Chapter 11

Intrusion Detection Algorithm for MANET

S. Srinivasan
Texas A&M International University, USA

S. P. Alampalayam
APS Technologies, USA

ABSTRACT

Mobile ad hoc networks (MANET) present the opportunity to connect transient nodes to the internet without having central control. This very design supports new nodes to join and leave the network based on their proximity to the MANET. Concurrently, it creates many security challenges for authenticating nodes that are not present in a traditional wired network. Much of the existing work on MANET security has focused on routing and mobility. In this paper, the authors present an algorithm that considers the neighboring nodes’ status to determine if a particular node is malicious or not. The authors used NS2 simulation tool to test the algorithm and present the results in the paper. The major benefits of this research work are in military applications.

INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of mobile nodes forming an adhoc network without central control of the network. The main benefit of MANET is that the nodes could enter or leave the network based on their proximity to the MANET. Such a network does not require any fixed infrastructure to support the mobile nodes. The major beneficiaries of the use of MANET are the first responders responding to a disaster or soldiers in a battlefield. MANET is one of the well researched areas in the literature. Even though MANETs have been looked at from various angles, much of the work involving MANET have been with regard to routing, performance, and mobility (Hubaux, Buttyan, & Capkun, 2001). These are important aspects to look at but, given the inherent nature of MANET to support many new nodes, authentication is an important aspect. Focusing
on security and dependability of the MANET is essential in order to support future applications involving these networks.

Traditional networks have been successful based on their reliability and the security guarantees. In such networks the nodes that enter the network have fixed access points such as a port in a router and stay on the network for an extended period of time. On the other hand, in a mobile ad hoc network there is no central server to authenticate nodes. By design, a MANET supports nodes that enter the network based on their proximity to the MANET and also leave the network after a brief period of time. So, one has to make sure that any node that enters the network has good intentions. This means that the node will have access to the network to reach an access point for the Internet and at the same time should facilitate other nodes that require the necessary forwarding of packets. Studies have shown that when a node is on a MANET, it tries to conserve power and the activity that drains much of the power is routing packets. It is estimated that a node on a MANET would use up 65 percent of its power in facilitating packet forwarding. For this reason, nodes tend to become greedy after a while to conserve power. Thus, algorithms are needed to detect when a node is no longer an active participant in the network. Given the mobile nature of a nodes’ participation in MANET this is not a major hurdle to overcome.

The most common method of securing a communication is by using encryption. It works well in wired networks which could support extensive decryption methodologies since electrical power is not a factor to be worried about. However, nodes in a MANET are power constrained and as such cannot support extensive decryption technologies (Zhang, Lee, & Huang, 2003). The alternative then is to monitor every node in a MANET. This would not be a major burden since the number of nodes in MANET at any given time is limited to less than 50 nodes. Another important factor to consider in an ad hoc network is trust between nodes. Since the nodes enter and leave an ad hoc network periodically there should be some way to build trust. This is one of the reasons why intrusion detection is essential in a MANET.

In the research literature we find a vast amount of material on various approaches to intrusion detection (ID). Zhang et al studied ID in wireless networks in general (Zhang, Lee, & Huang, 2003). Vigna et al. (2004) looked at ID in AODV-based ad hoc networks. AODV (Ad hoc On demand Distance Vector) networks find the shortest path from source to destination among a set of nodes that are neighbors. Bhargava and Agarwal (2001) as well as Klein-Berndt (2001) considered the security aspects of AODV protocols. Puttini et al.’s (2004) study involved a fully integrated approach to detecting intruders in a MANET. In another paper, Puttini et al. (2003) studied a modular architecture for distributed intrusion detection systems. This is an important contribution in that this identifies several new methods of distributed attacks. Alampalayam et al. (2005) viewed intrusion from a security perspective and developed a taxonomy. Sen and Clark (2009) did a similar study on intrusion detection in MANETs. Sterne et al. (2005) took a novel approach and studied a cooperative intrusion detection architecture. Li and Wei (2004) developed guidelines for selecting the appropriate method for intrusion detection. Mandala et al. (2007) did an extensive survey of intrusion detection methods. The results highlighted in this survey were also part of the other works cited in this paper.

Another important contribution in intrusion detection in wireless networks was presented by Nadkarni and Misra (2004). They took a novel approach to detect intrusion in wireless ad hoc networks (Nadkarni & Misra, 2004). The approach Patwardhan et al. (2005) took for considering intrusion detection was widely looked at by several others as well. They looked at ID from a secure routing perspective (Patwardhan et al., 2005). Traditionally the intrusion detection mechanisms are applied both to the AODV and