Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 700 – 707

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol

Parmar Amish[a] ,V.B.Vaghela[b]

[a]*Student, Sankalchand Patel College of Engineering, Visnagar-384315, India*
[b]*Principal, Jashodaba Polytechnic Institute, Sidhpur-384151, India*

Abstract

Unique characteristics like limited bandwidth, limited battery power and dynamic topology makes Wireless sensor network (WSN) vulnerable to many kinds of attacks. Therefore interest in research of security in WSN has been increasing since last several years. Infrastructure less and self-governing nature of WSN is challenging issue in terms of security. Wormhole attack is one of the severe attack in wireless sensor network. In this paper, the techniques dealing with wormhole attack in WSN are surveyed and a method is proposed for detection and prevention of wormhole attack. AOMDV (Ad hoc On demand Multipath Distance Vector) routing protocol is incorporated into these method which is based on RTT (Round Trip Time) mechanism and other characteristics of wormhole attack. As compared to other solution shown in literature, proposed approach looks very promising. NS2 simulator is used to perform all simulation.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: WSN; Wormhole attack; RTT; AOMDV; malicious node.

1. Introduction

Sensor nodes are used to perform communication in wireless sensor network. Nodes in network here communicate directly with each other using wireless transceivers with no fixed infrastructure. Sensor nodes are deployed in large number to monitor the environment or system by measurement of physical parameters such as pressure, characteristic of object temperature and their relative humidity or motion. Each node of the sensor network consist of the three subsystems: the processing subsystem which performs local computations on the sensed data, the sensor subsystem which senses the environment and the communication subsystem which is responsible for message

* Corresponding author.
E-mail address: amish.heartly@gmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.092

interchange with neighbouring sensor nodes. Cost and size on sensor nodes result in corresponding constraints on resources such as memory, energy, computational speed and communications bandwidth. The application scenarios for WSNs are many including military surveillance, commercial, medical, manufacturing and home automation to name many but few [1]. Due to the broadcast nature of the transmission medium and fact that sensor nodes often operate in hostile environments WSNs are vulnerable to variety of security attacks.

According to the layers of the OSI model classification of security attacks in WSNs is done. The attacks which operate at the network layer are referred to as routing attacks.

There are many types of attacks possible in network layer like selective forwarding, spoofed or replayed routing information, Sybil attack, sinkhole attack, Hello flood attack and Wormhole attack.

Section II describes about wormhole attack in detail. Section III describes related work proposed by various authors. Section IV deliberates our proposed work for detection and prevention of wormhole attack. Section V we present our results. In section VI we conclude.

2. Wormhole Attack

This attack has one or more malicious node and a tunnel between them. The attacking nodes captures the packets from one location and transmits them to other distant located node which distributes them locally. The tunnel can be established in many ways e.g. in-band and out-of-band channel. This makes the tunnelled packet arrive either sooner or with a lesser number of the hopes compared to the packets transmitted over normal multi hop routes. Routing mechanisms which rely on the knowledge about distance between nodes can get confuse because wormhole nodes fake a route that is shorter than the original one within the network [2]. They can then launch a variety of attacks against the data traffic flow such as selective dropping, eavesdropping, replay attack, etc. Wormhole can be formed using, first, in-band channel packet to another malicious node m2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following m2 nodes believe that there is no node between m1 and m2 employ an physical channel between them by either dedicated wired link or long range wireless link shown in *Fig. 1.*

When malicious nodes form a wormhole they can disclose themselves or hide themselves in a routing path. The former is an exposed or open wormhole attack, while the latter is a hidden or close one.

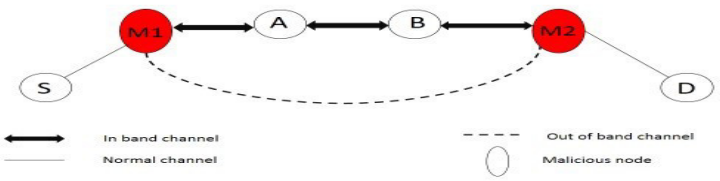

Fig 1 Wormhole Attack

In Fig 1, the destination D notice that the packet from the source S is transferred through the node A and B under hidden wormhole attack, while it believes that the packet is delivered via node A, m1, m2 and B under exposed wormhole attack.

3. Related Work