LIGHTWEIGHT SECURITY MECHANISM TO MITIGATE NETWORK LAYER BASED ACTIVE ATTACKS IN A MOBILE ADHOC NETWORK

By

UTHUMANSA AHAMED

A thesis submitted to the **Faculty of Applied Sciences, Rajarata University of Sri Lanka** in partial fulfillment of the requirements for the award of the degree of

MASTER OF PHILOSOPHY in **Computer Sciences**

Faculty of Applied Sciences
Rajarata University of Sri Lanka
Mihintale – Sri Lanka

May 2021

ABSTRACT

Mobile Ad hoc Network (MANET) is one type of an Ad hoc network. General properties of a MANET are self-configuration capability, open network boundary, infrastructure-less network nature, and limited resources. This nature of MANET opens the network to different security threats. Network layer-based Active attacks are widespread. Available security solutions for Active attacks contain complex calculations. Therefore, the objective of this research is to propose a lightweight security mechanism to enhance and strengthen the security of the data communications between source and destination nodes in a MANET. This research consists of three different experiments. Experiment I was designed to investigate the behaviours and impacts of malicious nodes on network performance. Experiment II was designed to identify the impacts and validity based on node mobility when designing security countermeasures in MANET. Experiment III was designed to propose a widely deployed lightweight security mechanism based on the results of experiments I and II. Ad-hoc On-Demand Vector is used as the routing protocol to detect network layer attacks. Blackhole and Grayhole attacks are used as network layer-based Active attacks. Packet Delivery Ratio (PDR), Average End to End Delay (AEED), Throughput, Average Data Dropping Rate (ADDR), and Simulation Processing Time at Intermediate Nodes (SPTIN) are measured by changing the number of connected nodes in the network and by changing the speed of the nodes. A network without attack is used to compare the performances of each network. In experiment I, due to the impact of the blackhole attack, compared to the network without attack, the PDR was found to be 0.28%, AEED was infinity and Throughput was 0.33%. In experiment II, PDR and Throughput values are increased by twice in higher node mobility than in lower node mobility. The network that is affected by a grayhole attack shows higher performance than the network that was affected by a blackhole attack and lower performance than the network without attack. In experiment III, the performances of the proposed security mechanism were compared with the network without attack, and the values of PDR, AEED, Throughput, and SPTIN were found to be 98.0825%, 100.9346%, 99.9988%, and 96.5660% respectively. The data packet delivery ratio was 100.00% compared to the network without attack. The network which was affected by a blackhole attack showed a higher amount of ADDR than the network without the attack and the lowest amount of PDR. The network that was affected by a blackhole or a grayhole attack showed underperformance than the network without the attack. It was also found that the blackhole attack degraded the network performance more than the grayhole attack. The mobility of nodes degraded the network performance. Node mobility either led to the breaking of the links between nodes or the creation of new links. Therefore, node mobility created an opportunity to break the link between malicious and other nodes in the network. Active attacks degraded the MANET performance. The main similarity of most Active attacks was the abnormal amount of packet dropping. Therefore, node mobility is a favourable factor for network security. Furthermore, this implied that the security mechanism should be flexible enough to handle security attacks amidst node mobility. Therefore, initial screening to detect malicious nodes was found to be effective in the presence of mobile nodes. The proposed security mechanism performs well in the presence of a blackhole attack. Moreover, it performs well in PDR, AEED, and Throughput compared to the network without attack. The performance of the AEED and SPTIN proves that the proposed solution is free from complex calculations. The scope of the proposed security mechanism can be expanded into a lightweight Intruder Detection System to handle different types of security attacks.

CONTENTS