Chapter 5
Attacks in Wireless Sensor Networks

George William Kibirige
Department of Informatics, Sokoine University of Agriculture, Tanzania

Camilius A. Sanga
Department of Informatics, Sokoine University of Agriculture, Tanzania

ABSTRACT

Wireless Sensor Networks (WSN) consists of large number of low-cost, resource-constrained sensor nodes. The constraints of the WSN which make it to be vulnerable to attacks are based on their characteristics which include: low memory, low computation power, they are deployed in hostile area and left unattended, small range of communication capability and low energy capabilities. Examples of attacks which can occur in a WSN are sinkhole attack, selective forwarding attack and wormhole attack. One of the impacts of these attacks is that, one attack can be used to launch other attacks. This book chapter presents an exploration of the analysis of the existing solutions which are used to detect and identify passive and active attack in WSN. The analysis is based on advantages and limitations of the proposed solutions.

1. INTRODUCTION

Wireless Sensor Networks (WSN) consists of small nodes with ability to sense and send data to base station (Rong, Eggen, & Cheng, 2011). WSN is used in different applications, for example in military activities, where there is a need of tracking movement of enemies. Also, it is used in fire detection and healthy service for monitoring heart beat (Chen, Song & Hsieh, 2010; Sharma & Ghose, 2010; Teng & Zhang, 2010). Unfortunately, most of WSN are deployed in unfriendly area and normally left unattended. Furthermore, many routing protocols used in WSN do not consider security aspect due to resource constraints which include: low computational power, low memory, low power supply and low communication range (Martins & Guyennet, 2010; Ngai, Liu, & Lyu, 2006). These constraints create chance for several attackers to easily attack WSN. There are two types of attacks, namely: passive and active attacks. In passive attack, a malicious node only eavesdrops upon the packet contents, while in

DOI: 10.4018/978-1-4666-8761-5.ch005

active attack; it may imitate, drop or modify legitimate packets (Sanzgiri, Dahill, Levine, Shields, & Belding-Royer, 2002). Examples of active attacks are sinkhole and selective forwarding attack. Example of passive attack is wormhole attack. In selective forwarding attack such attack adversary node creates their own path so attacker can drop the data packet and perform spy on those dropped data packet (Patel & Manoranjitham, 2013). This type of attack is difficult to detect (Tripathi, Gaur, Laxmi, & Jatav, 2012). Sinkhole attack is an active attack implemented in network layer where an adversary tries to attract many traffic with the aim of preventing base station from receiving a complete sensing data from nodes (Samundiswary, Sathian, & Dananjayan, 2010). Wormhole attack occurs when two or more adversary node create a higher level virtual tunnel between those two adversary nodes and advertise high link quality so that all other neighbors node transfer data packet through the virtual tunnel (Verma & Singh, 2011).

The purpose of this book chapter is to review existing solutions used to detect passive and active attack which include selective forwarding, wormhole, blackhole and sinkhole. Different solutions which are being used to detect and prevent attacks are suggested (Krontiris, Dimitriou, Giannetsos, & Mpasoukos, 2008; Tumrongwittayapak & Varakulsiripunth, 2009; Ngai, Liu & Lyu, 2007; BabuKaruppiah, Vidhya, & Rajaram, 2013; Sheela, Kumar, & Mahadevan, 2011; Kibirige & Sanga, 2015). Rule based detection solution as proposed by Krontiris, Giannetsos and Dimitriou (2008) to detect sinkhole attack. All the rules focus on node impersonation and are implanted in intrusion detection system. The intruder is easily detected when violate either of the rules. BabuKaruppiah, Vidhy and Rajaram (2013) proposed an energy efficient wormhole detection technique by traffic analysis in WSN. The technique use statistical method and involve base station in the detection process. Another centralized solution which involves base station in detection process is called a non cryptography scheme which use mobile agent in the network to prevent sinkhole attack (Sheela, Kumar, & Mahadevan, 2011).

This book chapter is organized into five sections. Section 2 presents the discussion of sinkhole, wormhole, blackhole and selective forwarding attacks and their mechanism. Section 3 presents the challenges in detecting attacks in WSN. Section 4 presents different approaches to detect wormhole, sinkhole, blackhole and selective forwarding attacks. Finally, section 5 concludes by proposing future work.

2. REVIEW OF WSN ATTACKS

2.1. Sinkhole Attack

Sinkhole attack is an insider attack where an intruder compromises a node inside the network and launches an attack (Ngai, Liu, & Lyu, 2007; Kibirige & Sanga, 2015). The compromised node try to attract all the traffic from neighbor nodes based on the routing metric in routing protocol. Due to communication pattern of WSN, there are many to one communication where each node sends data to base station. This makes WSN vulnerable to sinkhole attack (Ngai & Liu, 2007).

The following subsections present the techniques used in MintRoute protocol in launching sinkhole attack (Figure 1).

Sinkhole Attack in MintRoute Protocol

MintRoute protocol is a type of protocol which is commonly used in WSN. It was designed purposely for the WSN. It is suitable for sensor nodes which have minimum storage capacity, low computation power