Chapter 18

Trust Determination in Wireless Ad Hoc Networks

Hussein Al-Bahadili
University of Petra, Jordan

ABSTRACT

Wireless ad hoc networks are susceptible to attacks by malicious nodes that could easily bring down the whole network. Therefore, it is important to have a reliable mechanism for detecting and isolating malicious nodes before they can do any harm to the network. Trust-based routing protocols are one possible mechanism as they locate trusted routes dynamically to conform to network environment. However, such algorithms require reliable and effective trust determination algorithm. This chapter presents a detail description and evaluation of the trust determination algorithm, namely, the Neighbor-Weight Trust Determination (NWTD) algorithm. The performance of the algorithm is evaluated through simulation using the Mobile Ad hoc Network (MANET) simulator (MANSim). The simulation results demonstrated the effectiveness and reliability of the algorithm in isolating any maliciously behaving node(s) in a timely manner.

INTRODUCTION

Wireless ad hoc network is defined as a set of wireless mobile nodes communicate with one another for a purpose of data (message) exchange without relying on any pre-existing infrastructure or centralized control (Murthy & Manoj, 2004). Early ad hoc research papers assumed a friendly and cooperative environment and focused on problems such as wireless channel access, multi-hop routing, power consumption, while ignoring any network security issues. Network security involves securing computer network infrastructure from being attached by adversary or malicious nodes and has become a primary concern in order to provide protected communication between nodes in a potentially hostile ad hoc environment (Djenouri et al., 2005; Yang et al., 2004).

Wireless ad hoc networks are very vulnerable to and heavily suffer from maliciously behaving nodes or malicious nodes, which could easily degrade the network stability by exhibiting one or more of the following behavior: packet drop, battery drained, buffer overflow, bandwidth consumption, illegal node entering, stale packets, packet delaying, link break, message tampering,
message modification, denying from sending message, route modification, node isolation, stealing information, session capturing, etc. Therefore, it is important to have a reliable mechanism for detecting and isolating malicious nodes before they can do any harm to the network. One of these mechanisms is the trust-based routing protocols (Gonzalez et al., 2011; Ferdous et al., 2010; Hughes et al., 2003). In which only trusted nodes are accepted for forwarding control/data packets, so that each node to be part of the routing table, it should have a trust above a certain minimum acceptable trust (MAT). The main requirement and challenge to these protocols is the availability of an appropriate trust determination algorithm.

One of the earliest approaches for trust determination is Marsh’s formalism (Marsh, 1994). Marsh uses the outcomes of direct interactions among nodes to calculate situational and general trust. Situational trust is the level of trust in another for a specific type of situation, while general trust refers to overall trustworthiness irrespective of the situation. After each interaction, a node considers whether the other node fulfilled its obligations. If so, then trust increases, but trust decreases if commitments are broken. This formalism is the base of many subsequent models, which supplement trust based on direct interactions with other information sources to update decision-making. Throughout the years, a number of trust determination algorithms have been developed; however, still more powerful algorithms are required to meet network security needs (England et al., 2012; Cordasco et al., 2008; Liu et al., 2004).

This chapter describes and evaluates the performance of the new trust determination algorithm, namely, the Neighbor-Weight Trust Determination (NWTD) algorithm (El-Zayyat et al., 201), which is based on the weighted voting concept (COMAP, 2011). In this algorithm, each node in the network is timed to periodically broadcast message stoat’s one-hop neighbors containing the IDs of its one-hop trusted nodes and their trusts. Each node will receive a number of messages, most probably, equal to the number of its one-hop neighbors. After receiving these messages, each receiving node extracts the IDs and trusts of each node on the message; and consequently, a node may receive different trusts for the same one-hop neighbor from other nodes. Afterwards, the receiving node calculates the new trust for each of its one-hop neighbors by averaging the node trusts’ that is received from other one-hop neighbors using the weighted-average formula. The weight here is the weight of the node one-hop neighbors, therefore it is referred to as the NWTD algorithm. The node itself participates in the averaging process by giving itself a trust one and 100% weight.

The algorithm defines two types of nodes: the master and monitoring nodes. A master node is any trusted node in the network that can take the responsibility of testing new arriving nodes, determines their initial trust, and then broadcasts the initial trust to its one-hop neighbors. Each node in the network must define a master node for itself by applying a certain criteria on its one-hop neighbors and on itself; therefore, the network may have one or more master nodes. If a node could not find a master node for itself, it can be a master node for itself. A monitoring node is any node in the network that has the capacity to detect the malicious behavior of other nodes within its neighborhood, reduces the trust of the detected malicious nodes, and then uses the updated trust in the forthcoming trust determination process. The algorithm allows for one or more monitoring nodes to be active at the same time.

The NWTD algorithm is implemented and integrated with the mobile ad hoc network simulator (MANSim) (Al-Bahadili, 2010), which is used to evaluate the performance of the algorithm. In particular, in this work, MANSim is used to simulate three main scenarios. The first one simulates a network environment with no malicious nodes; the second scenario simulates a network with one monitoring and one malicious node; and the third scenario simulates a network with one monitoring and two malicious nodes.