Chapter 55
Security Issues on Outlier Detection and Countermeasure for Distributed Hierarchical Wireless Sensor Networks

Yiying Zhang
Shenyang Institute of Engineering, China

Lei Shu
Osaka University, Japan

Lin He
Korea University, South Korea

Takahiro Hara
Osaka University, Japan

Shojiro Nishio
Osaka University, Japan

ABSTRACT

Outliers in wireless sensor networks (WSNs) are sensor nodes that launch attacks by abnormal behaviors and fake message dissemination. However, existing cryptographic techniques have difficulty in detecting these outliers, which makes outlier recognition a critical and challenging issue for reliable and secure data dissemination when outliers exist in WSNs. This chapter is concerned about detection and elimination problems of outlier. To efficiently identify and isolate outliers, we present a novel "Outlier Detection and Countermeasure Scheme" (ODCS), which consists of three mechanisms: (1) An abnormal event observation mechanism (AEOM) for network surveillance; (2) An exceptional message supervision mechanism (EMSM) for distinguishing fake messages by exploiting spatiotemporal correlation and consistency; (3) An abnormal frequency supervision mechanism (AFSM) for the evaluation of node behavior. The chapter also provides a heuristic methodology which does not need the knowledge of normal or malicious sensors in advance. This property makes the ODCS not only to distinguish and deal with various dynamic attacks automatically without advance learning but also reduces the requirement of capability for constrained nodes. In our solution, the communication is limited to a local range, such as one-hop or a cluster, which can reduce the communication frequency and circumscribe the session range further. Moreover, the chapter also provides countermeasures for different types of attacks, such as the rerouting scheme and the rekey security scheme, which can separate outliers from normal sensors and enhance the robustness of network, even when some nodes are compromised by adversary. Simulation results indicate that our approach can effectively detect and defend the outlier attack.

DOI: 10.4018/978-1-4666-4707-7.ch055

INTRODUCTION

Wireless sensor networks (WSNs) can effectively employ different applications by collecting sensory information in unattended and often adversarial environments such as enemy detection in battle fields, or fire monitoring in urban areas (Aggarwal, 2001). Therefore, the security provision of confidentiality and authentication is a critical requirement for many wireless sensor network applications. However, sensor nodes are highly constrained in transmission power, on-board energy, processing capacity and storage, which requires careful resource management. Due to these limited resources and operation in hostile environments, WSNs are subjected to numerous threats and are vulnerable to attacks from inside, e.g., outliers (Akyildiz et al., 2002), (Sheng et al., 2007), (Liu, Cheng, & Chen, 2007), (Zhang et al., 2010), or from outside, e.g., eavesdropping (Bandyopadhyay & Coyle, 2003).

In this chapter, we focus on the outliers. The outliers are severely destructive to the function of WSNs. Since the outliers usually occupy the same network source as normal nodes, they can easily manufacture the fake messages or tamper with the real messages to impact the performance of network. However, the traditional techniques, such as cryptographic encryption, authentication etc., cannot detect and eliminate all attacks.

Although most of previous security works focus on outside attacks and try to establish a credible relationship among sensor nodes in WSN based on the traditional cryptography (Akyildiz et al., 2002), (Bandyopadhyay & Coyle, 2003), (Bellare, Canetti, & Krawczyk, 1996), (Branch et al., 2006), (Breunig et al.,2000), (Chan, Perrig, & Song, 2003), (Chang & Kuo, 2006), (Chen et al., 2002), (David et al., 2004), (Deng, Han, & Mishra, 2005), which cannot support sufficient protection from all attacks, especially outliers from outlier. Thus, it becomes very urgent and challenging to design an outlier detection scheme. In this chapter, we present a novel outlier detection scheme as well as a series of countermeasures.

PROBLEM STATEMENT

Outliers (also called Inside attacker) in WSNs are some sensor nodes controlled by adversary, they do not perform tasks as normal nodes but exhibit different types of abnormal behaviors, e.g., dropping received messages from their neighbors, forwarding messages to enemy, broadcasting redundant messages, and disseminating fake messages (Akyildiz et al., 2002), (Liu, Cheng, & Chen, 2007). The outlier has the same network resource as a normal sensor node, but its behaviors are different. Typically, outliers are compromised and remote-controlled by adversary. Outliers also attack WSNs by tampering with messages transferred in WSNs or generating bogus messages and forwarding them to critical nodes (e.g., aggregation nodes or sink node), which typically reduces network performance in terms of reliability and security because of the following consequences (Bandyopadhyay & Coyle, 2003):

1. Wasting network bandwidth;
2. Increasing energy consumption;
3. Interfusing illegal messages into sensory data streaming;
4. Causing communication obstruction or dynamic holes.

However, although the outliers seriously threat the network, they are difficult to be detected by traditional cryptographic techniques for the attacks come from network inside (Ash & Moses, 2005). Outliers usually could obtain all or part of the security materials, such as keys, which makes it easy for the outlier to tamper with, inject or eavesdrop messages in network. Thus, it is critical to establish an efficient secure and reliable scheme to detect and prevent outliers. The conventional methods such as encryption, authentication, etc. have the ability to protect the correctness and integrity in WSN. However, they cannot withstand outliers' attacks.