FUZZY-ASSISTED ANT-BASED SECURE ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORK

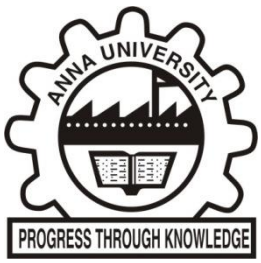
A THESIS

Submitted by

PUSHPALAKSHMI R

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY



FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

ANNA UNIVERSITY

CHENNAI 600 025

MARCH 2014

ABSTRACT

The usability of Mobile Ad hoc Networks (MANETs) has increased due to advancement in wireless technology and several series of real time applications that use such technology. The lack of centralized control and dynamic behaviour of ad hoc network enforces new demands on the routing protocol. We need a routing protocol that quickly adapts to topology changes and carries out transmissions in a secured manner without any alterations.

Quite many research activities have been carried out to develop on-demand routing algorithms for MANETs. Most on-demand routing algorithm such as Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV) discover routes by applying flooding concept. Although flooding is simple, it increases the routing overhead and causes broadcast storm problem that results in high channel contention and packet collision in the network. To reduce the impact of flooding and to support network scalability, a number of cluster based routing algorithms have been recommended over the years based on certain parameters, for example, node id, node degree, residual energy, node weightage or degree of future contact of node. Most of these approaches have focused on reducing number of clusters or discovering routes based on specific Quality-of-Service (QoS) parameters. They aim to improve the route discovery process without considering the behaviour of nodes in the network.

Typically MANET is more vulnerable to various network attacks. Usually, a common type of attacks targets at the underlying routing protocols. Malicious nodes have opportunities to alter, eavesdrop or discard routing information. Some routing protocols such as Secure Cluster Based Routing Protocol (SCBRP), Secure Ad hoc On-demand Distance Vector (SAODV) and Secure Ad hoc Routing (SAR) have been proposed to address the security issues in routing. They rely on cryptographic techniques to ensure security. However, the routing security mainly depends on dynamic behavior of the network nodes.

In this thesis, a trust-based clustering algorithm is proposed and strengthened to develop three new routing algorithms so as to improve the security level in route discovery process. The proposed algorithm is motivated by the fact that different types of attacks occur quite naturally in MANETs since centralized control is not available. The three newly developed algorithms are based on trustworthiness of nodes in MANETs that rely on node's packet forwarding status.

The trust computation process developed in this research forms the basis of the Dominating Set (DS) based routing approach that aims to improve the packet delivery ratio even in presence of attackers in the network. A fuzzy controller is designed to compute trust value for each node based on packet transmissions. The scheme selects the nodes with highest trust value and probability of future contact as cluster heads. Intra cluster communication is carried out directly through cluster heads, whereas the inter cluster communication is carried out by establishing virtual link between clusters

either by using common neighbors or connector nodes. It also applies a basic Key Management Scheme (KMS) to improve the security level of the routing process. The KMS generates secret key based on trust value of node and frequent traffic pattern exists between nodes.

Secure QoS routing protocol using Ant Colony Optimization (ACO) selects QoS aware, shortest, trustable routing path by employing ant algorithm. The general ACO algorithm is modified to allow in selection of routing path based on trust value of the nodes lying in the path and delay experienced in it. The third routing algorithm selects the trustable path based on length and trustworthiness of the path. The algorithm mainly applies a new KMS for establishing secure communication. The KMS combines the idea of fuzzy logic and traffic mining into key generation and key distribution process. Frequent traffic pattern that exists between the nodes are identified and employed in key generation process. Mobile agents are deployed to collect information about cluster members. The code and the data of mobile agents are protected by using cryptographic techniques.

Detailed performance evaluations are provided by using simulation to investigate the performance behaviour of the proposed routing algorithms under different network layer attacks and exhibiting their relative effectiveness against the existing approaches. The results reveal that the proposed algorithms minimize routing delay and achieve better packet delivery ratio and security-level. It also maintains resiliency against network attacks.