Chapter 6
SRIP:
A Secure Hybrid Routing Information Protocol for WSN

Rajshree
Babasaheb Bhimrao Ambedkar University, India

Ravi Prakash Pandey
Dr. Ram Manohal Lohiya Awadh University, India

Sanjeev Sharma
Rajiv Gandhi Prodyogiki Vishwavidyalaya, India

Vivek Shukla
Rajiv Gandhi Prodyogiki Vishwavidyalaya, India

ABSTRACT

Security in Mobile Ad hoc Network (MANET)/ Wireless Sensor Network (WSN) is very important issue. Due to dynamic topology and mobility of nodes, Mobile Ad hoc Networks/ WSNs are more vulnerable to security attacks than conventional wired and wireless network. Nodes of Mobile Ad hoc Network communicate directly without any central base station. That means in ad hoc network, infrastructure is not required for establishing communication. In this chapter we are describing Route Falsification Attack which is easy to launch in MANETs or wireless ad hoc network. Route Falsification attack is referred to as a node with no special hardware capability can use packet encapsulation and tunneling to create bogus short-cuts in routing paths and influence data traffic to flow through them. This chapter shows the implementation of a Secure Hybrid Routing Information Protocol (SRIP) which can be used to prevent route falsification attack in MANETs. We evaluated performance of SRIP in Qualnet Simulator with and without route falsification attack. Our analysis indicates that SRIP is very suitable to stop this attack and performs well with low overhead in normal networks.

DOI: 10.4018/978-1-61520-741-1.ch006

INTRODUCTION

Ad-hoc network is a collection of several wireless nodes that are capable of communicating directly with each other without having any infrastructure or any centralized administration. Multi hop communication can be created by making nodes as routers. That means all nodes which involve in ad hoc network can be act as router. The wireless node can give wide range of application because of node mobility and frequent topology changes. Especially in military operations and emergency & disaster relief efforts. Because of open wireless medium used, dynamic topology and distributed & cooperating sharing of channels, ad-hoc networks are more venerable to security attacks than conventional wired and wireless networks. B. Dahill, B. N. Levine, E. Royer & C. Shields. Aran (2002) stated that TCP/IP is unsuitable for sensor networks.

In this paper we are describing rout falsification attacks for MANETs. Sometimes this route falsification attack works as black hole attack. In a Route Falsification Attack, malicious node can work in both direction, source to destination during route request and destination to source during Route reply. When source sends request to destination node or when destination/ other node give reply for request. In this attack, malicious node falsify the route request and / or route reply packets to indicates a better/ shortest path to the source of a data connection for making large portion of the traffic go through them. Rajendra V. & Boppana Xu Su (2007) state that when the source selects the falsified path, the malicious nodes can drop data packets they receive silently (denoted Black hole attack), on forward the packets but keep the information to conduct the analysis of communication patterns such as sender-recipient matching, traffic timing volume and shape. After introduction the chapter includes the working of route falsification attack, description of the SRIP protocol, results that shows by SRIP route falsification attack can be totally removed and conclusion of the paper.

BACKGROUND

There are lots of researches have been going on and conducted on the topic of security. Wireless Sensor network is the very accepted area. Wireless sensor networks are often deployed in a hostile environment and work without human supervision, individual node could be easily compromised by the malicious node due to the constraints such as battery lifetime, smaller memory space and limited computing capability. Security in WSN has been one of the most important topics in the WSN research community. Here we only briefly review the reported works closely related to malicious node detection due to the limited space. To identify denial of service vulnerabilities, A.D. Wood and J. A. Stankovic (2002) analyzed two effective sensor network protocols that did not initially consider security. In their examples, they demonstrated that consideration of security at design time is the best way to ensure successful network deployment. Most recent ad hoc network research has focused on providing routing services without considering security. In their paper, B. Dahill, B. N. Levine, E. Royer & C. Shields. Aran (2002) detailed security threats against ad hoc routing protocols, specifically examining AODV and DSR. They proposed protocol, ARAN, that was based on certificates and successfully defeats all identified attacks. C.Karlof & D. Vagner (2003) proposed security goals for routing in sensor networks, showed how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduced two classes of novel attacks against sensor networkssinkholes and HELLO floods, and analyzed the security of all the major sensor network routing protocols. H. Yang, H. Luo, F. Ye, S. Lu & L. Zhang (2004) focused on the fundamental security problem of protecting the multihop network connectivity between mobile nodes in a MANET. They identify the security issues related to this problem, discuss the challenges to security design, and review the state-of-the-art security proposals.