Cache Based Secure Hybrid Routing Protocol in MANET

Amroj Kaur Gill¹ Dr. Rajneesh Talwar²
¹M. Tech Student ²Principal
Department of Electronics Communication Engineering
Chandigarh Group of Colleges Technical Campus, Jhanjeri

Abstract—Routing in Mobile Adhoc Networks is a widely researched area in the recent years. Many researchers have proposed various techniques for efficient route the data from source to destination and compared their approach with the already existing approaches. In this paper, a novel technique for hybrid routing is proposed which includes the properties of both proactive and reactive approaches and each node in the network stores the most frequent routes in its cache memory, so that it can be accessed within no time. The proposed approach is tested on both with attack and without attack scenarios and results of the same can be compared. In future the approach must be implemented for large network density and can be compared with other hybrid routing protocols.

Key words: Hybrid routing, MANET, WLAN

I. INTRODUCTION

1.1 Mobile Ad-hoc network is a collection of wireless devices called wireless nodes, which connect dynamically and transfer information. Wireless nodes can be anything like personal computers (desktops/laptops) attached with wireless LAN cards, Personal Digital Assistants (PDA), or any other types of wireless (or mobile) communication devices [1]. Ad-hoc networks are mobile wireless networks which have no fixed infrastructure. The routers are not fixed—instead each and every node acts as a router itself and forwards the traffic from other nodes. These ad-hoc networks were previously used for mainly military applications. There are presently two variations of mobile wireless networks infrastructure based and Infrastructure less networks [2].

The infrastructure based networks, also called as Cellular network, have fixed wired gateways. They have predetermined base stations that are connected through wires to other base stations. The transmission range [3] of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example of this type includes office wireless local area networks (WLANs). The other type of network, Infrastructure less network, is [4] known as Mobile Ad hoc Network (MANET). These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other.

In MANET, a mobile node can act as a source, a destination, or an intermediate node for data transmission. When wireless nodes play role [5] of intermediate node, it caters a router which receives and transmit the data packets into closer neighbor to destination node. Due to nature of the ad-hoc network, wireless nodes tend to move rather than stay still. Thus network topology may change time to time. Mobile ad-hoc network [6] have many advantages which are listed as: Low cost of deployment: It means ad hoc networks can be deployed on the fly; therefore no expensive infrastructure such as data cables or copper wires is required. Fast deployment: which means ad hoc networks are very handy and easy to set up since there are no cables used. Deployment time is reduced[7]. Dynamic Configuration: It means ad hoc network's configuration can change in time dynamically [8].

When compared to configurability of LANs, it is very easy to change the network topology of a wireless network.

Table driven: Table-driven routing protocols attempt to maintain the consistent, update routing info from every node to other node in network. These protocols are required each node to maintain one or more tables to store [10] routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast.

Source initiated (or demand driven): A diverse approach from table-driven routing is source-initiated or demand routing. In this type of routing, the routes are created only when requested by the source node. When a source node requires a route to the destination, it initiates a process known as route discovery process from within the network. This process is finished once a route is established or all possible route permutations have been examined. Once after a route is established [11], it is maintained by using a route maintenance method until either the destination becomes unapproachable along every path from the source or until that route is no longer desired.

Hybrid: This routing protocol can combine the features of two categories. Nodes are belong to a specific geographical region or with particular distance from concerning node are told in routing zone and use the table driven routing protocol. [12] Communication between the nodes in the different zones are relied on on-demand or source-initiated of protocols.

II. LITERATURE SURVEY

A routing protocol is responsible for building and maintaining paths between sources and destinations while optimizing performance network. The ability to compute and store, as well as the instability of the wireless communication medium result in topology changes fast and unpredictable.
Zone Routing Protocol [1] (ZRP) has the first hybrid protocol proposed in literature which employs both table driven and source initiated protocols. It defined the zone of each node that consists of k neighborhood. [2] Routing zone can be performed with the use of proactive protocol and routing between the nodes in distinct zones can be performed by the on-demand routing protocol. These ZRP can perform the effective route discovery via border-casting; route requests can be spread by the multicasting directly to nodes on border of its zone. Size of zone can be determined dynamically based on the network load [3].

Another routing protocol Zone-Based Hierarchical Link State (ZHLS) [4] is proposed which divides network into the non-overlapping zones that based on the physical location information. A routing zone is well defined for each and every node discretely, and the zones of the neighboring nodes overlap. The routing zone has a radius expressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most hops. It can be performed the zone assignments and zone sizes that do not vary dynamically. In broadcasting process [5], the broadcasting node sends a route request packet to each of its peripheral nodes. This type of one-to-many transmission can be implemented as multicast to reduce resource usage.

HARP, Hybrid Ad-hoc Routing Protocol, relied on Distributed Dynamic Routing [6] protocol to decompose the network into their zones. HARP may a hybrid protocol that separates the network into [7] several zones, which makes a hierarchical protocol as the protocol ZHLS (zone-based hierarchical link state). HARP is based on GPS (Global positioning system), which allows each node to identify its physical position before mapping an area with table to identify it to which it belongs. A number of forward nodes in every zone can responsible to communicate the nodes in their zones. HARP[8] can use own custom protocol for the inter-zone routing, whose goal can reduce the delays via early path maintenance. While HARP can create the zones of varied sizes, it contains no control over zones and doesn’t adjust dynamically their sizes.

SHARP (Sharp Hybrid Adaptive Routing Protocol) [9] can be utilized the proactive and reactive protocol which is used to perform the routing. Every SHARP node can be determined network neighborhood, which is called proactive zone, in the routing information pertain to it is disseminated proactively. In this, FSR [10], FishEye State Routing, may link-state protocol which exchanged the periodic link-state information. This period of link state propagation can be determined by one distance to other destination. ADV [11] may be Adaptive Distance Vector algorithm which defines the demand of characteristics to vary the frequency and size of the routing updates. Some researchers examined the reactive protocols with their timer-directed route to produce the backup routes prior to the closing of primary link. Their protocol can be used fixed timer value across all the nodes that can be determined offline from the past history of link failure statistics.

III. PROBLEM FORMULATION
The problem with both reactive and proactive routing protocol can be dealt using hybrid routing protocol. In proactive routing protocol each node in the network has to manage routing table information which requires a considerable amount of memory and moreover the information which it stores sometimes can never be used. It has to update its routing table time to time. In reactive routing protocol the route can be predicted in real time which requires the source node to flood the network either with the complete message or a beacon signal. This operation requires huge amount of bandwidth and also it creates congestion in the network.

So, an optimize routing protocol is required which is capable of solving both problems which comes across while using reactive and proactive protocol. Hybrid of these protocols can be used which has a capability of finding the route in real time and also stores the most frequent routes. Many of the nodes in the network are attack prone and the data or information which these malicious nodes carry can be lost or corrupted. So our hybrid routing protocol must also consider the routes which consist of trusted nodes.

IV. OBJECTIVE
The objective of this work is to propose a routing protocol which can predict the route in real time by using the properties of both reactive and proactive routing protocols by flooding the network with the beacon signal and updating the route information in the limited and fast memory available with the nodes, in order to use these routes for future transmission which satisfies the condition of proactive routing. These routes are updated time to time according to the frequency of their use.

The routes predicted by the Hybrid routing protocol, also consists of the trusted nodes. The trust of the node is mainly contributed by the number of retransmissions of the particular node.

V. PROPOSED METHODOLOGY
In Mobile Ad hoc Network (MANET) the hybrid routing protocol is used which is the combination of both proactive and reactive routing protocol. The proposed approach in this work maintains a cache memory which saves the routing information.

Initially, each route in the network must be found out using the reactive protocol mechanism which minimizes the excess bandwidth used in case of proactive protocol and the route information is stored in the cache memory which is limited and can be accessed fast as compared to any other memory and same machine cycle (time to access the memory). Now, as the routing information is saved in the memory and constantly updated time to time, routing through the most frequent route is looked as proactive in which the route is fixed and saved in the memory. This helps in overcoming the drawback of reactive routing in which there is no need to flood the network every time for the most frequent routes and the route request delays. So, using this scheme a single protocol acts as both reactive and proactive routing protocol.

Trust factor of each node is calculated by taking the two parameters i.e. frequency of its use and number of retransmissions from that node. Frequency of use of any node is maintained in the cache memory along with the route information. The more the frequency of node the more is the trust factor. Another important parameter is the
number of retransmissions from that node means the data lost while it is routed or transmitted from that node. It also includes the energy consideration regarding that node. As the number of retransmissions from any node increases, the energy required to retransmit the data also increases.

The routing table maintained in the cache memory updates itself according to the trust value which further reduces the routing overhead.

VI. RESULTS AND DISCUSSIONS

Fig. 1 shows the graph between Average Energy consumed by the node to transfer data and the Number of nodes. As the nodes in the network increases, energy consumed also increases but energy consumed by the proposed model is less than the energy consumed by the basic hybrid routing protocol approach.

![Fig. 1: Average Energy Consumed vs. Number of Nodes](image)

Fig. 1: Average Energy Consumed vs. Number of Nodes

Fig. 2 shows the graph between the throughput of the network and the number of nodes. The graph shows that the throughput of the network in the proposed cache based approach is better than the basic hybrid routing protocol approach.

![Fig. 2: Throughput of the Network vs. Number of Nodes](image)

Fig. 2: Throughput of the Network vs. Number of Nodes

Fig. 3 shows the comparison of the average packet delivery delay for both basic and proposed approach. Here basic approach means the route calculated consists of nodes which are non trusted and in the proposed approach the nodes considered in determining the route as trusted.

![Fig. 3: Packet Delivery delay vs. Number of Nodes](image)

Fig. 3: Packet Delivery delay vs. Number of Nodes

VII. CONCLUSION AND FUTURE SCOPE

In a cache memory based frequent route saving approach, the most frequent route is saved in the memory and updated likewise. The result shown above validates our protocol in both the scenarios i.e. with or without black hole attack. Also proposed protocol outperforms the basic approach for both throughput and energy consumed. It means that the transfer of packet is both energy efficient and consumes less time to reach to the destination.

In future, the proposed protocol must be tested for large number of nodes and with heavy data transfer on the network.

REFERENCES


All rights reserved by www.ijsrd.com 987


