Computer Networks 73 (2014) 173–184

Contents lists available at ScienceDirect

Computer Networks

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

Struggling against simple and cooperative black hole attacks 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 19 November 2011
Received in revised form 20 November 2013
Accepted 22 July 2014
Available online 20 August 2014

Keywords:
Wireless ad hoc network
Routing protocol security
Simple black hole
Cooperative black hole

ABSTRACT

In multi-hop wireless ad hoc networks, nodes not in direct range rely on intermediate nodes to communicate. In order to preserve its limited resources or to launch a DoS attack, an intermediate node drops packets going through it instead to forward them to its successor. In this paper, we deal with this misbehavior called black hole attack, and we propose an authenticated end-to-end acknowledgment based approach in order to check the correct forwarding of packets by intermediate nodes. Our approach detects the black hole conducted in simple or cooperative manner, the modification and the replay of messages attacks. Through simulation using OPNET simulator, we show the detection efficiency and evaluate the performance of our approach in both proactive and reactive routing based networks in terms of end-to-end delay and network load. Also, we compare the approach we propose with 2-hop ACK and the watchdog approaches in terms of detection ratio, delivery ratio and additional overhead.

1. Introduction

A multi-hop wireless ad hoc network is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network. It can be easily and rapidly deployed without the aid of any established infrastructure or centralized administration. Such network has some special features such as open and unreliable wireless links, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes. While these features make the network more flexible, they introduce specific security concerns. Indeed, an ad hoc network is vulnerable to various types of attacks including passive eavesdropping, impersonation, and denial-of-service. Preventive or detective security measures using cryptographic tools such as digital signature, public key encryption, and non-cryptographic tools such as Intrusion Detection System (IDS), can improve the security of the network. However, these techniques can address only a subset of the threats, and the problem remains always open and the remedy is far from being obvious.

In multi-hop wireless ad hoc networks, the cooperation amongst nodes is essential to deliver packets to the destination node. An intermediate node, that participates voluntarily in routing and packets forwarding operations, can behave selfishly or maliciously to drop packets going through it, instead of forwarding them to its successor. The dropper aim is the preservation of its resources like its limited energy (selfish behavior), or the launch of denial of service attack (malicious behavior). This misbehavior, called black hole attack, can be conducted by one intermediate node (simple black hole) or results on the cooperation of several intermediate nodes (cooperative black hole). To cope with this attack, existing approaches are mainly based on monitoring individual nodes, and they

* Corresponding author.
E-mail addresses: abderrahmane.baadache@gmail.com (A. Baadache), albelem@yahoo.fr (A. Belmehdi).

http://dx.doi.org/10.1016/j.comnet.2014.07.016
1389-1286/

focus on the black hole conducted in single or cooperative manner, but not both simultaneously. In this paper, we propose an end-to-end authenticated ACK based approach to check the correct forwarding of packets by intermediate nodes. Our main goal is the detection of simple and cooperative black hole attacks, and as a secondary objective, we detect the modification and the replay of messages. We note that the modification and the replay of messages, completely ignored in existing approaches, are essential to deliver packets to the destination node. Through simulation we show the detection efficiency and evaluate the performance of our approach in terms of end-to-end delay and network load in both AODV [18] and OLSR [19] based networks. Also, we compare the approach we propose with the 2-hop ACK (Two hop acknowledgment) [3,5,14] and the watchdog [24] approaches in terms of detection ratio, delivery ratio and additional overhead.

The remainder of this paper is organized as follows: Section 2 summarizes the related work. Section 3 describes how simple and cooperative black hole attack are conducted. Section 4 presents our approach. We analyze and discuss simulation results in Section 5. Finally, we conclude the paper in Section 6.

2. Related work

The black hole attack causes a serious damage on the network. In [2], authors provided a simulation study in which an AODV-based network performance, in the presence of black hole nodes, is reduced up to 26%. To cope with this attack, researchers proposed solutions against black hole attack acting in an individual or a cooperative manner, or they proposed security mechanisms to cope with other attacks additionally to the black hole attack.

Deng et al. [20] propose a routing security protocol, where the intermediate node sends back to the source its next hop information with the reply. To verify whether the next hop has a link with the intermediate node, the source sends a further request packet to the next hop. The latter should send back a further reply message which includes the check result. If the next hop ensures that the intermediate node exists, the source starts to establish a route to the destination through this intermediate node. This protocol generates an important overhead due to further request and reply packets. Authors in [3] suggest a modular solution structured around five modules: first is a monitoring module to control packets forwarding, second module detects monitored nodes misbehavior, third one isolates the detected misbehaving nodes whereas fourth module investigates accusations before testifying whether the node has not enough experience with the accused and the fifth module responds to witness requests of the isolator. In [13], Hongsong et al. propose an intrusion detection model to combat the black hole in AODV. In this model, a security agent is used to detect attacks that exploit the route request (RREQ) and the route reply (RREP) packets. The agent monitors RREQ and RREP packets at real-time. If any detection rule is violated, the black hole is detected and blacklisted. Authors in [11] try to detect abnormality that occurs during the black hole attack in AODV-based network. To do that, a normal state is defined from a dynamic training data updated at regular time intervals. To express the state of the network, the following features are used: the number of sent out RREQ packets, the number of received RREP packets and the variation of the sequence number used by AODV to determine the route freshness degree. Although this method is effective, but a high processing overhead is needed for its implementation, which makes it not scalable. In [4], authors propose a solution, where the receiving node of RREP message compares the sequence number to a dynamically updated threshold. If the sequence number is higher than this threshold, the node is suspected and blacklisted.

Cooperative black hole is when several malicious nodes work together as a group. To identify multiple black hole nodes acting in cooperation, authors in [6,17] propose a slight modification in AODV, where a Data Routing Information (DRI) table is used to save information on routing data packet from/through the node. The DRI helps to determine reliable nodes used to discover secure paths from source to destination. In [7], authors use a data structure called fidelity table, wherein every participating node will be assigned a fidelity level to measure its reliability. If the fidelity level decreases to 0, the corresponding node is considered as black hole attacker. Agrawal et al. [8] propose a complete protocol, which consists in sending an equal and small data blocks and monitors the traffic flow in the neighborhoods of both source and destination nodes. Later, monitoring results are gathered by a trusted backbone network in order to detect a chain of cooperating malicious nodes. Authors in [9] investigate the impact of the cooperative black hole attack against OLSR [19], and they propose an acknowledgment based scheme to mitigate the loss of topology information due to the dropping of topology control (TC) messages. Two kinds of messages are used, 3hop-ACK message which is used to acknowledge the reception of a TC message from the 3-hop neighbors, and HELLO-rep message used to advertise the 2-hop neighbors to a requesting MPR node. In [1], authors propose an ACK based approach, in which all nodes from the source to the destination need to acknowledge the packet reception. Based on these ACKs, the source node constructs a binary tree in order to check the forwarding of packets, and hence, avoids black hole nodes.

In [24], authors propose the watchdog and pathrater mechanism to mitigate the dropping packets misbehavior. The watchdog principle is that each node monitors its successor after sending a packet to it, 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 of packets. Using this mechanism, it is impossible to detect the cooperative black hole attack. Indeed, the first malicious node seems to forward well the traffic to the second one, which is supposed to be monitored by the first malicious node. The latter does not forward the traffic but the earlier one, also being malicious, does not report this misbehavior to the source of the traffic. In [5], authors propose a monitoring approach that overcomes some of watchdog's shortcomings. In this solution, each node monitors its successor and an authenticated 2-hop ACK is used to acknowledge received messages. In [12], authors propose