Survey on Secure and Efficient AODV Routing Protocol Using Trust Mechanism

Dushyant Trivedi¹, Yash Patel²

¹Information Technology, PIET
²Information Technology, PIET

Abstract — In Ad-hoc networking its devices found network for the communication and it is self-governing of a central infrastructure, no central ability and self-organization. Organization the devices in the ad-hoc network can move randomly gives rise to various kind of problems, such as routing and security. Its work on trust based secure routing protocol and it will more secure AODV routing protocol. Purpose of this work is to reduce the path breakage due to the smaller amount battery power by dynamically replacing the nodes with very less power by the nodes having enough amount of power. Only power aware routing is lacking for MANET, thus we introduce, and trust based routing along with power. Apart from considering battery power of nodes, the proposed system considers the location of the node. The relay nodes are chosen towards the destination to reduce packet drops. In this algorithm has also been developed to reduce the packet dropping attack in MANET which has been simulated on Network simulator-2 (NS-2) and demonstrated an increase in packet delivery ratio, throughput while decrease in average end-to-end delay as compared the basic AODV protocol.

Keywords— Mobile Ad hoc Network, Routing Protocol, Path maintenance, Trust based secure routing Protocol, Power Aware Trust Based Protocol.

I. INTRODUCTION

Mobile and Ad-hoc Network (MANET) is a structure less, self-organizing network where each node can move and does not require any central base station. Therefore, the routes between two nodes in the MANET for the data communication may have many hops. In the MANET any node can act as a host as well as a router for forwarding the data packets to other nodes. Due to the node mobility frequent topology changes occurs in the network. Nodes in the MANET have very limited resources such as very limited communication ranges, so some node in the network cannot communicates directly.

Routing is a very important issue in the MANET. Routing is used for the data transfer between any two nodes if they are not directly connected. Number of routing algorithms have been proposed for mobile ad-hoc network. There are two basic classes of routing protocols used in the MANET. One is proactive routing protocols which are table driven routing protocols. Another class is reactive routing protocols also known as on-demand routing protocols. The reactive routing protocols creates and maintains routes only when needed. Most widely used and efficient reactive routing protocol in MANET is Ad-hoc On-demand Distance Vector (AODV) routing. AODV routing protocol works in two phases, one is Route discovery phase and other is Route maintenance. AODV protocol uses the various control packets like RREQ, RREP, and RERR etc. for route discovery and route maintenance process.

In this work an algorithm has been developed where dynamic change of routes are carried out when any chance of path breakage occurs by considering the node mobility and battery power simultaneously which helps in saving the network energy. Another objective here is to secure the network from the various types of packet dropping attacks.

II. RELATED WORK

AODV routing protocol performs both unicast and multicast routing. It maintains the route as long as they are needed by the source node. It uses the sequence number field to avoid the looping and to ensure the freshness of the route. As wireless network are prone to path breakage due to the mobility of the nodes, fading environment etc., so it is beneficial to provide some stable routes which can improves the performance of AODV protocol. Many researchers have proposed changes in the AODV protocol for increasing the efficiency, stability and security of the MANETs. The main problems that should be considered are energy efficiency and security in Ad hoc networks [1].

Yang et al. have proposed a PAMP (Power aware multipath routing protocol) where routes are created by calculating the remaining power of nodes and recorded in RREQ packets. The resources present in MANET are limited, e.g., battery power MANET is very important resource as it has limited life and are not easily rechargeable. So we have to reduce the energy consumption in MANET by using an efficient routing algorithm for data transmission.

When destination node receives this RREQ packet it calculates the amount of power needed for data transmission and compares the both. If remaining power is less than the required power then destination node waits for the next RREQ.
consequently very long delay occurs in the route creation process. Wang et al. [4] have proposed a power efficient routing and maintenance protocol in MANET which removes some drawbacks of PAMP protocol.

This protocol mainly considers the transmission bandwidth between two nodes and creates the routes on the basis of the power available for the data transmission in those routes. The proper security mechanism for detecting the possible attacks in AODV routing protocol needs to be incorporated for the security. Many type of attacks are possible in MANET and the most frequent one is packet dropping attack. John and Vivekanandan [11] have proposed a framework for secure routing in Mobile and ad-hoc network. This protocol focus on cooperation in packet forwarding. A secure energy efficient routing protocol for wireless ad-hoc networks has been proposed by Mahimkar et al which selects the paths along nodes with a higher reputation number and higher residual battery capacity.

III. LITERATURE SURVEY

The advancement in wireless technology in the present era have created networks with low cost and low power consumption. One of such networks which exist is called as Mobile Ad-hoc network which is characterized by wirelessly connected nodes with frequent change in network topology. As the nodes are connected wirelessly a routing mechanism (routing protocols) is required for successful transmission of packets.

Sometimes two or more nodes sending the information simultaneously results in collisions. Hence medium access controls (MAC protocols) are required for efficient transmission and avoiding collision. In this research work performance of various attributes like throughput, average jitter, end-to-end delay for two Routing protocols (AODV and DSR) is analysed by increasing the mobility of node, applying different MAC layer protocols (CSMA and ALOHA) and changing the type of scenario.

Mobile Ad Hoc Networks (MANETs) are collections of mobile nodes that can communicate with one another using multihop wireless links. MANETs are often deployed in the environments, where there is no fixed infrastructure and centralized management. The nodes of mobile ad hoc networks are susceptible to compromise. In such a scenario, designing an efficient, trustworthy and secure routing protocol has been a major challenge over the last many years. In this paper, they propose a Trust Based Secure on Demand Routing Protocol called “TSDRP”. Ad hoc On-demand Distance Vector (AODV) routing protocol has been modified to implement TSDRP for making it secure to thwart attacks like Blackhole attack and DoS attack. To evaluate the performances, they have considered Packet Delivery Fraction (PDF), Average Throughput (AT) and Normalized Routing Load (NRL).

A mobile ad hoc network is a wireless network with high of mobility, no fixed infrastructure and no central administration. These characteristics make MANET more vulnerable to attack. In ad hoc network, active attack i.e. DOS and blackhole attack can easily occur. These attacks could decrease the performance of the routing protocol. They have proposed a new trust mechanism to secure the AODV routing protocol called Trust AODV. In this paper, they have improved the performance of proposed secure protocol by using an ant algorithm. Ant agent put a positive pheromone when the node is trusted. Path communication is chosen based on pheromone value. An evaluate and compare the performance of proposed protocol before and after using ant algorithm in term of packet delivery ratio and throughput. However, in term of end-to-end delay there is no significant effect to the performance.

Rapid advances in wireless ad hoc networks lead to increase their applications in real life. Since wireless ad hoc networks have no centralized infrastructure and management, they are vulnerable to several security threats. Malicious packet dropping is a serious attack against these networks. In this attack, an adversary node tries to drop all or partial received packets instead of forwarding them to the next hop through the path. A dangerous type of this attack is called black hole. In this attack, after absorbing network traffic by the malicious node, it drops all received packets to form a denial of service (DOS) attack. In this paper, a dynamic trust model to defend network against this attack is proposed. In this approach, a node trusts all immediate neighbours initially. Getting feedback from neighbours’ behaviours, a node updates the corresponding trust value. The simulation results by NS-2 show that the attack is detected successfully with low false positive probability.

In that Ad-hoc networking portable devices establish network for the communication and it is independent of a central infrastructure. Due to the absence of central Infrastructure the devices in the ad-hoc network can move randomly gives rise to various kind of problems, such as routing and security. In MANET resources are very limited. Battery power of the node or Energy of the node is an important resource for the MANET [2].

The Ad-hoc on demand Distance Vector Routing is most widely used protocol in MANET. AODV routing protocol creates the routes On-demand when any node has some data for the communication. In AODV routes breaks due to due to the node mobility and/or less battery power. Purpose of this work is to reduce the path breakage due to the less battery power by dynamically replacing the nodes with very less power by the nodes having sufficient amount of power.
A distributed algorithm has also been developed to reduce the packet dropping attack in MANET which has been simulated on Network simulator-2 (NS-2) and demonstrated an increase in packet delivery ratio, throughput while decrease in average end-to-end delay as compared the basic AODV protocol.

In this paper two algorithms are proposed to improve the energy consumption and security of MANET. The proposed algorithms utilize the dynamic route shortening and local route repair scheme to improve the reliable packet delivery and enhance the route maintenance if route breaks occur due to less remaining energy in the nodes.

IV. POWER AWARE TRUST BASED ROUTING IN MANET

1. Security Model

Trust Model

Trust value of each node is evaluated based on the various parameters like length of the association, ratio of number of packets forwarded successfully by the neighbors to the total number of packets sent to that neighbor and average time taken to respond to a route request. Based on the above parameters trust level of each node can be of the following types:

a) Node i is a stranger(S) to neighbor node j If node i has never send/receive messages to/from node j.

b) Node i is a acquaintance (A) to neighbor node j If node i has send/receive few messages from node.

c) Node i is a friend (F) to neighbor node j If node i has send/receive plenty of message to/from node j.

Trust value is initially set to zero. It is incremented based on how many numbers of packets are successfully transmitted from node i to node j. Following Table I show the trust levels and corresponding trust value that is used to determine the reliable route.

Route request

1. When source node wants to communicate with another node (destination), if no routing information is available, it initiates path discovery by sending the route request that contains source id, broadcast id, destination id and trust values of each neighbor and reliability of source node and, hop count.

2. On accepting the route request the neighbor node calculates its reliability using Table II by checking its trust value and the remaining energy and takes the following decision.
   If the reliability is very low (0.0) the node discards the route request Else if the reliability is an acceptable value, cumulative reliability is found by adding the predecessor reliability with its reliability.
   If the node has already received the route request with same source address and same broadcast id and if the cumulative reliability is less than the cumulative reliability of current route request, the previous route request path is rejected and the current route request path is recorded.

3. The route request is then forwarded to the intermediate node’s neighbors which contains trust values of each neighbor and cumulative reliability. Each time when route request is forwarded from one node to another, hop count is incremented and that is also send along with the route request.

Route Reply

1. When two or more route request reaches the destination from the same source and same broadcast id and in different path, it selects the most reliable path by finding the average reliability. Average reliability is computed as follows:
   \[
   \text{Avg reliability} = \frac{\text{Cumulative reliability}}{\text{Number of hops}}
   \]

2. If average reliability of one path is greater than reply another path, that path is selected and the route is send by the destination in that path to the source.

3. The source receives the new path and sends the packet in that reliable path and record the path for future use.

2. Energy Model
In this phase the main aim is to reduce the energy consumption in the route maintenance case. In original AODV when any route breaks then the upstream node sends the Route error (RERR) message to the source node which initiate process to create the new route to provide the further communication. In the proposed work the route is created locally by using the neighboring nodes of the upstream nodes which have the highest energy. By this we can increase the life of the node.

Here node maintains the some energy weights on the basis of their remaining energy.

1) If any node has the energy more than 70% it means it has sufficient energy to take part in the routing process and it can take part for the longer time, then assign the highest energy weight. If it has energy less than 30% then it cannot take part in the routing process for the longer time. So the routing process avoids these type of nodes and minimum energy weight 1 is assigned to such node 1 otherwise weight 2 will be given as shown in Fig. 1.

![Fig. 1. All the nodes with their energy weights](image)

2) When any route breaks during the data transmission then the upstream node creates the route locally and sends the local route request message (LRREQ) to all the neighboring node then

![Fig. 2. Selection of alternate local route on the basis of energy weights](image)

3) All the neighboring nodes send the route reply message with its energy weights and the upstream node selects the highest energy weight among them. The process is shown in Fig. 2. After the creation of new route on the basis of the remaining energy power in the node, some node becomes dead due to the less remaining energy power. In the energy implementation part we are applying the dynamic route change strategy in the network. In this method we are trying to recover the route locally whenever route breakage occurs due to the less remaining energy in the node.

CONCLUSION

Two algorithms are proposed to improve the energy consumption and security of MANET. To improve the security of the network, trust based routing is carried out to transmit packets to destination. The proposed algorithms utilize the dynamic route shortening and local route repair scheme to improve the reliable packet delivery and enhance the route maintenance if route breaks occur due to less remaining energy in the nodes. The proposed schemes can be incorporated into any Ad-hoc on demand routing protocol. The application of proposed algorithms produces better performance of the AODV protocol which is validated by simulation results.

REFERENCE


