ISSN No. 0976-5697

Volume 2, No. 2, Mar-Apr 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Performance Evaluation on Reactive Routing Protocols for Ad Hoc Networks

D. Suresh kumar*
School of Computing Science & Engineering
VIT University
Vellore-632014, Tamilnadu, India
sureshkumard2009@vit.ac.in

K. Manikandan
School of Computing Science & Engineering
VIT University
Vellore-632014, Tamilnadu, India
kmanikandan@vit.ac.in

M. A. Saleem Durai
School of Computing Science & Engineering
VIT University
Vellore-632014, Tamilnadu, India
masaleemdurai@vit.ac.in

***Abstract*:** Ad Hoc Networks are wireless networks which do not have any fixed any fixed infrastructure or any centralized server system. These networks reorganize themselves dynamically and the routing from one node to another change often .The differentiating feature of an ad hoc network is that the functionality normally assigned to infrastructure components, such as routers, access points and switches. In most cases it is an assumption that the participating nodes are movable may not have guaranteed uptime and have limited energy resources .In an Ad Hoc Network routing between source nodes to destination node securely and efficiently is a challenging task in the real time. In our research we will be comparing various routing protocols and find which protocol is best for which type of network. We will discuss about genetic algorithm (GA) and backup routing protocols which are popular and we will further incorporate the security by adding authentication to nodes that participates in the network as the attribute in the routing protocols in order to provide secure routing in ad hoc network.

Keywords: Ad hoc network; genetic algorithm; routers; backup routing; authentication.

I. INTRODUCTION

The growing wireless network with flexibility and simplicity has been got increasing applications in various places. Most of these wireless networks are based on infrastructure less in which no access point or a router needed. An ad hoc network is a collection of mobile hosts forming a temporary network without the aid of any established infrastructure, or support of any base station. An Ad Hoc Network has no central administration point. All the hosts work at the same time as routers and communicate with each other over wireless connections. The nodes may also be mobile; they can move freely, and organize themselves randomly i.e. each host can dynamically enter and leave the network. These types of network are especially suitable in scenarios like where the deployment of an infrastructure is either not feasible or is not cost effective .In infrastructure-based wireless networks, such as cellular networks or Wi-Fi, the wireless connection goes only one-hop to the access point or the base station, the remainder of the routing happens in the wired domain. Thus, the network topology may change frequently and rapidly. This means that the network has to adapt itself to the current topology. An Ad Hoc Network may either work as a self-configured stand-alone network or may be connected to the Internet through gateway nodes.

II. AD HOC ROUTING PROTOCOLS

The growth Ad Hoc Network is due to the high mobility of the nodes, and no centralized administration in the routing protocol. But in Ad Hoc network routing is big task to maintain. The routing protocol can be classified in two types, a) Table driven approach (*proactive*) and b) On Demand routing protocol (*reactive*).

Proactive routing protocols are the table driven approach in which every nodes has to maintain at least one routing table .The tables and nodes are been updated frequently by the changing routing information between nodes periodically. In order to maintain the updated routing information at all the hosts the network information has to be exchanged between all the nodes in a frequent time. But the performance of the Ad Hoc Network is highly affected due to updating information is done periodically where the infrastructure changes periodically.

Unlike table driven approach routing protocols, reactive protocols initiate a route discovery only when a path from source to destination is needed. This reduces the overhead as compared to proactive protocols, but it increases the transmission delay. But, it is required to re-establish a new route whenever the route is needed or old route is broken down. Each move of the mobile nodes will change the topology of the network in the transmission route. Sometimes leads to the disconnection of link, because communication is through radio waves. When there is a poor environment and distance between the nodes increases the link disconnection may occur. And due to lack of trusted

nodes Ad Hoc Networks require specialized authentication protocol. Hence it is understood that it is necessary to have some authentication when a node participates in the routing process. These challenges are been answered with large number of routing protocols and ad hoc routing remains an active and dynamically evolving research area.

There are many existing routing protocols for ad hoc networks showing different implementation situation. But the basic goal is to minimize control overhead, packet loss ratio, and energy usage while maximizing the throughput.

A. Reactive routing protocols (on-demand routing protocols)

The on-demand routing protocols represents are the set of routing protocols where the route is created only when the source request for a route to destination. A route discovery process is initiated when the route is been requested by the source. Once a route is formed or multiple routes are obtained to the destination, the route discovery process comes to an end. Then the next step is route maintenance procedure maintains the active routes for the duration of their lifetime. The route maintenance phase is a difficult phase because the nodes have to update their table in a regular time interval since it is a Ad Hoc Network where the link may change at anytime .There are many reactive routing protocols available and we analyze few routing protocols and discuss its strength and weakness.

III. AD HOC ON-DEMAND DISTANCE VECTOR (ADOV)

The AODV routing protocols [1] are widely used protocol in Ad Hoc Network where a source node seeking to send a data packet to a destination node checks its route table to see if it already has a valid route to the destination node. If a route exists, it simply forwards the packets to the next hop along the way to the destination. On the other hand, if there is no route in the table, the source node begins a route discovery process. As the first step in route discovery process the source node broadcasts a route request (RREQ) packet to its immediate neighbors, and those nodes broadcast further to their neighbors until the request reaches either an intermediate node with a route to the destination or the destination node itself. This RREQ packet contains the IP address of the source node, IP address of the destination node, current sequence number, and the sequence number known last. This packet will be sent to all the neighbors of the source node initially and it moves to the one hop neighbor of the source node. An intermediate node will reply to the request packet only when it has the destination sequence number that is greater than or equal to the number contained in the route request packet header. Whenever the intermediate nodes forward the route request packets to their neighbors, they record in their route tables the address of the neighbors from which the first copy of the packet has come from. This recorded information is later used to construct the reverse path for the (RREP) route reply packet. If the same RREQ packets arrive later on, they are discarded. When the route reply packet arrives from the destination or the intermediate node, the node forward it along the established reverse path and store the forward route entry in their route table by the use of symmetric links. By simulating AODV in NS-2 we come to know that the dropping packets is medium when compared to DSR and the End to End delay is low that is less than 2 sec but the total processing time is high when compared to the other routing protocols . The Fig 1 shows the minimal processing time vs. throughput of receiving bits.

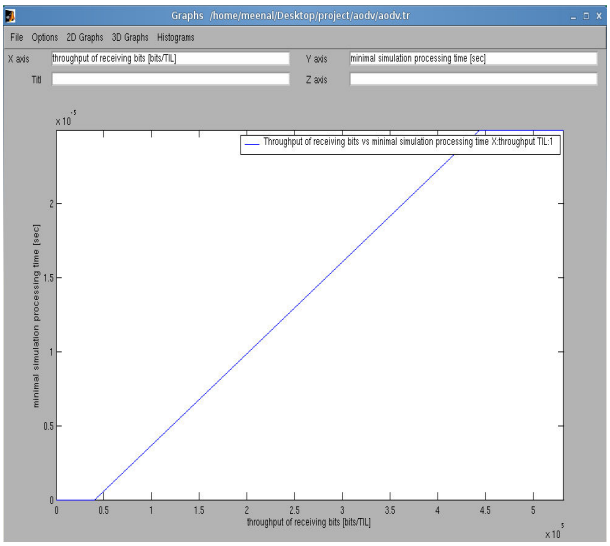

Figure 1. AODV comparison between receiving bits vs minimal simulation processing time

IV. DYNAMIC SOURCE ROUTING (DSR)

DSR is the most widely used routing algorithms [2], which has route discovery phase and route maintenance phases. Route discovery phase contains both rote request message (RREQ) and route reply message (RREP). In a route discovery phase when a node wishes to send a message, it first broadcast a route request packet to its neighbors. Every node within a broadcast range adds their node id to the route request packet and again rebroadcasts. Finally, one of the broadcast messages will reach either to the destination node or to a node that has the recent route to the destination. Since each node maintains a route cache, it first checks its cache for a route that matches the requested destination. If a route is found in the cache, then the node will return a route reply message to the source node rather than forwarding the route request message further. The first packet that reached the destination node will have a complete route. A route reply packet is sent to the source that contains the complete route from source to destination. Thus, the source node knows its route to the destination node and can initiate the routing of the data packets. The source caches this route in its route cache. In route maintenance phase, two types of packets are used, namely route error and acknowledgments. DSR ensures the validity of existing routes based on the acknowledgments received from the neighboring nodes that data packets have been transmitted to the next hop. A route error packet is generated when a node has failed to receive acknowledgment. This route error packet is sent to the source in order to initiate a new route discovery phase. Upon receiving the route error message, nodes remove the route entry that uses the broken

link within their route caches. By simulating DSR routing protocol using NS-2 we get the performance graph by X-graph tool we analyze that dropping packets ration is low when compared to any other routing protocols. The processing time is medium but the End to End delay is minimum 2 sec which is average when compared with AODV protocol. Fig 2 shows the comparison between throughputs of receiving bits vs minimal simulation processing time.

V. A CROSS-LAYER EFFECIENT ROUTING PROTOCOL FOR AD HOC NETWORKS

A novel cross-layer efficient Routing Protocol (CLERP) [3], which adopts cross-layer approach to repair the broken links and adaptive mechanism for link connectivity to configure the rate of sending hello packets. Traditional layered architecture like the seven-layer open systems interconnect (OSI) model is not optimal for Ad hoc network. The architecture forbids direct communication between nonadjacent layers and communication between adjacent layers is limited to Procedure calls and responses. CLERP is presented by sharing the cross-layer cache information while still maintaining separation between the MAC layer (802.11) and the route layer (AODV) in protocol design. To enhance the connectivity of the network cross layer cache is used where the nodes updates its cross layer cache if there is any communication from its neighbor. Whereas the backup paths are found during the route request or ACK exchange procedure. If a node that is not present in the route gets ACK messages not for itself transmitted by a neighbor, it records MAC address of the receiver and the sender of the packet. When a node again receives the ACK message, it verifies the last stored sender of the RTS is same the receiver of the ACK then the receiver of the ACK is neighbor and will be updated in the cross layer cache. When a node finds a link failure then the node caches the packets transmitted and sends the RREQ message to all its one hop neighbor nodes. If any of the neighbor node having the route to the destination then the data packets are transmitted and never been dropped in the case of link failure. We perform the simulation of this protocol using NS-2 and we use X graph to make the performance evaluation.

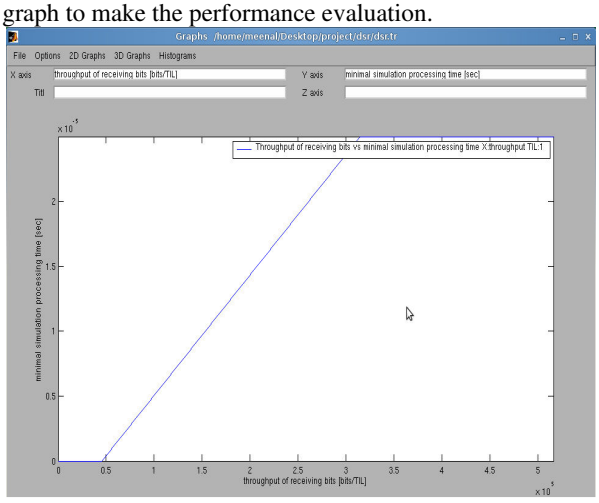

Figure 2. DSR comparison between receiving bits vs Minimal simulation processing time

By varying the packet rate we study the performance of CLERP with AODV. We fix the max speed as 10m/s and number of connections as 10. The CLERP provides lower delay for the same throughput.

With the help of result we come to know that the throughput is more when compared to the AODV with minimal delay time and its suitable for minimum processing time scenarios.

VI. IMPROVED AODV ROUTING PROTOCOL

In the AODV routing protocol [4] we come to know that there exist some problems like link failure due to long latency in receiving Hello message and the local repair mechanism is not optimal way to control network overhead and so on. So in this protocol they have improved the above problems by improving hello mechanism, enhanced route repair process and single route improvement.

So in the improvement of hello mechanism they have defined a hello-flag stored in node information where it's initialized as 1 in default. Where the value 0 shows that the node can send hello message and 1 means not to send. Hence by using this network congestion is been avoided. Where as in local route repair process if we didn't get reply from our neighbor node in a time out we decide that is link failure.

And choose the alternate path from the node that is failed. But in enhanced route repair process we broadcast the RREQ message to the next to next hop node then the next to next hop node send the RREP message that the message has reached then the route is been updated in the Source node. Hence by using this route repair process the network wide flooded is avoided, the time taken to route discovery is reduced and the control packets are used are less than the local route repair process.

And instead of maintaining single route from source to destination we find multiple paths from source to destination. This enhances the protocol in the case of route failure also to avoid route discovery when link failure occurs.

On simulating the protocol in NS-2 and obtaining the result in X graph we can make performance analysis that throughput time is minimized. The result shows the minimal simulation time vs delay. By observing the result we can observe that the delay taken to send a packet from source to destination is minimal.

VII. SECURE ON-DEMAND ROUTING PROTOCOL FOR MANET USING GA

The AODV protocol discovers a route when a node wants to establish a route between the source and destination node. But the performance is been affected when a link or a node fails then the route discovery phase is been reinitiated. The route discovery phase maybe initiated plenty of times since it is a MANET where the nodes move more frequently. To improve the routes stability and to improve

the trust on participating nodes, this paper present a secure backup on demand routing protocol for mobile ad hoc network. SBMR discovers multiple routes from source to destination in order to store a backup route to the destination node to be used in case of link or node failure which avoids the reroute discovery phase. The nodes are been authenticated well in order to know that the participating nodes are not intruders to break the link. And to find the optimal paths from the available multiple paths we use genetic algorithm in our protocol. Initially by using the concepts of AODV multipath routing protocol we find multiple paths available from source to destination node. The design of the GA has components like genetic representation, population initialization, fitness function, selection scheme, crossover and mutation. A routing path contains of sequence of nodes in network. The genetic algorithm is applied to paths that is been obtained from the route discovery phase. GA is to find the shortest path, lowest throughput between source and destination and the larger buffer size that the path has. It is important to obtain the shortest path and lowest delay time as the primary concern then we can choose according to the buffer size.

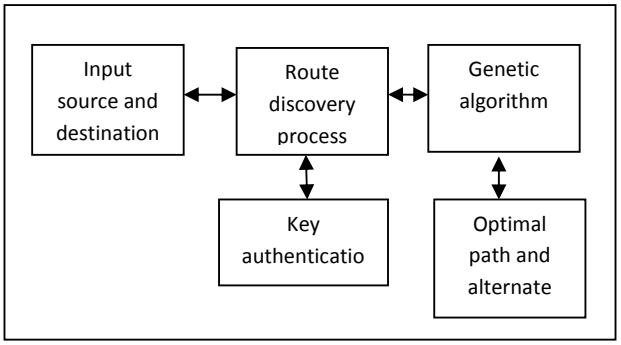

Figure 3. Complete workflow model

The fitness of each chromosome can be calculated as,

$$f(Ch_i) = [\sum_{l \in P(s,r)} c_l + c_d]$$

The Ch represents the chromosome fitness value and Cd the delay time taken by each chromosome where Cl represents the cost of the path. Crossover is done to find the better solution from current one. Since chromosome are been used as path structure, every time we choose two chromosomes Ch_i and Ch_j for crossover. Ch_i and Ch_j should have at least one common node mentioned as *v*. Now we have two paths $Ch_i(s \rightarrow r)$ and $Ch_j(s \rightarrow r)$. Now we have v in both paths can be mentioned as $Ch_i(s \rightarrow v)$ and Ch_i $(v \rightarrow r)$, $Ch_j(s \rightarrow v)$ and $Ch_j(v \rightarrow r)$. Now we exchange the sub path Ch_i $(v \rightarrow r)$ and $Ch_j(v \rightarrow r)$. The population will undergo mutation after the crossover had been performed. Both crossover and mutation may produce infeasible solution so we check it is acyclic. The crossover can be explained with the following example.

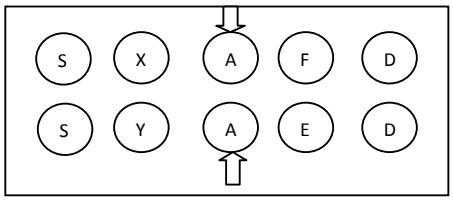

Figure 4. Initial chromosome

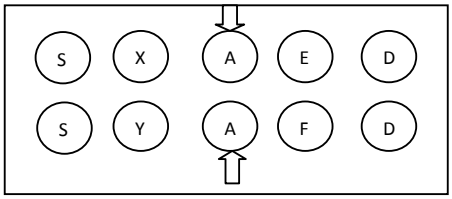

Figure 5. Chromosomes obtained from Initial chromosome

In the above example A is the common node in both chromosomes. So by performing GA we obtain new two more chromosomes in order to obtain optimal value. By using GA we obtain the optimal path from source to destination, and in the same phase we find an alternate path to be used in link failure. The alternate path will be next best path when compared to the optimal path. By this method when a primary path fails we can recover the connection by utilizing the backup paths.

An intruder node can launch any type of attacks like routing misbehavior or packet forwarding misbehavior or sometimes both attacks also. The routing misbehavior attacks means the malicious node may advertise wrong routing information or a wrong distance metric than its actual size to be or a wrong sequence number. The packet forwarding misbehavior means the malicious node purposely disturbs the data forwarding activity. In order to avoid these attacks we use self organized security mechanism which monitors their neighbor nodes and packet forwarding behavior of its neighbor at all time. So we use a valid token to be carried out by the entire legitimate node which is certified while any node without token are been thrown out of network membership. The legitimate node can renew its token from its neighbor before the token expires. In collaborative monitoring all the nodes within a local neighborhood monitor each other. Token renewal: all the legitimate nodes renew the token with their neighborhood node. Token revocation: The neighbors of a malicious node collaboratively revoke its current token. We evaluate and compare the performance of ordinary genetic algorithm for MANET with secure on demand routing protocol for MANET using GA by using NS-2. Fig 6 illustrates the comparison of packet delivery ratio, in which the ordinary genetic algorithm for MANET with secure on demand routing protocol for MANET using GA. Simulation results shows that the packet delivery ratio is more than the ordinary GA because we use security also

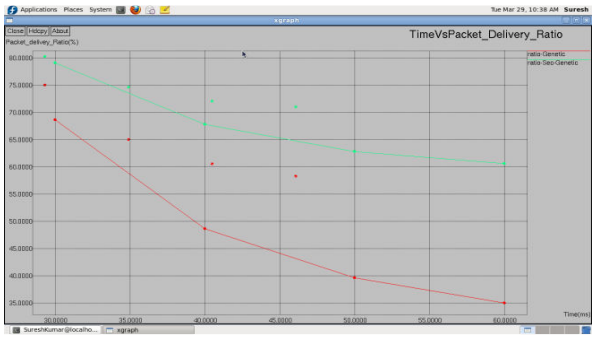

Figure 6. Packet delivery ratio

in our protocols which provides us a confirmation that there is no malicious node present in the routing. Fig.7 illustrates the comparison of packet drop ratio in the network by using the normal GA for MANET and secure on demand routing protocol for MANET using GA. Inititally the there maybe liitle packets loss in our protocol but it will be overcomed in few seconds to give us a better

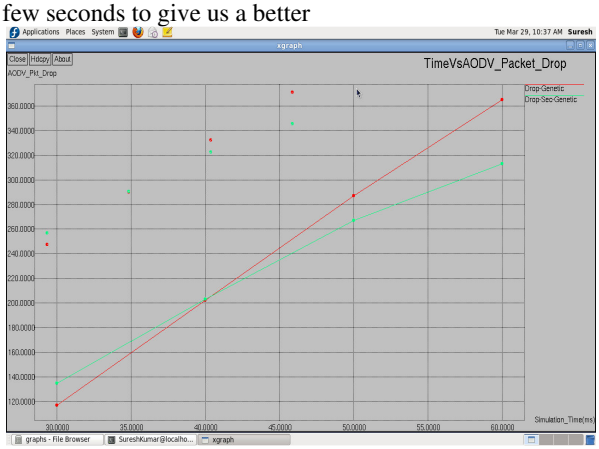

Figure 7. Packets drop

result. Hence by using the backup path no packets will be dropped. No malicous nodes can participate in the network since we use security agent in the network to provide secured routing rotocol.

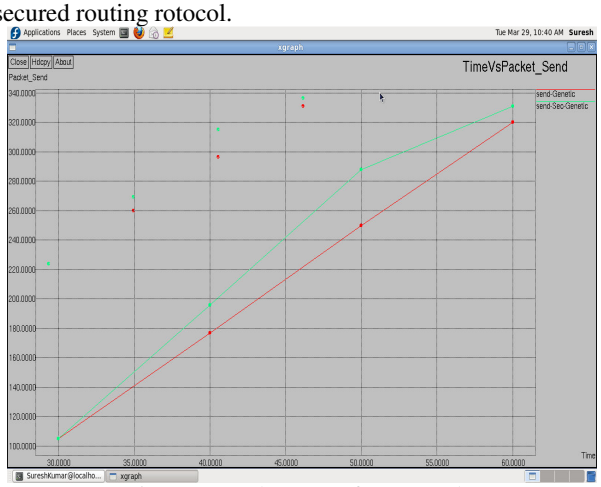

Figure 8. Packets sent from a node

Fig.8 shows the packet sent by secure on demand routing protocol for MANET by GA and ordinary genetic algorithm. The packets sents are more when compared to ordinary GA because we consider buffer size as the parameter in GA to provide maximum data to be sent in a time. So we can transmit more amount of data than the normal routing protocols. So we get a efficient protocol to transmit large amount of data in a small period of time.

VIII. CONCLUSION

Every routing protocol has the same goal that the algorithm should reduce packet overhead, to increase the throughput, to minimize the end to end delay, to reduce route discovery mechanism in the case of link failure and to provide secure route. We have plenty of routing protocols present but we can't state that this specific routing protocol is suitable for all kinds of network and scenarios. Each and every routing protocol has its own advantages and disadvantages like performance time, end to end delay and so on. But we can say that a multipath routing protocol is suitable for all kinds of network because in case of link failure we can use the backup nodes instead of performing route discovery process again. And it reduces the performance time also.

IX. REFERENCES

[1] C. Perkins, "Ad Hoc On-Demand Distance Vector (AODV) Routing," RFC3561, IETF MANET Working Group, July 2003.

[2] D.Johnson and D.Maltz. Dynamic source routing in ad hoc wireless networks. In T.Imielinski and H.Korth, editors, Mobile computing, Kluwer Academic Publishers, Norwell,MA 1996,pp,153-181.

[3] Wang qing-wen, Shi hao-shan, Jiang yi and Cheng Wei, "A Cross Layer effecient Routing Protocol for Ad hoc Networks" IEEE second international workshop, vol.0 pp.154-158, 2010.

[4] Fei Jiang , Jian Jun Hao "Simulation of An Improved AODV Algorithm for Ad Hoc Network", IEEE , vol.1 ,pp.540-543, 2010.

[5] Seyed Hossein Hosseini nazhad Ghazani, "A New Survey of Routing Algorithms in Ad Hoc Networks:, IEEE, vol.3, pp. 684-688, 2010.

[6] G.Lavanya,C.Kumar and A.rex Macedo arokiaraj, "Secured backup routing protocol for Ad hoc networks", IEEE,pp.45-50, 2010.
Tsung-Chuan Huang, Sheng-Yu Huang and Lung Tang, "AODV-Based Backup Routing Scheme in Mobile Ad Hoc Networks" IEEE, pp.254-258, 2010.

[7] Wenjing YANG, XinyuYANG, Shusen YANG, "A Stable Backup Routing Protocol Based on Link Lifetime in Mobile Ad hoc Networks", IEEE , pp. 202-207, 2010.

[8] Luo Chao, Li Ping'an , " An efficient routing approach as an extension of the AODV protocol", IEEE, vol.1,pp. 95-99,2010.

[9] Siyu Zhan, Yongxiang Peng ,Yaling Yang, Jiangping Li, "An Open Architecture for the Routing protocols Design in Ad hoc Networks" , IEEE,pp.18-22, 2010.

[10] Kilhung Lee, "A backup path routing for guaranteeing bandwidth in mobile ad hoc networks for multimedia applications", in proc. springer multimedia tools appl, 11 January 2011.