Improved Reliable Data Forwarding Using Homomorphic Encryption Against Blackhole Attack in Mobile Ad hoc Networks

By

Mazharul Islam
Roll: 1807102

A thesis submitted in partial fulfilment of the requirements for the degree of
"Bachelor of Science in Computer Science and Engineering"

Supervisor:

Professor Dr Kazi Md. Rokibul Alam
Professor
Department of Computer Science and Engineering
Khulna University of Engineering & Technology, Khulna

_____
Signature

Department of Computer Science and Engineering
Khulna University of Engineering & Technology
Khulna 9203, Bangladesh
August, 2023

Acknowledgement

All the praise to the almighty Allah, whose blessing and mercy succeeded me to complete this work fairly. I gratefully acknowledge to our highly esteemed teacher and My supervisor, Professor Dr Kazi Md. Rokibul Alam sir, Professor, Department of Computer Science and Engineering, Khulna University of Engineering & Technology (KUET), for his excellent advices, guidance and right directions without which this thesis may not have reached a state it is in now. I would like to thank my seniors who inspired us to implement different Ideas throughout this project. We would also like to thank our friends for their association also.

Any constructive comments, suggestions, criticism from teachers as well as seniors will be highly appreciated and gratefully acknowledged.

Authors

Mazharul Islam

Abstract

MANETs consist of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. They form a highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes. For the highly dynamic behaviour and due to mobile nodes, threats from compromised nodes inside the network, limited physical security, scalability and lack of centralized management MANETs is more vulnerable. So, Ensuring Security is must and also challenging for node-to-node communication. Black hole attacks are very dangerous and is not considered by any routing protocol, instead most of the routing protocols don't concern about network security. Any malicious node can practically drop data instead of forwarding them. Hence a new method is proposed for reliable data forwarding in MANETs during Blackhole attacks based on ad-hoc on-demand multipath distance vector (AOMDV) protocol. Message is divided in some parts and sent. At the receiver end using homomorphic encryption to sum up the encrypted message. The performance is measured by simulating the scenario in NS2 calculating throughputs, packet delivery ratio etc. It is more reliable than General AOMDV, while AOMDV is vulnerable with the intrusion of malicious nodes.

Contents

Lists of Tables

Lists of Figures