Chapter 56
Secure Route Discovery in DSR against Black Hole Attacks in Mobile Ad Hoc Networks

P. Subathra
Thiagarajar College of Engineering, India

S. Sivagurunathan
Gandhigram Rural Institute – Deemed University, India

ABSTRACT

A Mobile Ad hoc Network (MANET) is a collection of wireless nodes communicating over multi-hop paths without any infrastructure. Nodes must cooperate to provide necessary network functionalities. The security in routing protocols like Dynamic Source Routing (DSR) can be compromised by a "Black Hole" attack. Here, a malicious node claims to have the shortest path to the destination and attracts all traffic and drops them, leading to performance degradation. The situation becomes worse when two or more nodes cooperate and perform the "Cooperative black hole" attack. This chapter proposes a solution based on probing to identify and prevent such attacks. The proposed solution discovers a secure route between the source and destination by identifying and isolating the attacking nodes. Simulation results show that the protocol provides better security and performance in terms of detection time, packet delivery ratio, and false negative probability in comparison with trust and probe based schemes.

INTRODUCTION

Wireless networks can be implemented either as an infrastructure based networks or an infrastructure less networks. The infrastructure based networks use fixed base stations, which are responsible for coordinating communication between the mobile hosts (nodes). The Mobile Ad hoc Network (MANET) falls under the class of infrastructure less networks (Sergio Marti et al., 2000).

Ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of ad hoc network is dependent on the trust and cooperation amongst the nodes. Nodes help each other in conveying information about the topology of the

DOI: 10.4018/978-1-4666-4707-7.ch056

network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes (Deng et al., 2002; Milanovic et al., 2004). All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves collectively.

The MANETs are categorized into two types: closed MANET and open MANET (Miranda & Rodrigues, 2002). In a closed MANET, all mobile nodes cooperate with each other towards a common goal, such as emergency search/rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be the most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish/misbehaving nodes and their behavior is termed as selfishness/misbehavior (Miranda & Rodrigues, 2002). One of the major sources of energy consumption in the mobile nodes of MANETs is wireless transmission (Rerney & Nilsson, 2001). A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

The misbehavior of a node can be due to any one of the following reasons: A node may try to conserve its energy by not forwarding data packets for other nodes from the network; node may be overloaded, broken, compromised or congested in addition to intentionally being selfish/malicious (Yang et al., 2006 & Hubaux et al., 2001). Misbehavior can be divided into two categories (Yang et al., 2006): routing misbehavior (failure to behave in accordance with a routing protocol) and packet forwarding misbehavior (failure to forward the packets). This work proposes an algorithm that enables packet forwarding misbehavior detection.

A single black hole attack (Papadimitratos & Haas, 2002) is a specific type of attack, where a malicious node injects false route replies to the route requests it receives by advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious nodes for eavesdropping, or simply to attack all traffic to it in order to perform a Denial of Service (DoS) attack by dropping the received packets. In a cooperative black hole attack two or more nodes cooperate amongst themselves and when a packet is forwarded to any of these nodes they collude with each other and drop it. Since the nodes cooperate with each other they do not reveal the identity of the node that actually drops the packet to the external world and thus the trust information given by these would be a fake one. This makes the identification of such attacks more difficult.

This article provides a novel approach to detect both the single and cooperating black hole nodes and to remove them from further routing path to improve the network's performance. The rest of the article presents the state of the art, the model and the assumptions related to this work along with the proposed algorithm. The evaluation of the algorithm is also presented.

RELATED WORK

The literature review carried out in this area revealed that the problem of packet dropping attack is basically handled by five different types of techniques as shown in Figure 1.

Authentication Based Techniques

Authenticating the nodes of a network may be the first and foremost preventive measure against attacks on MANETs. Cryptographic based authentication schemes have been extensively used in the field of MANETs to provide security. Some of it