in ad hoc network. Also, we have compared our approach with the watchdog and the 2-hop ACK which are well-known approaches in the literature.

1. Introduction

A wireless ad hoc network is a collection of nodes using a wireless medium to communicate, and cooperate together to make possible the communication between any pair of nodes in the network, without using any pre-existing infrastructure or central administration. Military or civilian applications of ad hoc networks have different requirements on what an ad hoc network should offer to them, but both applications require security and reliability as quality criteria of such a network. The opening of the communication medium and the possible mobility are the most important characteristics, which make an ad hoc network easy and less expensive to deploy. But in return, these characteristics make the network more vulnerable to various security attacks.

Broadly speaking, securing an ad hoc network is ensuring mutual authentication of participants, confidentiality and integrity of exchanged data, availability of the network resources, access control to the communication medium and the anonymity. Cryptographic tools such as digital signature, public key encryption, and non-cryptographic tools such as Intrusion Detection System (IDS), have been used to implement such security services. Despite the diversity of existing security solutions in the literature, but a perfect security is still far from clear.

In this paper, we focus on an attack in which an intermediate node drops packets passing through it. The motivation of the dropper node is the preservation of its resources, such as its limited battery, while at the same time using the resources of others to deliver its data. It is qualified as selfish node in this case. A denial of service attack can be the aim of the dropper node to destruct the end-to-end communication. The dropper node is qualified as malicious node in this case. To carry out its attack, the dropper node must firstly be in the path between the source and the destination nodes, then it drops packets going through it. According to the routing protocol used in the network, the manner in which the dropper node behaves is different. In Section 3, we will explain how the dropper node conducts a successful attack in AODV (Perkins et al., 2003), which is a reactive routing protocol, and in OLSR (Clausen and Jacquet, 2003) which is a proactive routing protocol.

Our approach is based on the following idea: Let A, B and C be three nodes which succeed in the data path. The node A holds the value δ precalculated from values α (owned by A), β (owned by B) and λ (owned by C). To acknowledge the message *msg* sent from A through B, the node C sends back its value λ to B, and B sends back the received value λ and its value β to A. When A receives β and λ, it recalculates δ from α (its own value), β and λ. If the recalculated value δ is the same that already held, so *msg* was well delivered by B, else B is a possible dropper node. To implement this idea, we have used the principle of Merkle tree (Buchmann et al., 2008). Through simulation, we have shown the efficiency and evaluated the performance of our approach. Also, we have compared our approach with the watchdog (Marti et al., 2000) and the 2-hop

* Corresponding author. Tel.: +213 661 766 422.
E-mail addresses: abderrahmane.baadache@gmail.com (A. Baadache), ali.belmehdi@gmail.com (A. Belmehdi).

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.12.012

acknowledgment (2-hop ACK) (Djenouri and Badache, 2008, 2009) approaches which are well-known approaches in the literature.

The remainder of this paper is organized as follows: Section 2 introduces the previous work that has been done in the area, followed by Section 3 which presents the attack model. Section 4 describes how our approach copes with the packet droppers, followed by Section 5 where we show the detection efficiency, evaluate the performance of our approach and compare it with similar works. Finally, we conclude and highlight future directions.

2. Related work

The packet dropping attack has certainly a negative impact on the network functioning. Sharma and Gupta (2009) provided a simulation study in which an AODV-based network performance, in the presence of packet droppers, is reduced up to 26%. Another simulation study performed by Marti et al. (2000) shown that if 10–40% of nodes misbehave on packets forwarding, then the average in the network's throughput degrades by 16–32%. For demonstrating that an effective protection against selfish and malicious nodes is absolutely mandatory for ad hoc networks, Kargl et al. (2004) have done a number of simulations, where they modeled a varying number of selfish nodes, with node mobility speed ranging from 1 m/s to 20 m/s. The obtained result confirms that, the number of selfish nodes has a negative effect on the rate of packets that are successfully delivered in the network. Also, the simulation study performed in Buttyán and Hubaux (2003) has revealed a similar result on the throughput of the network, which decreases as the fraction of less cooperative nodes increases. Based on these simulation studies, we conclude that the effect of droppers nodes on the network functioning is undoubtedly negative, and that a solution which address this attack is necessary.

Several terms have been used by researchers to designate the packet dropping misbehavior. Black hole is the term that designates an attack in which the dropper node drops all packets passing through it. Gray hole is the one in which packets are dropped selectively. Selfish or egoistic is the attack in which packets are dropped for preserving the dropper's resources, while the resources of others are used to deliver its packets. Other terms like dropper and cheater are used also. Since the malicious action is always the packet dropping, we preferred to use *dropper node* as term, which we will use it in the remainder of the paper. Various approaches for mitigating, preventing, detecting, minimizing, isolating or eliminating packet droppers were proposed in the literature. These approaches could be classified into two main categories: detective or preventive approaches.

2.1. Detective approaches

Detective approaches are those in which the dropper node is detected and eventually eliminated when it appears in the network. In Marti et al. (2000), the watchdog and pathrater mechanism is proposed for mitigating routing misbehavior. In each node, the watchdog monitors the successor node, after sending to it a packet, by overhearing the channel and checking whether it relays or drops the packet. The pathrater accuses a monitored node for misbehaving if this latter drops more than a given number (threshold) of packets. This mechanism presents several weakness that are listed in Djenouri and Badache (2006). Djenouri and Badache (2008) propose a monitoring approach that overcomes some watchdog and pathrater's shortcomings. Like the watchdog, in this solution, each node *A* monitors its successor *B* which must carry the message to its successor *C*. In addition, the node *C* acknowledges *A*'s messages sent through *B*, using 2-hop ACK, and for that the node *A* generates a random number and encrypts it with *C*'s public key (*PK*). Upon receiving it, *C* decrypts it using its secret key (*SK*), which encrypts it using *A*'s *PK* and sends back it, in a 2-hop ACK, to *A* via *B*. We note that this approach uses the asymmetric cryptography, that requires a key distribution mechanism for enabling a security association between each pair of nodes. Promiscuous Listening Routing Security Algorithm (PLRSA) Li and Lee (2006) is also a monitoring approach, in which every node keeps a local connectivity list (LCL) to record all nodes in its communication range, and maintains this LCL by promiscuously monitoring all packets passing through it. Furthermore, LCL maintains a trust level value, updated dynamically for any node in LCL. If the value of trust level is lower than an already defined threshold, the node may be considered as a malicious one by PLRSA. Deng (2002) propose a routing security protocol whose principle is to send back, with the reply message, its next hop information to the source when an intermediate node replies to a request route. To verify whether the next hop has a link with the intermediate node, which sent back the reply message, the source sends a further request packet to the next hop, and this latter should send back a further reply message which includes the check result. If intermediate node's next hop ensures that the intermediate node exists, the source starts to establish a route to the destination through this intermediate node. Djenouri and Badache (2009) suggest a modular solution structured around five modules. The first one is the monitor which controls packets forwarding. The second module is the detector of monitored nodes misbehavior. The third module is the isolator of detected misbehaving nodes. The fourth module is the investigator which investigates accusations before testifying when the node has not enough experience with the accused one, and the last module is the witness which responds to testimony requests of the isolator.

Some dedicated approaches for particular routing protocols have been proposed. Focused on Ad hoc On-Demand Distance Vector (AODV) (Perkins et al., 2003) routing protocol, Kurosawa et al. (2007) try to detect abnormality which occurs during the packet dropping attack by defining a normal state from dynamic training data that is updated at regular time intervals. To express the state of the network, the following features are used: number of sent out route request (RREQ) messages, number of received route reply (RREP) messages, and the variation of the sequence number value, used by AODV to determine the route freshness degree. Raj and Swadas (2009) propose a solution for AODV, in which the receiving node of RREP message compares the sequence number value with a dynamic updated threshold. If the sequence number value is found to be higher than the threshold value, the node is suspected and blacklisted. Here, the threshold considered can miss exactitude what brings back to false alarms. Hongsong et al. (2006) propose an intrusion detection model to combat the black hole attack in AODV. In this model, a security agent tries to detect two cases of attack. Those exploiting AODV control messages RREQ and RREP. The agent monitors the RREQ–RREP messages at real-time and if any detection rule is violated, the black hole attack is detected and the malicious node is isolated and blacklisted.

A cooperative attack is when several droppers nodes work together as a group for launching packet dropping attack. Agrawal et al. (2008) propose a complete protocol to detect a chain of cooperating malicious nodes in an ad hoc network. The proposed protocol is based on sending equal and small sized blocks of data and monitoring the traffic flow at the neighborhoods of both source and destination, then gathering results of monitoring by a trusted backbone network, with the assumption that a neighborhood of any node has more trust than malicious nodes. Djahel et al. (2008) investigate the effects of the cooperative packet