Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security in Fuzzy Improved Adaptive Delay Multicast Routing Protocol

B.Ravi Prasad
Research scholar,CSE Dept
GIT, GITAM University
RRSCET, Hyderabad, India

Dr.G.Veereswara Swamy
Professor
GIT, GITAM University
Visakapatnam, India

Dr.G.Venkateswara rao
Associate Professor,Dept of IT
GIT, GITAM University
Visakapatnam, India

***Abstract-* Multicasting can improve the efficiency of the wireless link when sending multiple copies of messages by exploiting the inherent broadcast property of wireless transmission. Although multicast routing algorithms in MANETs could be efficient in many situations, but the devices in MANETs are more vulnerable to attacks. In the areas where secured information is primary requirement then developers need to concentrate on security in multicast routing in MANETs. In this paper the ROUTE_REQ packet in Fuzzy improved ADRP is modified to achieve security in multicast routing. By doing this even though number of paths are decreased and simulation time increases, secured paths are find out between source to destination. A ns-2 simulation study performed and our results revealed that secured paths are find between source to destination, increase in simulation time and reduce in number of routing messages in Secured Fuzzy improved ADRP compared to Fuzzy improved ADRP.**

General Terms __*Theory and Protocol*

***Keywords-* Mobile Ad hoc networks, Multicast Routing, Adaptive Delay Multicast Routing, Fuzzy method, Security, NS-2**

I. INTRODUCTION

A mobile ad-hoc network (MANET)[1] is an autonomous collection of mobile nodes that communicates over bandwidth constrained wireless links. This network is not supported by any fixed infrastructure or central administration. The nodes are self organized and can be deployed anywhere, any time to support a particular purpose. Typically application areas of it includes battle fields, rescue sites and data acquisition in remote areas. An ad-hoc network is also useful in conventions and classrooms where participants share information dynamically.

In a typical ad hoc environment, network hosts work in groups to carry out a given task. Hence, multicast data transfer is more predominant than unicast data transfer. In military networks, multicast traffic dominates due to need of group communications. Multicasting involves the transmission of a datagram to a group of zero or more hosts identified by a single destination address, and is intended for group oriented computing. The use of multicasting within MANETs has many benefits. It can improve the efficiency of wireless channel while sending multiple copies of same data to different hosts. Instead of sending data via multiple unicast, multicasting minimizes channel consumption, sender and router processing, energy consumption and delivery delay.

Multicast routing in MANETs is much more complex than in wired networks and faces several challenges. Multicast group members move, which prevents the use of a fixed infrastructure multicast topology. Various multicast protocols have been proposed to perform multicasting in ad-hoc networks. Multicast Routing protocols for MANETs have traditionally used shortest path routing to obtain paths to destinations, and do not consider traffic load or delay as an explicit factor. ADRP [4] gives a path source to destinations in which the delay is less than mean delay which is extension of wardrop routing in wireless networks[3]. The main concern is that overhead that ADRP create. Fuzzy Improved Adaptive Delay Multicast Routing Protocol uses Fuzzy method and Reducing overhead method to control overhead in ADRP to achieve low end to end delay , High packet delivery ratio and low energy consumption compared to ADRP. Security-Aware ad hoc Routing [10] used in Fuzzy improved ADRP [11] to find secured paths between source and destination which leads to minimization in number of routing messages and increase in simulation time.

This paper is organized as follows: Section 2 provides description of ADRP. Section 3 describes Fuzzy improved ADRP. Section 4 describes Security-Aware ad-hoc routing. Section 5 describes simulation environment. Section 6 provides simulation results and concluding remarks in section 7.

II. ADAPTIVE DELAY MULTICAST PROTOCOL OVERVIEW

ADRP[4] is mesh based source initiated multicast routing protocol which includes the neighboring concept and load adaptive concept. The routes are built and maintained using traditional request and reply messages. A soft state approach is used for multicast group maintenance.

A. Different Steps in ADRP

Step 1: Neighbor Awareness in ADRP

In ADRP each node keeps the information of all of its neighbors of one-hop distance in a neighbor table. Node periodically transmits HELLO packet shown in Figure 1 to find out its neighbour information.

Type	Source ID	Sequence	Neighbor ID	Neighbor Delay

Figure 1: HELLO packet

Step 2: Creation of Multicast Mesh

In ADRP, A new source initially sends a ROUTE-REQ packet shown in Figure.2. The ROUTE-REQ packet has a data payload field. When an intermediate node receives the ROUTE-REQ packet, it caches the upstream node and updates the field with its own address before forwarding it to next nodes. When a receiver receives the ROUTE-REQ packet, it sends a REP packet to the node from which it received the packet. The upstream node receives the REP packet and adds an entry for the group to its routing table. Then it forwards the REP packet to its own upstream node, and the REP packet eventually reaches the source node. The intermediate nodes that relay the REP packet become forwarding nodes. The forwarding node information is maintained in Forwarding group table. A multicast mesh of a group consists of sources, receivers, forwarding nodes, and links connecting them. The nodes in a multicast mesh are called mesh nodes. After receiving the all the reply packets, at source node mean delay is calculated. Out of all the paths between source to destination, the path which have lesser delay than mean delay is selected for data transmission. By considering all the possible paths between source to multiple destinations , multicast mesh is created.

Type	Sequence no	Timestamp
Source id	Neighbor id	Destination id
FC	Delay	Pay load

Figure 2: ROUTE-REQ packet

Step 3: Multicast Mesh Maintenance

Each source node periodically transmits a LOCAL-REQ packet shown in Figure 3 and only mesh nodes and group neighbor nodes relay the packet. Therefore, all nodes two hops away from the mesh nodes receive the LOCAL-REQ packet. This mechanism repairs most link failures caused by node movements. REP packets to LOCAL-REQ packets are relayed to a source in the same way as REP packets to ROUTE-REQ packets. Forwarding nodes and group neighbor nodes along a multicast mesh are updated as REP packets are relayed to a source.

Type	Sequence no	Timestamp
Source id	Mesh node id	Destination id
FC	Delay	Pay load

Figure 3: LOCAL-REQ packet

Step 4: DATA Packets Transmission

When a node receives a DATA packet, it consults *DataCache t*o see if the packet is duplicate. If so, it discards the packet. Otherwise, it updates *DataCache* to reflect the packet header information, especially the sequence number and the packet is re-broadcast if the receiving node is a forwarding node.

ADRP has many advantages but it suffers from high overhead. This overhead is attributed mainly due to the mesh delivery structure and the network wide broadcasting of ROUTE-REQ packets. When there are many nodes or multicast sources in the network, data and control overhead increases significantly, especially for large networks.

Therefore, one important point to consider is how to reduce the overhead for the mesh creation and maintenance.

III. FUZZY IMPROVED ADRP

In this section, two main approaches are used for increasing the performance of multicast routing in a MANET. First, fuzzy logic based approach[5] is used to deal with imperfect knowledge about link and node characteristics. Second, the domain of control packet flooding[6] is restricted to reduce the overhead. Finally, how these approaches can be integrated into Adaptive delay Multicast Routing Protocol are demonstrated to reduce overhead.

A. Fuzzy Logic Based Approach

In the Mobile Ad-hoc Network, nodes are classified as strong and weak nodes. The strong node has properties like high power level, high bandwidth availability, low loss rate and low moving speed. A strong forwarding group is formed by using strong nodes. The probability of data delivery is increased by using strong forwarding group in the path. These strong forwarding groups are formed by using fuzzy logic based approach which should lead to decreased resources consumption and higher stability of the delivery structure.

In ADRP , any node which receives a ROUTE-REQ packet it catches the upstream node and updates the field with its own address before forwarding to next nodes. It does not consider whether the node is strong or weak from which it receives.

We add several fields to the ROUTE-REQ packet shown in Figure 4.which carry extra information on e.g. bandwidth availability, loss rate experienced, moving speed, and power level to allow the nodes to perform a better route selection in the route request process. Based on such information, the next nodes will be able to compute the probability of caching and forwarding the received ROUTE-REQ message.

Type	Sequence	Source ID	Neighbor ID
Bandwidth	Loss	Speed	Power
Query	Destination ID	FC	Hop count
Delay	Number of previous forwarding group		

Figure 4: Modified ROUTE-REQ packet

Once a node receives a ROUTE-REQ packet, it needs to process the parameters like bandwidth, speed, power and loss rate of the previous node. To process the above parameters node need to use fuzzy logic to handle network dynamics, imprecise information and uncertainty. A simple membership function is used to fuzzify parameters. The value of node parameters are shown in horizontal axis and membership probability is shown in vertical axis. By using the parameters value node have to classify them as low, medium and high probability nodes. Before forwarding node replaces its own parameters information in ROUTE-REQ packet.

Figure 5 show each node's decision process based on the fuzzy logic. Input to this process is the previous node's operating parameters (such as bandwidth, speed , power and loss rate) where the probability of caching and forwarding is the output of the process.

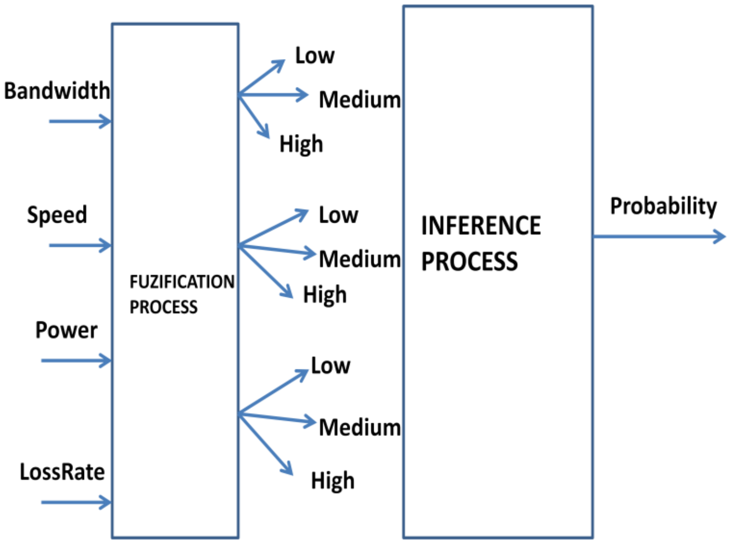

Figure 5: Fuzzification Process

In the inference stage of the fuzzy process, inference laws shown in Algorithm 1 are used to compute the probability of caching and forwarding based on the simple rules.

If ((bandwidth is high) and (power is high) and (speed is low)and(loss rate is low)) then Increase prob. of forwarding ROUTE-REQ packet
If ((bandwidth is low) and (power is low) and (speed is high)and(loss rate is high)) then Decrease prob. of forwarding ROUTE-REQ packet
If ((bandwidth is low) and (power is high) and (speed is medium)and(loss rate is medium)) then Do not change prob. of forwarding ROUTE-REQ packet

Algorithm 1: Inference Rules

B. Reducing the Overhead

In ADRP, Hello packets are periodically send to find out neighbors, ROUTE-REQ packets are used to construct mesh and LOCAL-REQ packets are used to maintain session. All these packets are lead to increase overhead in the mobile ad hoc networks. In the reducing the overhead method, the new forwarding group can be established from the current forwarding group which leads to decrease in the mobility of ROUTE-REQ packets. To implement this idea, Number of previous forwarding group field is added to ROUTE-REQ packet. If a ROUTE-REQ packet has visited many nodes but it does not see any previous forwarding group nodes, then the packet will be discarded. Therefore, when a node receives a new ROUTE-REQ packet, it extracts NOPFG (Number of previous forwarding group) and Hop count fields from the incoming packet. Hop count field is the number of hops to this node from the sender. When a node receives a ROUTE-REQ packet with a hop count greater than the minimum value, it decides if the ROUTE-REQ packet will be forwarded or discarded based on a random value. This random value is based on the forwarding probability which is calculated by fuzzy model (Figure 5). The minimum value of hop count allows a ROUTE-REQ packet to traverse sufficient number of hops to prevent from discarding all copies of ROUTE-REQ packets.

This method does not work for very low density networks. So, before using this, network to be checked. After checking by using algorithm 2, it is decided to use Fuzzy improved ADRP or simple ADRP to construct mesh in the network.

```
Route_req_handle_function ( Route_req_packet jq_packet)
{
If jq_packet isn't a new Route-Req then exit;
If (type==0) do Fuzzy improved ADRP
 If (type==1) do the simple ADRP
}
```

Algorithm 2: ROUTE-REQ Handle

C. Fuzzy Improved ADRP Method

The combination of fuzzy logic based approach and reducing the overhead method is applied on ADRP is to reduce the overhead. The following algorithm 3 shows Fuzzy improved ADRP method function.

```
Fuzzy based ADRP_function (ROUTE_REQ_packet rr_packet)
{
Get hop_count and num_fg from rr_ packet fields;
If rr_packet was discarded then exit;
Get parameters (loss rate, bandwidth, speed, power)
from rr_packet fields;
Fuzzify parameters;
Compute probability of Route-Req forwarding
based on fuzzification results;
Replace parameters of this node to rr_packet fields;
Forward rr_packet based on the computed
probability;
If rr_packet was forwarded then cache rr_packet;
}
```

Algorithm 3:Fuzzy Improved ADRP

In the above algorithm rr_packet is discarded when it has travelled several hops but not seen any node from previous forwarding group.

In Fuzzy improved ADRP, by using fuzzy logic and reducing overhead methods overhead is decreased compared to ADRP. In this main concentration is on how to reduce overhead , by decreasing the necessity of transmitting of ROUTE_REQ and LOCAL-REQ packets but nothing to do with HELLO packets. Order-Optimal neighbor discovery is used to reduce transmitting requirement of HELLO packets in turn leads to reduction in overhead.

IV. HANDLING SECURITY IN FUZZY IMPROVED ADRP

In this section, handling of security in Fuzzy improved ADRP is described. Fuzzy improved ADRP's original behaviour is retained. The packet formats of ROUTE-REQ and REP packets are modified shown in Fig 6. to carry additional security information. The modified Fuzzy improved ADRP is called as Secured Fuzzy improved ADRP.

Type	Sequence	Source ID	Neighbor ID
Bandwidth	Loss	Speed	Power
Query	Destination ID	FC	Hop count
Delay	Number of previous forwarding group		
SEC-REQUIREMENT		SEC-GUARANTEE	

Figure 6.: Modified ROUTE-REQ packet

In Secured Fuzzy improved ADRP , ROUTE-REQ packets have an extra field called SEC-REQUIREMENT[10] that indicates required security for the route the sender wishes to discover. This field is only set once by the sender and does not change during the route discovery phase. When an intermediate node receives a ROUTE_REQ packet, the protocol first checks if the node can satisfy the security requirement indicated in the packet. If the node is secure/capable enough to participate in the routing, Secured Fuzzy improved ADRP behaves like Fuzzy improved ADRP and the ROUTE-REQ packet is forwarded to its neighbors. If the intermediate node cannot satisfy the security requirement, the ROUTE-REQ packet is dropped and not forwarded. When an intermediate node decides to forward the request, a new field in the ROUTE-REQ packet is updated. SEC- GUARANTEE[10] indicates the maximum level of security afforded by the paths discovered.

In the above approach, malicious nodes in the network can change the SEC-REQUIREMENT field. To avoid this protocol must provide cooperation of nodes. This cooperation is achieved by encrypting the ROUTE-REQ headers, or by adding digital signatures and distributing keys to nodes that belong to the same level in the trust hierarchy that can decrypt these headers and re-encrypt them when necessary. The arrival of a ROUTE-REQ packet at the destination indicates the presence of a path from the sender to the receiver that satisfies the security requirement specified by the sender. The destination node sends the REP packet as in Fuzzy improved ADRP, but with additional information indicating the maximum security available over the path. The value of the SEC-GUARANTEE field in the ROUTE-REQ packet is copied to SEC- GUARANTEE field in the REP packet. When the REP packet arrives at an intermediate node in the reverse path, intermediate nodes that are allowed to participate, update their routing tables as in Fuzzy improved ADRP and also record the new SEC-GUARANTEE value. This value indicates the maximum security available on the cached forward path. When a trusted intermediate node answers a ROUTE-REQ query using cached information, this value is compared to the security requirement in the ROUTE-REQ packet. Only when the forward path can guarantee enough security is the cached path information sent back in the REP.

V. SIMULATION ENVIRONMENT

NS-2 simulator was used for performance simulation. NS-2 is originally developed by the University of California at Berkeley and the VINT project and extended to provide simulation support for ad hoc networks by the MONARCH project [8] at Carnegie Mellon University. Reference [9] gives a detailed description about physical layer, data link layer, and IEEE 802.11 MAC protocol used in the simulation. Recently VINT project[2] gives extensions to ns-2 simulator.

Our simulation modeled a network of up to 500 mobile nodes that were placed randomly within 1000m x 1000m area. Radio propagation range for each node was 250 meters and channel capacity was 6 Mbits/sec. The 500 nodes are classified into three levels (high, medium and low), each with 150, 150, and 200 nodes respectively.

When a node sends out the ROUTE-REQ, it uses its own security level as the security requirement for the route. In all measurements, the same amount of data (about 1000 packets) is sent, using the same number of flows (20), and sending at the same rate. The simulation is run until all flows complete sending.

Nodes move according to the "random way-point" model which is characterized by a *pause time*. A pause time of 10 seconds was used in our simulation. Each movement scenario was made on the basis of the model. Member nodes were randomly selected. Each member node joins at the beginning of the simulation and remains as a member throughout the simulation. Each multicast source sends two 512-byte packets per second.

Two different traffic patterns are used to drive the simulations. Traffic pattern 1(P1) consists of 50 CBR flows. 20% of the flows are between the high level nodes, 30% between the medium and 50% between the low level nodes. Traffic pattern 2(P2) also has 20 CBR flows, but the distribution is 33%, 33%, 34% for the high, medium, and low level nodes.

Table I :Simulation Environment

Area	1000m*1000m
Radio Propagation range	250m
Channel capacity	6 Mbits/sec
Pause time	10 sec
Simulation time	80 sec
Packet size	512

VI. SIMULATION RESULTS

Secured Fuzzy improved ADRP has larger ROUTE-REQ and REP packets compared to Fuzzy improved ADRP so The behavior of Secured Fuzzy improved ADRP and Fuzzy improved ADRP cannot be compared directly. The nodes participating in the route discovery in Secured Fuzzy improved ADRP must do additional processing.

A. Path Discovery

On the same traffic patterns , Secured Fuzzy improved ADRP and Fuzzy improved ADRP are executed to observe number of paths are discovered and number of paths are violated security requirement.

Table II:Number of paths discovered

	P1	**P2**
Paths identified by Fuzzy improved ADRP	85	87
Paths identified by Secured Fuzzy improved ADRP	74	70
Security violated paths in Fuzzy improved ADRP	10	15

Secured Fuzzy improved ADRP discovered fewer paths, but these paths are guaranteed to obey the trust requirements of their senders.

B. Routing Message Overheads

Table III shows the numbers of routing protocol messages in Secured Fuzzy improved ADRP and Fuzzy improved ADRP . We observe that there is a drop in the number of ROUTE-REQ messages sent in Secured Fuzzy improved ADRP . This is because the ROUTE-REQ is dropped and not forwarded when the intermediate nodes cannot handle the security requirement of the ROUTE-REQ packets. These results imply that Secured Fuzzy improved ADRP generates fewer routing messages, while enabling applications to find more relevant routes. In the case of Pattern 1, there was a decrease of 5% in ROUTE-REQ messages and 30% in REP messages. For Pattern 2, the results were more accentuated (43% in ROUTE-REQs, and 29% in REPs). This is due to the fact that the trust hierarchy is more equitably distributed in Pattern 2 and paths tend to be smaller.

Table III: Routing Message Overhead

	ROUTE-REQ		**REP**	
	P1	P2	P1	P2
Secured Fuzzy improved ADRP	1800	1027	75	66
Fuzzy improved ADRP	2100	2030	90	83

C. Overall Simulation Time and Transmitted Data

Security restrictions may force packets to follow longer in Secured Fuzzy improved ADRP, but more secure paths and result in taking more time to finish communication. In Table IV the overhead of the protocol is illustrated which shows the overall time to complete transmission of all the traffic flows in both Secured Fuzzy improved ADRP and Fuzzy improved ADRP , and the total amount of data transmitted.

Table IV: Overall Simulation time and transmitted data

	Simulation Time		**Transmitted Data**	
	P1	P2	P1	P2
Secured Fuzzy improved ADRP	2942	3027	9724	9850
Fuzzy improved ADRP	2733	2843	9520	9641

Although Secured Fuzzy improved ADRP takes marginally more time to finish communication, it still finds paths in most cases and delivers almost the same amount of data from senders to the receivers.

VII. CONCLUSION

In this paper by including field SEC-REQUIREMENT in ROUTE_REQ packet in Fuzzy improved ADRP tried to find secured paths from source to destination. This improves security , reduces channel overhead and increases amount of data transmitted in a stipulated time. By using this worm-hole attack and black hole attack are handled successfully. In future work remaining attacks like Sybil etc can be handled.

REFERENCES

[1] Internet Engineering Task Force (IETF) Mobile AdHoc Networks (MANET) Working Group Charter.http://www.ietf.org/html.charters/manet-charter.html.

[2] Kevin Fall, and Kannan Varadhan, editors, "ns notes and documentation,"The VINT Project, UC Berkeley, LBL, USC/ISI and Xerox PARC, Nov.2011. Available at http://www.isi.edu/nsnam/ns/ns-documentation

[3] Raghunathan v and Kumar P.R. "wardrop routing in wireless networks" in IEEE transactions on mobile computing, May 2009 Issue 5 pages 636-652

[4] B Ravi Prasad, Dr.A.Damodaram, Dr.G.Venkateswara rao "Implementation of Adaptive Delay Multicast Routing Protocol" in IJARCCE March 2013

[5] Shams Shafigh, A., K. Abdollahi and A.J. Kassler,2010. Improving performance of ODMRP by Fuzzy Logic Control.WCNIS2010, China.

[6] Abdollahi, K., A. Shams Shafigh and A.J. Kassler,2010. Improving performance of ODMRP by Deleting Lost Join Query Packets. ACIT2010, Spain.

[7] Sudharhan Vasudevan, Micah Adler, Dennis Goeckel , Don Towsley "Efficient Algorithms for Neighbor Discovery in Wireless Networks " IEEE/ACM Transactions on Networking , vol 21,No.1 February 2013

[8] "The CMU Monarch Project"s wireless and mobility extensions to ns," The CMU Monarch Project, Aug. 1999. Available at http://www.monarch.cs.cmu.edu/.

[9] J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," *Proceedings of the Fourth Annual ACM/IEEE InternationalConference on Mobile Computing and Networking*, ACM, Dallas, TX, Oct. 1998.

[10] A Security-Aware Routing Protocol for Wireless Ad Hoc Networks by Seung Yi, Prasad Naldurg, Robin Kravets Dept. of Computer Science University of Illinois at Urbana-Champaign Urbana, IL 61801 Proceeding Mobi Hoc01 Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing 2001

[11] B Ravi Prasad, Dr.A.Damodaram, Dr.G.Venkateswara rao "Fuzzy Improved Adaptive Delay Multicast Routing Protocol" in IJCA March 2014