Chapter 8
Security in Pervasive Computing:
A Blackhole Attack Perspective

Sunita Prasad
Centre for Development of Advanced Computing, India

Rakesh Chouhan
Centre for Development of Advanced Computing, India

ABSTRACT

Pervasive computing has wide application in military, medical and smart home domain. In pervasive computing, a large number of smart objects interact with one another without the user intervention. Although the technology is promising but security needs to be addressed before the technology is widely deployed. Pervasive networks are formed spontaneously and the devices communicate via radio. Thus, mobile ad hoc networking is an essential technology for pervasive computing. An ad hoc network is a collection of wireless mobile nodes, which acts as a host as well as a router. The communication between the nodes is multihop without any centralized administration. AODV (Ad Hoc On demand Distance Vector) is a prominent on-demand reactive routing protocol for mobile ad hoc networks. But in existing AODV, there is no security provision against well-known attack known as "Black hole attack". Black hole nodes are those malicious nodes that agree to forward the packets to destination but do not forward the packets intentionally. Thischapter extends the watchdog mechanism for the AODV routing protocol to detect such misbehavior based on promiscuous listening. The proposed method first detects a black hole node and then gives a new route bypassing this node. The experimental results show that in a lightly loaded, hostile environment, the proposed scheme improves the throughput compared to an unprotected AODV protocol.

INTRODUCTION

In 1991, Mark Weiser, father of ubiquitous computing, described the vision for 21st century computing. He stated that "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" [Weiser 1991] He named it ubiquitous computing aka pervasive computing. Pervasive computing is a rapidly developing area

DOI: 10.4018/978-1-61520-741-1.ch008

of Information and Communication Technology (ICT). The term refers to the increasing integration of ICT into people's lives and environment. This is made possible by the growing availability of wireless embedded systems with inbuilt communication facilities. Pervasive computing has many potential applications from health care and home care to environmental monitoring and intelligent transport systems. Consider a heart patient wearing an implanted monitor that communicates wirelessly with computers trained to detect and report deviations from the normal behavior. The monitor should know when to raise the alarm, based on its knowledge about the environment. Pervasive computing is not just wireless communication but a complex system. The goal is to meet the claim of computing anytime anywhere. Millions of embedded microprocessors allow the technology to recede into the background. A pervasive computing technology involves three converging areas of ICT namely computing devices, connectivity and user interfaces. The technology involves embedded devices, which may be stationary as well as mobile. These components are linked to each other and communicate via radio. The pervasive system forms the network spontaneously. Mobile networking is the key technology to pervasive computing.

Pervasive computing systems (PCS) are complex as there are billions of processors having complex interaction. Integrating the pervasive computing components raises severe security issues. The complex system is a paradise for hackers and virus in absence of any security measures. The system may propagate false information, selective information or completely block the information of individuals or organizations. Pervasive computing cannot become a reality until these issues are addressed. Security involves preventing unauthorized persons from viewing and/or manipulating the data and also protection from both internal and external attacks. Thus secure communication is of vital importance in these networks. This paper discusses a specialized attack known as the blackhole attack in ad hoc networks, which is the underlying technology for connectivity in PCS. A mobile ad hoc network (MANET) is an autonomous system of mobile hosts connected by wireless links. There is no static infrastructure such as base station. The hosts are free to move around randomly, thus changing the network topology dynamically. Thus routing protocols must be adaptive and able to maintain routes in spite of the changing network connectivity. Such networks are very useful in military and tactical applications such as emergency rescue or exploration missions, where cellular infrastructure is unavailable or unreliable. Commercial applications include home area networking, on-the-fly conferencing applications, networking intelligent devices or sensors, communication between mobile robots, etc. Ad hoc networks are ideal in situations where installing an infrastructure is not possible because the infrastructure is too expensive or too vulnerable.

The communication in a MANET is essentially multihop due to limited transmission range. This decentralized operation relies on the cooperative participation of all nodes. Thus security becomes an essential component even for the basic network operation like packet forwarding and routing (Deng, 2002). The malicious node could simply block or modify the traffic traversing through it by refusing to cooperate. Security in wireless ad hoc network is a challenging task. In general, the MANET is vulnerable due to its fundamental characteristic of open medium, dynamic topology, and absence of central authorities, distributed cooperation, and constrained capability.

Security Requirements

Routing in ad hoc network is trivial and based on implicit "Trust your neighbor" relationship. If all the nodes are within the transmission range, then the destination can be reached by a single hop. However, when the destination is not within a single hop then multi-hop routing is required.