International Conference on Advanced Material Technologies (ICAMT)-2016

27th and 28th December 2016

Dadi Institute of Engineering and Technology (DIET), Visakhapatnam, Andhra Pradesh, India.

Secure Fisheye State Routing Protocol

Dr.V.Sangeeta
Professor, Dept.of.CSE
Dadi Institute of Engineering and Technology

Amulya Pentakota
Computer Science Department
Dadi Institute of Engineering and Technology Visakhapatnam

ABSTRACT: Wireless technology is an emerging technology that will allow users to access information and services regardless of their position. In contrast to infrastructure based networks, in wireless ad hoc networks, all nodes are mobile and can be connected dynamically in an arbitrary manner. Fisheye state routing introduces the notion of multilevel fisheye scope to reduce routing update overhead in large networks. All nodes in the networks behave as routers and take part in discovery and maintenance of routers to other nodes in the network. Nodes exchange link state entries with their neighbours with a frequency which depends on distance to destination. Fisheye state routing is similar to Link State routing, but uses a fisheye technique to reduce the consumption of bandwidth by control over head.

Keywords: FSR, GSR, Link state, Scope

1. INTRODUCTION

An ad hoc network works without infrastructure. Thus, it usually applies to temporary networks or wherever is difficult to build infrastructure. It turns out that a message should be Delivered from node to node across a number of hops in an ad hoc network [2]. Therefore, an efficient routing protocol can help message exchanging in an efficient way. There are many protocols designed for different purposes such as shortest path, energy consumption, etc. Existing routing protocols can be classified into categories such as reactive, proactive and hybrid schemes [1].

Ad hoc wireless networks are self-organizing, self configuring and instantly deployable in response to application needs without a fixed infrastructure existence. Therefore ad hoc networks are very attractive for tactical communication in military and law enforcement. They are also expected to play an important role in civilian forum such as convention centres, conferences, and electronic class rooms. Mobility potentially very large number of mobile nodes and limited resources make routing

in ad hoc networks extremely challenging. The routing protocols for ad hoc wireless networks have to adapt quickly to the frequent and unpredictable changes of topology.

2. RELATED WORK

Routing could be a method of sending a message from one host to another it is called unicast. Routing protocols for ad-hoc wireless networks are measure typically used for mobility management and scalable design, in which mobility management is completed through information exchanges between mobile nodes in the ad-hoc wireless network. Commonly, the information exchanges occur often, the network maintains correct information of host locations and alternative relevant information since they consume a lot of communication resources like bandwidth and power [2]. With less frequent information exchanges, these metrics diminish however there is a lot of uncertainty concerning the host location. Scalable design requires each routing protocol and resource consumptions to be scalable.

A routing protocol provides the discovery and maintenance of route should consume less overhead and data bandwidth. Routing within the ad-hoc wireless network poses special challenges as a result of its infrastructure less network and its dynamic topology. However, when all hosts move including the home agent such a strategy can't be directly applied. Routing information should be localized to fastly to changes such as hosts' moveable. A routing protocol is crucial whenever a packet wants to be bimanual over via many nodes to achieve at its destination [5]. A routing protocol has to discover a route for data packet delivery and prepare the packet delivered to the destination. Routing Protocols have been associate active space of research several for several years; many protocols are prompt keeping applications and type of network.

Routing protocols are classified they are:

1. Proactive or Table Driven Protocols
2. Reactive or On-demand Protocols
3. Hybrid Protocols

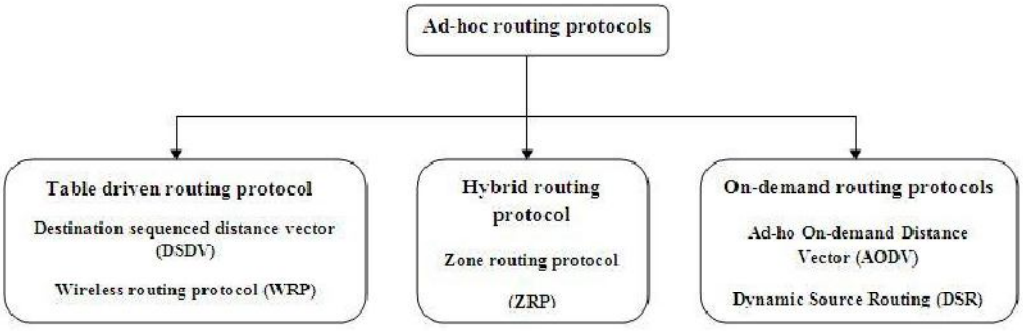

Fig: - 1 Basic routing protocol

2.1. Proactive (or) Table driven:

A proactive routing protocol is also called as table driven. Each node within the network maintains complete routing information concerning the network by sporadically changing the routing table. One or additional routing tables are maintained at every node and are exchanged sporadically to share the topology information with the neighbouring nodes so as to take maintain of within the network. Thus, when a node must send data packets, there's no delay for locating the route throughout the network. The best network context for proactive protocols is that the low (or) no mobility networks [5]. The foremost accepted proactive protocols are FSR, DSDV and OLSR. This kind of routing protocols works the same way as that of routing protocols for wired networks.

2.2. Reactive or On-demand:

Reactive routing protocols, also called on-demand routing, Routes to the destination are discovered only when really needed. When current node wants to send packet to some destination, it checks its routing table to see whether or not it has a route. If no route exists, Current node performs route discovery procedure to search a path to the destination. Reactive routing protocols will dramatically minimize routing overhead as a result of they are does not have to be compelled to look for and maintain the routes on that there's no data traffic. Such property is so much necessary within the recurrent limited environment.

.

The most accepted reactive protocols are DSR and AODV. They do not initiate route discovery by themselves, till they are requested, when a current node request to find out a route. These protocols setup routes when demanded. When a node needs to communicate with new node in the network, and the current node will not have a route to the node it needs to communicate with, reactive routing protocols can establish a route for the end to end node.

2.3. Hybrid routing protocols:

Hybrid protocols inherit the advantage of high-speed routing type proactive and less overhead control messages from reactive protocols. The characteristics of proactive and reactive routing Protocols are often able to integrate to realize hybrid routing technique. Hybrid routing protocols might exhibit proactive or reactive behaviour depending on the circumstance, thus permit flexibility based on the wireless network. Communication between nodes in several zones can deem the on-demand or source initiated protocols. The foremost typical protocols are ZRP and TORA [3].
FSR originates from two routing protocols i.e. GSR and LSR.

Link State Routing:

Link state routing protocols maintain complete road map of the network in each router running a link state routing protocol. Each router running a link state routing protocol originates

information about the router, its directly connected links, and the state of those links. This information is sent to all the routers in the network as multicast messages. Link-state routing always try to maintain full networks topology by updating itself incrementally whenever a change happen in network. Each router in the network keeps a copy of it, without changing it. After obtaining the complete picture of network topology, each router will independently calculate its own best paths to reach the destination networks.

Global State Routing (GSR):

The GSR protocol is based on the traditional Link State algorithm. However, GSR has improved the way information is disseminated in Link State algorithm by restricting the update messages between intermediate nodes only [4]. In GSR, each node maintains a link state table based on the up-to-date information received from neighbouring nodes, and periodically

Fisheye State Routing (FSR)

Fisheye state routing protocol is implemented based on link state routing protocol and global state routing protocol.

The FSR protocol is the descendent of GSR. FSR reduces the size of the update messages in GSR by updating the network information for nearby nodes at a higher frequency than for the remote nodes, which lie outside the fisheye scope. This makes FSR more scalable to large networks than the protocols described so far in this section. However,

Scalability comes at the price of reduced accuracy. This is because as mobility increases the routes to remote destination become less accurate. This can be overcome by increasing the frequency at which updates are sent to remote destinations proportional to the level of mobility.

FSR is similar to Link State (LS) routing. A topology table is maintained at each node. Routing table updating differentiates FSR from LSR. Link state routing broadcasts the update messages to the whole network, while in FSR, the routing information is disseminated. The control messages can be reduced by adopting different periods for exchanging update messages [4]. Fisheye state routing protocol uses the”fisheye” technique proposed by Klein rock and Stevens to reduce the size of information required to represent graphical data. The eye of a fish captures with high detail the pixels near the focal point. The detail decreases as the distance from the focal point increases. Based on this idea, mobile nodes exchange update messages more frequently with nearer mobile nodes, and less frequently with farther nodes.

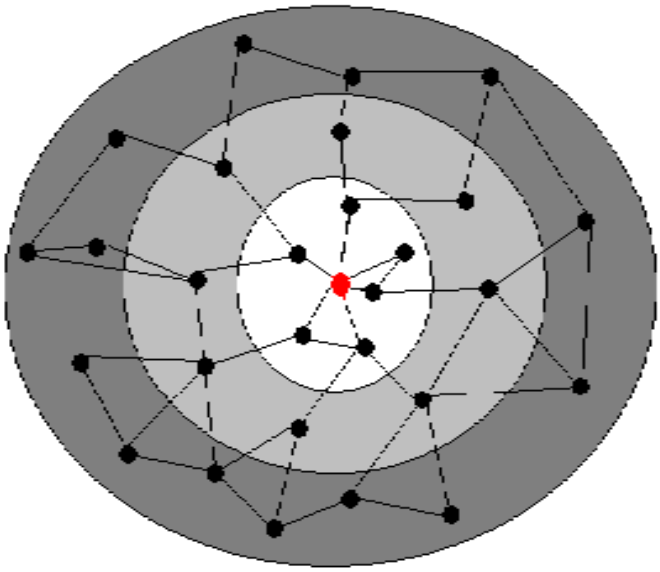

Fig: - 2. Scope of FSR

The accuracy of the nodes information depends on how far a node is. The node information is more accurate if it is nearer, while the node information becomes less accurate if it is farther. In other words, path information appears to have progressively less detail as the distance increases [3]. However, the imprecise route path will be corrected by each forwarding node on the route path. The route becomes progressively more accurate as the packet gets closer to destination. Therefore, FSR can reduce control overhead but does not seriously compromise the routing accuracy.

3. METHODOLOGY

Mobile Ad hoc networks are different from traditional wired networks due to its mobility and infrastructure less topology [1]. Mobile Ad hoc networks do not provide security to the data. As it is shared between neighbours it is very difficult to provide security due to these attacks occurs on the data. This behaviour makes the MANET vulnerable to different security threats. The threats on a MANET can be from the unauthorized nodes those are outside the network or from the nodes inside the network. Threats from the nodes outside of the network are likely to be more easily detected than the internal nodes of the network. The threats from the internal nodes are difficult to detect as they are from trusted sources. Threats on the MANET can be broadly divided into 2 categories.

- External Threats
- Internal Threats

FSR follows hop by hop data forwarding. The source node or any intermediate nodes retrieve the destination address from the data packet, and look at their routing tables. If the route is known, i.e., there is an entry for the destination, the data packet is sent to the next hop node. This procedure

repeats until the packet finally reaches the destination. FSR does not provide any security feature for preventing a node's misbehaviour for not forwarding the data packet to the next node.

Types of Attacks on FSR The attacks on FSR protocol can be divided into 2 categories.

(i) Active attacks

(ii) Passive attacks

Active attacks are attacks which are lunched intended to disrupt the service of a network. Such attacks produce threats to confidentiality, integrity and availability of data and services in MANET [2]. Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service. Here the term active attack has been used to mean that if any of the node's intention in the network to disrupt any of the security goals intended, such types of attack can be termed as active attack. In contrast the passive attack is an attack which is performed by the nodes to benefice itself only. The node has no other intention to disrupt the service of the network.

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

Usually in FSR data is shared among the neighbours of each and every node, so there is a chance of lack of security. To attack the network there may be any chance of entering node as new node and disturbing the network, we need to identify these types of malicious nodes for providing security to the network.

Black hole attack

In networking, **black holes** refer to places in the network where incoming or outgoing traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. When examining the topology of the network, the black holes themselves are invisible, and can only be detected by monitoring the lost traffic.

The black hole attack comes under the category of passive attacks which is launched by a selfish or malicious node to benefice itself in terms of conserving its energy or battery power. A node which is a black hole has two properties – it participates in the route discovery process and the second property is that, it sometimes does not forward the data packet towards to destination. These nodes create problems in data transmission if they come in the route to destination. The nodes in the MANET are resource constrained; resource may be bandwidth, energy etc. Most of the nodes in MANET rely on batteries as their source of power; so, some of the nodes behave maliciously to conserve their limited battery power. So, when the data packets are forwarded to the destination these selfish nodes simply do not forward the data packets towards the destination. So all the packets

move up to that node and disappear. Hence, these nodes act as a black hole which causes data packet dropping. Black hole attack can be launched both on control packets and data packets, but here we have considered the case of data packets, because in fisheye state routing algorithm the number of control packets are very less compared to the number of data packets. But, when forwarding data packets if some of the packets are dropped, then alternate route is searched to forward the packets even if that route is the shortest one. This increases the time complexity of the protocol.

Proposed Solution to minimize black hole attacks in FSR

This problem can be minimized by selecting the appropriate route where the number of malicious nodes will be minimum. This can be done in a two step process. (i) By detecting the malicious nodes (ii) By avoiding the malicious node while computing optimal path to detect the malicious node we have proposed one method which uses a time stamp along with the data packets. If a node forwards a packet to the next hop then the next to next hop can acknowledge the source by replying the time stamp to the source which is at a distance of two hops. In the traditional FSR algorithm each node has one list and three tables. In the modified version that is proposed here a weight list is maintained in each node in addition to the previous list and the three tables. The weight list stores the weight assigned to each link in the network. The weight is assigned on the basis of the number of times a node has behaved maliciously. A threshold is maintained depending on the requirement of level of security of the network. If any link cost exceeds the threshold value then that link is moved from the table in the next route discovery process. While calculating the shortest distance to each destination using the traditional Dijkstra‟s algorithm used in FSR it has been modified slightly. Instead of taking the number of intermediate hop counts for calculation as in the case of the FSR algorithm, the actual link cost is taken into consideration. The weight function has been modified to consider the assigned link cost based on the number of malicious behaviour instead of number of hop counts. The route calculated using this algorithm may not be the

Shortest one, but it provides the optimal route all the time which contains least number of malicious nodes. So the amount of data packet dropping can be minimized.

4. CONCLUSION

We present a new routing scheme, Fisheye State Routing, which provides an efficient, scalable solution for wireless, mobile ad hoc networks. We have compared the performance of our routing protocol with on demand routing protocols such as AODV and DSR. When the number of communication pairs increases, on demand routing protocols will generate considerable routing overhead. A simulation shows that FSR is more desirable for large mobile networks when mobility is

high and the bandwidth is low. By choosing proper number of scope levels and radius size, FSR proves to be a flexible and provides security.

REFERENCES

[1] Securing Fisheye State Routing Algorithm against Data Packet Dropping By Malicious Nodes in MANET, **Prof. Pabitra Mohan Khilar** Department of Computer Science and Engineering National Institute of Technology, Rourkela, India 2009.

[2] Po-Wah Yau; Mitchell, C.J., "Reputation methods for routing security for mobile ad hoc networks" Mobile Future and Symposium on Trends in Communications, 2003.

[3] Guangyu Pei, Gerla,M, Tsu-WeiChen, “Fisheye state routing: a routing scheme for ad hoc wireless networks” Communications, IEEE International Conference on Volume 1, Issue , Pages: 70-74 vol.1, 2000. [4] C. E. Perkins and P. Bhagwat, “Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers,”Comput. Commun. Rev., vol. 24, pp. 234–244, Oct. 1994.

[4] Fisheye Routing Protocols (FSR) for http//en.wikipedia.org/wiki/Fisheye_State_Routing.

[5] Mohammad, S.N, Ashraf, M.J,Wasiq, S.,Iqbal, S.,Javaid, N. “Analysis and Modeling of Network Connectivity in Routing Protocols for MANETs and VANETs”. IEEE wireless. Areas Commun., pp. 528– 533, Oct. 2013.