ISSN 2320-9984

Volume 1, Issue 4, December 2013 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Secured On Demand Multicast Routing

Nirmal Patel
Department of Computer Science
Gyan Ganga College of Technology
Jabalpur, (M.P.) [INDIA]

Prof. Shekhar Tandan
Assistant Professor
Department of Computer Science
Gyan Ganga College of Technology
Jabalpur, (M.P.) [INDIA]

Abstract—*Wireless routing is an area of research which is being focused mainly for congestion avoidance and security. Various routing protocols and techniques are being included in wireless network and making it an area for further research. The need is increasing more due to invention and adaption of wireless communication devices for wireless communication. This work is focusing on security over multicast routing and simulations are being proposed to show the improved packet delivery ration, end to end delay and reduced packet drop rate for Ad hoc On Demand Distance Vector (AODV) routing protocol.*

Attacks are being avoided proactively by including changes in the basic implementation of AODV routing protocol. This work proposed to provide access control technique and unique key based authentication for AODV.

Keywords:—*Wireless Networks, Multicast Routing, AODV, Packet Delivery Ratio, Security*

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are technically different from the traditional wireless networks (e.g. wireless LANs, cellular, digital trunked radio or satellite networks). In traditional wireless networks, the fixed network infrastructures such as access points, base stations or satellites are necessarily required to function as the repeaters to relay/ retransmit the signal from one node to the others. However, none of these network infrastructures is required in ad hoc networks, that is why ad hoc networks are sometimes called as infrastructure less wireless networks.

Moreover, in traditional wireless networks, data can be transmitted from source to destination within two hops. One hop is required to send data from source to fixed infrastructure, and another from this fixed infrastructure to destination. While data can be sent to destination with one or more hops in ad hoc networks. This means that data can be directly sent to destination by using just one hop if destination is in transmission range of source. However, if it is not in this range, data can be delivered through one or more intermediate nodes until reaching destination. This is simply called multihop communication.

Mobile Adhoc Network (MANET) is a group of mobile nodes which work independently and use radio waves to communicate with each other. Nodes which are nearer and come in the radio range of each other can directly communicate. It provides clear communication & low noise or other disturbing factors are reduced. Whereas, if nodes are far apart from each other then intermediate nodes perform routing to pass the packets to adjacent nodes and deliver to the other end. Distant nodes suffer from problems such as no clear communication, high noise or other disturbing factors etc. These without infrastructure networks are distributed in nature and can work at any place making them extensible and robust in working. [1]

Other important characteristics of these networks are such as wireless communication, nodes performing two roles (hosts and routers), no requirement of centralized controller, dynamic topology and self configuring behavior etc. These characteristics make them extremely useful in current communication based era and are being applied in almost all areas. Major application areas of these networks include military battlefields, disaster relief efforts, conferences, classrooms, taxicabs, sports stadiums, boats, and small aircraft etc.

As these networks are being applied in various fields, the challenges are also growing to make them free of vulnerabilities being imposed. The major problems being faced in MANET communication are congestion and security. [1]

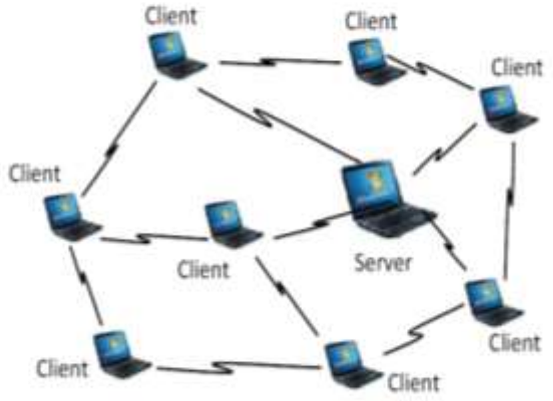

Figure 1: Network Topology for MANET with a trust management server [1]

Initially MANET oriented research efforts were focused on functionality [9]. Nowadays, security is on highest priority since MANETs are being deployed in hostile environments. For achieving security, required services include authentication, confidentiality, integrity, availability, and non-repudiation.

Security measures applied in wired networks are not applicable to MANETs as the characteristics of wireless networks are different due to their “open” network architecture, shared wireless medium, resource constraints, and dynamic network topology impose restrictions for MANETs.[2]

The protocols implemented in ad hoc networks can be roughly classified into two main classes which are proactive (table-driven) and reactive (on-demand) routing protocols. In proactive routing protocols, each node in the network keeps finding the paths to other reachable nodes and inserts them into its own routing table. Note that these paths can be computed based on the routing information which is distributed from the other nodes at predefined interval. In other words, each node periodically maintains and updates its routing table. Hence, each source can immediately send data to destination without waiting for the time required to find a path. However, more routing overhead messages caused by routing advertisement are generated in return which results in some amount of bandwidth consumption.

Whereas the nodes implementing reactive routing protocol find paths to destinations only when they are needed. If source has data to be transmitted, it cannot immediately send the data until path to destination is found. This can be achieved through route discovery process which is occurred on demand. In this process, source sends the route request message in order to either gather the route information or set up the path to destination. Once it receives route reply message, this means that route discovery process is completed and source can start sending the deferred data. This can cause the path set up delay. However, the routing overhead is much reduced due to the fact that the routing overheads including route request and reply messages are flooded only when required by source.

2. AD HOC NETWORKING

Ad hoc networks are spontaneously forming networks of equal nodes. Every node acts as a router and provides routing information to other nodes. Ad hoc networks can adapt quickly to changes in network topology. The topology changes are often caused by nodes changing physical locations, going to power saving mode, or losing contact with other nodes because of external disturbances.

2.1. The Ad-hoc On-demand Distance Vector protocol

The Ad-hoc On-demand Distance Vector (AODV) protocol is a suggested protocol for mobile ad hoc networks (MANETs). It is an on -demand, or reactive, routing protocol in its basic configuration. No effort is made to find new routes before a need arises to transmit packets to a destination for which no route exists. The routes are maintained as long as they are needed by existing connections

2.2. AODV multicast operation

The AODV multicast algorithm uses similar RREQ and RREP messages as in unicast operation. The nodes join the multicast group on-demand, and a multicast tree is created in the process. The tree consists of the group members and nodes connected to the group members. This enables a recipient host to join a multicast group even if it is more than one hop away from a multicast group member. The unicast operation of the protocol also benefits from the information that is gathered while discovering routes for multicast traffic. This cuts down the signaling traffic in the network.

2.3. Route discovery

When a node wishes to find a route for a multicast group, it sends an RREQ message. The destination address in the RREQ message is set to the address of the multicast group.

If the node wants to join the group in question, i.e., to become a multicast router, the J_flag in the message is set.

Any node may respond to a RREQ merely looking for a route, but only a router in the desired multicast tree may respond to a join RREQ. The corresponding RREP message may travel through nodes that are not members of the multicast group. This means that the eventual route may also include hops through non-member nodes.

The multicast RREP message is slightly different from the unicast RREP. The address of the multicast group leader is stored in a field called Group_Leader_Addr. In addition, there is a field called Mgroup_hop. This field is initialized to zero and it is incremented at each hop along the route. Mgroup_hop contains the distance in hops of the source node to the nearest member of the multicast tree.

2.4. Group Hello messages

Because the protocol relies on a group-wide DSN to ensure fresh routes, the group leader broadcasts periodical Group Hello messages. The Group Hello is an usolicited RREP message that has a TTL greater than the diameter of the network. The message contains extensions that indicate the multicast group addresses and the corresponding sequence numbers of all the groups for which the node is the group leader. The sequence number for each group is incremented each time the Group Hello is broadcast. The Hop_Cnt field in the message is initialized as zero and incremented by the intermediate nodes.

The nodes receiving the Group Hello use the information contained therein to update their request tables. If a node does not have an entry for the advertised multicast group, one is inserted. The hop counts are used to determine the current distance from the group leader.

2.5. Multicast tree maintenance

In a network consisting of mobile nodes, link breakages are bound to happen. The breakages should be repaired promptly to ensure maximal connectivity of the multicast group. Multicast tree maintenance has three different scenarios: activating a link when a new node joins the group, pruning the tree when a node leaves the group, and repairing a broken link. Repairing consists of re-establishing the branches when a link goes down and reconnecting the tree after a possible partition in the network.

3. PROPOSED WORK

It uses ODMRP, which is not a popular reactive protocol for implementation of multicasting in MANET. It applies measurement based detection and accusation-based reaction techniques which are applied when attack has been detected means attacks are already existing in the system and might have harm the performance and theft data. It bounds the impact of attacks means minimizes it.

In this work I will be using a proactive mechanism for avoiding the security threats and attacks in the system using following Algorithm:

Step 1: System will check the integrity of the communicating nodes by using identification of the nodes with an access control mechanism

Step 2: If the nodes being participating in the communication will not be able to pass identification test or access control mechanism test then they will not be used for communication by the AODV

Step 3: If the node passes the tests then AODV will accept it as one of the neighbour node.

Step 4: For implementation, I will use RREQ & RREP messages which are unicast messages and will not be burdening the system in terms of multicast routing

3.1. Identification Mechanism

Each node shall be provided with a unique id generated locally on the node and will be specific in a company environment for communication.

3.2. Access Control

Nodes will be group together in clusters of departmental or administrative communication basis and will be having a unique access rule defined on them and when nodes will communicate they will follows the access rules for the communication.

4. SIMULATION MODEL AND PERFORMANCE METRICS

Even though the performance evaluation/ analysis of ad hoc routing protocols is usually measured in homogeneous network, this evaluation is not much effective in the real applications where nodes have different capabilities. To study the efficiency and the effectiveness of routing protocols in heterogeneous ad hoc networks, NS-2 simulator [12] is used to construct the simulation. The details of the simulation scenarios and performance metrics are illustrated in the following sections.

4.1. Simulation Model

In heterogeneous ad hoc networks, each node normally has different capabilities since some nodes are portable devices with limited capacity and battery life, while the others may be stationary or equipped with vehicle. These nodes are not power-constrained and usually have higher capacity than the former one. In this research work, there are two types of nodes which are High-capacity nodes (H-nodes) and General capacity nodes (G-nodes). These two types of nodes have different capacity which are bandwidth and transmission range.

Simulation scenarios are constructed by varying number of nodes. In each scenario, a few nodes approximately 5-20% are included as malicious nodes. For example, if there are totally 50 nodes in the heterogeneous networks, 5 nodes of them are the malicious nodes while other nodes are correct nodes performing good communication practices.

4.2. Performance Evaluation Metrics

The performance metrics which are used to analyze the performances of routing protocols in heterogeneous ad hoc networks are discussed in the following:

- Packet delivery ratio (PDR): the ratio of total number of packets received by destinations to total number of packets sent by sources

∑ Number of packet receive / ∑ Number of packet send

The greater value of packet delivery ratio means the better performance of the protocol.

- Average end-to-end delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

The lower value of end to end delay means the better performance of the protocol.

- Routing overhead: the amount of control information generated/ forwarded to the network by routing algorithm

- Packet Drop Rate: the amount of packets drop rate during the communication

Packet lost = Number of packet send – Number of packet received .

Packet Drop Rate = Average Difference of Packets Received and sent

The lower value of the packet lost means the better performance of the protocol.

5. RESULT & DISCUSSION

Simulation is being performed for the proposed work using NS-2 (2.32) and results are drawn.

Table 1: End to End Delay Measured Using Proposed Work

NUMBER OF NODES	DELAY(MS)
20	130.32
40	34.63
50	174.13
75	627.51
100	1436.67
200	2769.49
300	2873.21

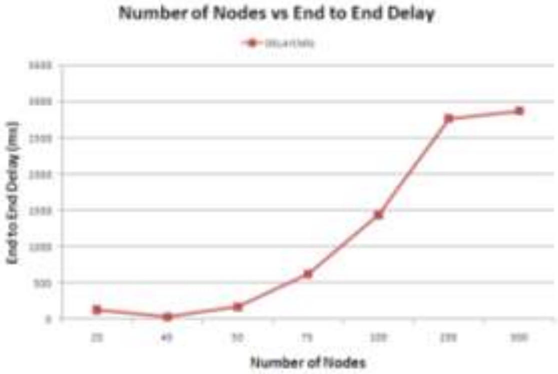

Figure 2: End to End Delay for the Proposed Work

The end to end delay is an indicator of how good communication links and the proposed work is showing a gradual increase in end to end delay with the increase of the number of nodes. A sudden increase in case of 200 nodes has been seen which is occurring due to placement of the nodes. A smooth decrease for 300 nodes verifies the above reason.

Table 2: Routing Overhead Measured Using Proposed Work

NUMBER OF NODES	ROUTING OVERHEAD
20	16.09
40	19.05
50	25.94
75	21.98
100	20.85
200	21.13
300	21.51

Routing overhead is a measure for extra load being applied on the routing protocol and communication system. It is measured in % and from the readings and graphs it is found that the proposed work do not impose much routing overhead on the system. Even when the number of nodes are too many, the routing overhead is under control and do not show any abnormal growth.

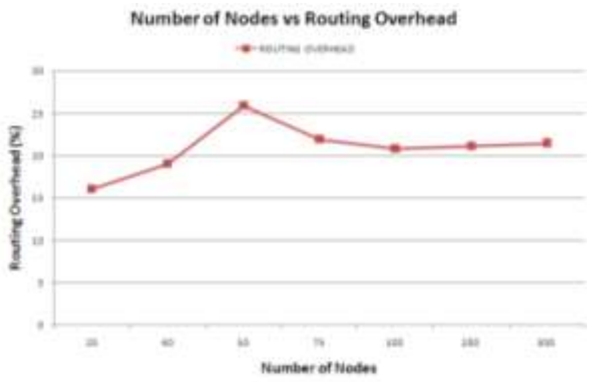

Figure 3: Routing overhead for the Proposed Work

Table 3: Drop Packet Rate Measured Using Proposed Work

NUMBER OF NODES	DROP PACKET RATE
20	13.32
40	31.66
50	15.41
75	16.83
100	13.32
200	17
300	15.24

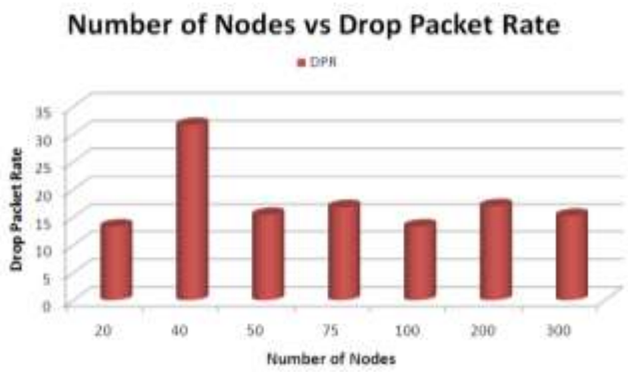

Figure 5: Drop Packet Rate for the Proposed Work

From the figure it is clear that the drop packet rate is also having an average value with the increase of the number of nodes in the network topology.

6. CONCLUSION

The proposed work in this research is focusing on the security aspect of the wireless networks in multicasting environment. The need of security is growing day by day as the newer wireless communication devices are invented and adapted. The proposed work is providing better end to end delays, routing overheads, packet delivery ratio and drop packet rate values and the results drawn are showing the better performance.

The proposed work can be tested for other routing protocols for the MANET such as DSR, OLSR etc. Security can be further made flexible by incorporating a mechanism for modifying the key through an user interface.

REFERENCES:

[1] Jing Dong Reza Curtmola Cristina Nita-Rotaru, “Secure High-Throughput Multicast Routing in Wireless Mesh Networks”, Proceedings of SECON 2008

[2] Rajneesh Agrawal1 and Sandeep Sahu, “Secured Routing Over Manet Using Enhanced Secured Routing (ESR)”, 2013 International Conference on Control, Computing,

Communication and Materials (ICCCCM), 978-1-4799-1375-6/ ©2013 IEEE

[3] J. Dong, R. Curtmola, and C. Nita-Rotaru, "On the pitfalls of using highthroughput multicast metrics in adversarial wireless mesh networks," in Proc. of IEEE SECON '08, 2008.

[4] Y. B. Ko and N. H. Vaidya, "Flooding-based geocasting protocols for mobile ad hoc networks," Mob. Netw. Appl., vol. 7, no. 6, 2002.

[5] R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymous gossip: Improving multicast reliability in mobile ad-hoc networks," in Proc. Of ICDCS, 2001.

[6] Y.-B. Ko and N. H. Vaidya, "GeoTORA: a protocol for geocasting in mobile ad hoc networks," in Proc. of ICNP. IEEE, 2000, p. 240.

[7] E. L. Madruga and J. J. Garcia-Luna-Aceves, "Scalable multicasting: the core-assisted mesh protocol," Mob. Netw. Appl., vol. 6, no. 2, 2001

[8] S. J. Lee, W. Su, and M. Gerla, "On-demand multicast routing protocol in multihop wireless mobile networks," Mob. Netw. Appl., 2002

[9] E. M. Royer and C. E. Perkins, "Multicast ad-hoc on-demand distance vector (MAODV) routing," in Internet Draft, July 2000.

[10] J. G. Jetcheva and D. B. Johnson, "Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks." in Proc. of MobiHoc, 2001, pp. 33–44.

[11] H. Lundgren, E. Nordstrom, and C. Tschudin, "Coping with communication gray zones in IEEE 802.11b based ad hoc networks," in Proc. Of WOWMOM '02. ACM Press, 2002, pp. 49–55.

[12] D. S. J. D. Couto, D. Aguayo, J. C. Bicket, and R. Morris, "A high throughput path metric for multi-hop wireless routing," in Proc. Of MOBICOM '03. ACM, 2003, pp. 134 –146.