ISSN 1746-7659, England, UK
Journal of Information and Computing Science
Vol. 7, No. 4, 2012, *pp*. 296-302

Trust Based Selective Forwarding Attacks using Channel Aware Approach in Wireless Mesh Networks

Anand Nayyar

[1] Department of Computer Applications & IT

KCL Institute of Management and Technology, Jalandhar, Punjab, India

(*Received July10, 2012, accepted September 28, 2012*)

Abstract. This Research Paper introduces a channel aware detection (CAD) algorithm that can effectively identify the selective forwarding misbehavior from the normal channel losses. It is a special case of denial of service (DoS) attack in wireless mesh networks (WMNs) known as selective forwarding attack .The CAD algorithm is based on two strategies. With such an attack, a misbehaving mesh router just forwards a subset of packets it receives but drops the others. Channel estimation is the procedure to estimate the normal loss rate due to bad channel quality or medium access collision. Traffic monitoring is to monitor the actual loss rate, if the monitored loss rate at certain hops exceeds the estimated loss rate, those nodes involved will be identified as attackers. To determine the optimal detection thresholds that minimizes the summation of false alarm and missed detection probabilities. In this work the system is free from collision or jamming attacks, when an attacker introduces noise to simulate a noisy channel, it indeed affects the sensing process which in turn leads to inaccurate threshold. This project uses CAD approach to demonstrate the efficiency of discriminating selective forwarding attacks from normal channel losses through extensive computer simulations.

Keywords: Wireless Mesh Network, Selective forwarding attack, Gray Hole Attack, Channel Aware Detection, Optimal Detection threshold.

1. Introduction

Wireless Mesh Network (WMN) is a communications made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet. The coverage area of the radio nodes working as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to create a radio network. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediatenodes. Wireless mesh networks can be implemented with various wireless technology including 802.11, 802.16, cellular technologies or combinations of more than one type. A wireless mesh network can be seen as a special type of wireless ad-hoc network. It is often assumed that all nodes in a wireless mesh network are immobile but this need not be so. The mesh routers may be highly mobile. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the wireless mesh network differs from an ad-hoc network since all of these nodes are often constrained by resources.

1.1 Architecture of Wireless Mesh Network

Wireless mesh architecture is a first step towards providing high-bandwidth network over a specific coverage area. Wireless mesh architectures infrastructure is, in effect, a router network minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops. Intermediate nodes not only boost the signal, but cooperatively make forwarding

decisions based on their knowledge of the network, i.e. perform routing. Such architecture may with careful design provide high bandwidth, spectral efficiency, and economic advantage over the coverage area.

Example of three types of wireless mesh network:

- Infrastructure wireless mesh networks: Mesh routers form an infrastructure for clients.
- Client wireless mesh networks: Client nodes constitute the actual network to perform routing and configuration functionalities.
- Hybrid wireless mesh networks: Mesh clients can perform mesh functions with other mesh clients as well as accessing the network.

Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic in an infrastructure mesh network is either forwarded to or from a gateway, while in ad hoc networks or client mesh networks the traffic flows between arbitrary pairs of nodes.

1.2 Management

This type of infrastructure can be decentralized (with no central server) or centrally managed (with a central server) both are relatively inexpensive, and very reliable and resilient, as each node needs only transmit as far as the next node. Nodes act as routers to transmit data from nearby nodes to peers that are too far away to reach in a single hop, resulting in a network that can span larger distances. The topology of a mesh network is also more reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbors can find another route using a routing protocol.

1.3 Applications

Mesh networks may involve either fixed or mobile devices. The solutions are as diverse as communication needs, for example in difficult environments such as emergency situations, tunnels and oil rigs to battlefield surveillance and high speed mobile video applications on board public transport or real time racing car telemetry. A significant application for wireless mesh networks is VoIP. By using a Quality of Service scheme, the wireless mesh may support local telephone calls to be routed through the mesh. For example, miner safety has improved with VOIP phones communicating over a mesh network.

1.4 Multi-Radio Mesh

Multi-radio mesh refers to a unique pair of dedicated radios on each end of the link. This means there is a unique frequency used for each wireless hop and thus a dedicated CSMA collision domain. This is a true mesh link where achieve maximum performance without bandwidth degradation in the mesh and without adding latency. Thus voice and video applications work just as they would on a wired Ethernet network. In true 802.11 networks, there is no concept of a mesh. There are only Access Points (AP's) and Stations. So a Multi-radio wireless mesh node will dedicate one of the radios to act as a station, and connect to a neighbor node AP radio. Single and dual-radio mesh use proprietary means to repeat the signal which means that more than two nodes are in the same collision domain and frequency.

2. Related Work

Y. L. Sun et al [13] have proposed the performance of distributed networks depends on collaboration among distributed entities. To enhance security in distributed networks, such as ad hoc networks, it is important to evaluate the trustworthiness of participating entities since trust is the major driving force for collaboration. We present a framework to quantitatively measure trust model trust propagation, and defend trust evaluation systems against malicious attacks. In particular, we address the fundamental understanding of trust, quantitative trust metrics, mathematical properties of trust, dynamic properties of trust, and trust models. The attacks against trust evaluation are identified and defense techniques are developed. The proposed trust evaluation system is employed in ad hoc networks for securing ad hoc routing and assisting malicious node detection

There are three primary aspects associated with evaluating trust in distributed networks.