Journal of Computer and System Sciences 80 (2014) 644–653

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Detection and mitigation of sinkhole attacks in wireless sensor networks

H. Shafiei [a,*], A. Khonsari [a,b], H. Derakhshi [a], P. Mousavi [a]

[a] Department of Electrical and Computer Engineering, University of Tehran, Tehran, Iran
[b] School of Computer Science, IPM, Tehran, Iran

ARTICLE INFO

Article history:
Received 30 November 2012
Received in revised form 30 April 2013
Accepted 14 June 2013
Available online 2 July 2013

Keywords:
Sensor networks
Security
Sinkhole attack

ABSTRACT

With the advances in technology, there has been an increasing interest in the use of wireless sensor networks (WSNs). WSNs are vulnerable to a wide class of attacks among which sinkhole attack puts severe threats to the security of such networks. This paper proposes two approaches to detect and mitigate such attack in WSNs. It provides a centralized approach to detect suspicious regions in the network using geostatistical hazard model. Furthermore, a distributed monitoring approach has been proposed to explore every neighborhood in the network to detect malicious behaviors. Our simulation experiments validate the correctness and efficiency of the proposed approaches.

1. Introduction

Wireless sensor networks (WSNs) have drawn fair amount of research attention during last decade. Their limited resources along with the hostile deployment environment put severe challenges to the research studies. Various aspects of such networks have been already studied and these types of networks are now well-established for many applications ranging from habitat monitoring to surveillance [1].

Security is a vital concern in WSNs. Without availability, data confidentiality and integrity many real-world applications of WSNs are in vain. As a result, many studies have been focused on providing security solutions for these networks [2].

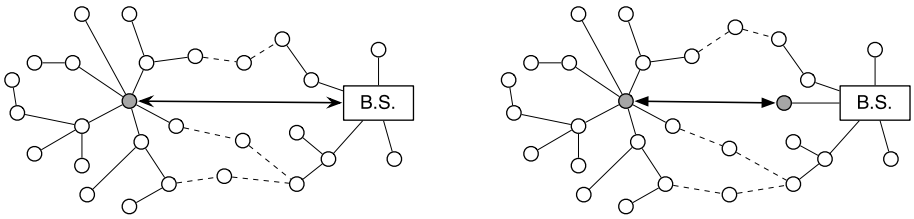
Detection and mitigation of attacks against WSNs has been an attractive topic amongst researchers, especially, considering the unique challenges of these networks which are mainly imposed by their resource constraints. Many types of attacks have been introduced, analyzed and eliminated in the literature [2,3]. Sinkhole attack is one of the earliest among them that has been identified in WSNs [4].

Sinkhole attack threatens the security of WSNs at almost every layer of their protocol stack. The main deception of the attack is that a malicious node attracts the traffic of its neighbors by pretending that it has the shortest path to the base-station. The attack may jeopardize many important security measures. The sinkhole may launch a variety of attacks against the data traffic, such as selectively dropping the data packets, tampering data aggregation algorithms or interfering with clustering protocols. Various approaches have been proposed to combat the attack either by manipulation of routing algorithms [5,6] or by utilization of an IDS [7,8].

In this paper we propose two approaches to detect the sinkholes in the network. The rationale behind these approaches is that the nodes around the sinkhole deplete their energy faster than other nodes since the routes to the base-station that pass through sinkhole are more attractive thus are used more frequently. Thus, an *energy hole* forms around each sinkhole. In the first approach the base-station utilizes a geostatistical method to sample the residual energy of every sensing region

* Corresponding author.
E-mail addresses: h.shafiei@ut.ac.ir (H. Shafiei), ak@ipm.ir (A. Khonsari), h.derakhshi@ut.ac.ir (H. Derakhshi), pa.mousavi@ut.ac.ir (P. Mousavi).

0022-0000/$ – see front matter
http://dx.doi.org/10.1016/j.jcss.2013.06.016



(a) An example of sinkhole attack. Shaded node (sinkhole) delivers packets to the base-station.

(b) An example of sinkhole attack using wormhole. Shaded nodes conduct a wormhole tunnel.

Fig. 1. Various types of sinkhole attacks.

and estimates the possibility of existence of the sinkhole in each region using an extracted statistical estimator. Based on the value of the estimator, the base-station instructs all of the nodes to avoid the suspicious region in their routing. The second approach is a distributed monitoring method to detect regions with lower average residual energy level. Our contribution can be summarized as follows:

- A geostatistical hazard model has been proposed to estimate energy holes.
- We introduce a centralized model to detect sinkhole attacks based on the proposed hazard model.
- A distributed monitoring approach has been proposed to explore every neighborhood in the network to detect energy holes.
- An analytical model is provided to capture the interactions between various contributing parameters in the proposed detection methods.
- We describe a lightweight mitigation method to eliminate sinkholes.
- Finally, we provide extensive simulations to verify the obtained results.

The sinkhole attack can be considered as an intrusion to the victims' normal mode of operation, and thus, our proposed approaches to detect and mitigate the attack can be viewed as an IDS.

The rest of the paper is organized as follows. We first describe related works in Section 2. Two detection approaches have been introduced in Section 3. Section 4 describes the mitigation approach. Section 5 presents extensive simulation results. Finally, Section 6 provides some concluding remarks and outlines directions of future research.

2. Background and related work

2.1. Sinkhole attack

WSNs are susceptible to a wide class of attacks among which sinkhole attack has been identified as one of the serious threats. In this type of attack, a malicious node advertises itself as a best possible route to the base-station which deceives its neighbors to use the route more frequently. Thus, the malicious node has the opportunity to tamper with the data, damage the regular operation or even conduct many further challenges to the security of the network.

Two types of attackers may establish sinkhole attacks; a malicious insider or a resourceful outsider. In the former case, an adversary utilizes a compromised node to launch the attack in which a route is advertised to deceive neighbors. In the latter case, a laptop-class adversary equipped with high performance computation and communication capabilities conducts a single-hop route from its surrounding region to the base-station which convinces the neighbors to forward all the traffic through such route. Furthermore, the high quality route not only attracts the neighbors of sinkhole but also it attracts almost all the nodes that are closer to the sinkhole than to the base-station (may be from several hops away) which amplifies the threat. Fig. 1(a) depicts a sinkhole attack.

The sinkhole also can be conducted using wormhole attack. In this type of attacks, a malicious node first captures a routing packet from one of its neighbors and utilizes a secret tunnel to send the packet to another colluded node. The colluded node eventually delivers the message to the base-station. Even though the two ends of the tunnel may be at a longer distance compared with other routes, it can prevent the source from discovering other legitimate routes greater than two hops away from the destination and thus disrupts network functionality. Fig. 1(b) illustrates an example of such attack.

Various research studies have been focused on detection and mitigation of the sinkhole attack [5–10]. Ngai et al. [9] propose a lightweight algorithm to detect sinkhole attacks. In their approach the base-station collects the network flow information using a distributed approach, and then an identification algorithm analyzes the collected data to locate the sinkhole. Their work also considers a case in which there exist multiple colluded attackers in the network. [10] utilizes a dynamic trust management system to counter such attacks. A distributed network-coding-based approach to detect security attacks related to routing has been proposed in [5]. In [6] authors propose a method to detect sinkhole attack using LQI-based routing. In another interesting approach Krontiris et al. [7] propose an IDS system to detect such attacks. The