© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Optimized Multicast Routing Algorithm Based on Tree Structure in MANETs

K. Navaneethan, V. Prasannakumar, M. Vignesh, N. Purushothaman

Information Technology, SKP Engineering College, Tiruvannamalai, Tamil Nadu, India

ABSTRACT

Mobile Ad hoc Networks play an key role in crisis communications where network needs to be fabricated temporarily and quickly. Since the nodes move erratically, routing protocols must be highly current and consistent to guarantee successful packet delivery. Based on the data delivery structure, most of the existing multicast routing protocols can be classified into two folders: tree-based and mesh-based. We observe that tree-based ones have high furthering proficiency and low consumptions of bandwidth, and they may have poor robustness because only one link occurs between two nodes. As a tree centered multicast routing protocol, MAODV (Multicast Ad hoc On-demand Vector) shows an excellent performance in lightweight ad hoc networks. As the load of network increases, Quality of Service is degraded obviously. In this paper, we evaluate the impact of network load on MAODV protocol, and propose an optimized protocol MAODV-BB (Multicast Ad hoc On-demand Vector with Backup Branches), which improves stoutness of the MAODV protocol by combining advantages of the tree structure and the mesh structure

Keywords : MANET'S, Routing Algorithm, Backup Branches, Tree Structure, Mesh Structure.

I. INTRODUCTION

Mobile ad hoc networks(MANETs) are self-organizing wireless networks short of any fixed set-up and centralized management. All the nodes move randomly, which communicate with each other from end to end multi-hop wireless links. If two mobile nodes are not within radio range, the communication between them can be established through one or more intermediate nodes. Multicast is an efficient way to convey packets from one point or multi-points to multi-points, which can reduce the depletions of network bandwidth and host power by directing the same data to numerous recipients. Consequently, multicasting plays an important role for statement in MANETs, where group tasks are often de-ployed.

II. METHODS AND MATERIAL

1. MAODV Protocol Introduction

MAODV is an on-demand routing protocol based on distance vector, which is indorsed by IETF MANET. In this section, we initially give a transitory narrative of route mechanism in MAODV and then converse the impact of network capacity on the MAODV protocol.

Route Mechanism

MAODV is a routing protocol deliberate chiefly for ad hoc networks. In addition to unicast routing, MAODV backings multicast and broadcast as well. MAODV protocol figures a joint delivery tree to sustenance multiple senders and receivers in a multicast session. The route mechanism in MAODV chiefly involves of route formations and route maintenances.

As a tree-based multicast routing protocol, MAODV relies on submerging through the whole network to realize the routing path and create the multicast tree. When a source node requests to join a multicast group or has data to refer to the multicast cluster, it will broadcast a route request (RREQ) message. In-between nodes establish reverse route and forward the RREQ message. After getting a RREQ message, the members of multicast cluster answer a route reply (RREP) message to setup a frontward path. If the source node accepts one or more RREP messages from the terminus nodes before timeout, it chooses one of the routes with the largest sequence number and the lowest hop count. Then it activates the route by unicasting a multicast activation (MACT) message to the next hop and starts to direct multicast data packets.

In MAODV, when an on-tree node perceives a link broken, it will start the route regaining instantaneously. Firstly, it needs to govern whether the cracked link is upstream or not. If it is, the node will delete the upstream node in its next-hop list, drop multicast data packets which should be sent and then send RREQ message with the flag J to recreate anew tree branch. Otherwise, the node will obliterate the downstream node in its next-hop list and formerly set pruning timer.

Impact of Network Load on the MAODV Protocol

In light load ad hoc networks, the above contrivance of multicast route regaining is effective. Because most applications allow a lesser amount of packets lost earlier the multicast route retrieval is completed. However, when the network is highly loaded, huge number of packets will be discarded and poor toughness of the tree-based protocols appears. Therefore, only dependent on the original route maintenance in MAODV cannot ensure the network performance.

Improvement of Multicast Routing

To overwhelmed the impact of network load and improve robustness of the MAODV protocol, we cover MAODV protocol to build a multicast tree with backup branches from two pieces. One is the process of backup branches variety and addition, the other is the mechanism of multicast tree maintenance.

Grph Message Expansion

In MAODV, the cluster leader at times broadcasts GRPH messages to keep posted or keep the multicast group information. In order to select and add backup branches correctly, we cover original GRPH (Group-hello) messages with the amount of active downstream branches in MAODVBB (Backup Branches).

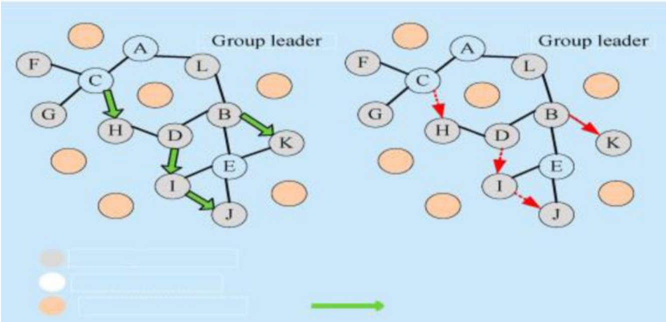
In our testing, we set an upper limit with the rate of three. In practice, when the number of downstream branches is higher than the upper limit, the presentation of protocols will not be developed further

Backup Branches Selection and Addition

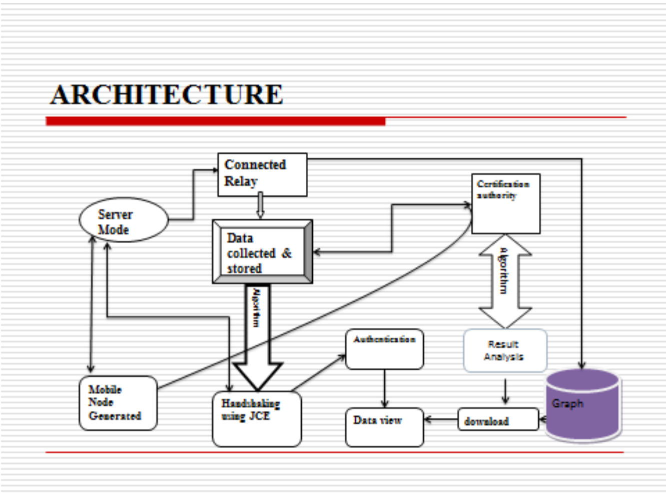
In MAODV protocol, when an on-tree node initially takes a GRPH message with the matching multicast group leader address and multicast group address, it keep posted the multicast group information in its group leader table and multicast routing table. Usually, the GRPH message is identified as the multicast group leader address and the multicast group address. We enlarge one backup routing table for each on-tree node to save the information of its backup tree branch in MAODV-BB. In order to accomplish the improvement, the task after receiving a GRPH message is modified as followed:

a. lf it is the initial time for the on-tree node to get the GRPH message, then turn to b), otherwise discard the GRPH message;
b. Determine whether the GRPH message is received from its upstream node or not. If it is, the node desires to achieve the same task as MAODV, otherwise turn to c);
c. If the hop to the group leader in the GRPH message is less than that in multicast routing table and the amount of dynamic downstream branches is lower than the limit, then update the tree branch, otherwise tum to d);
d. Judge whether there is a offered backup branch or not. If there is, try to e), else add a new backup branch in the backup routing table;
e. If the hop to the cluster leader in the GRPH message is a lesser quantity of than that in the backup routing table, then keep posted its backup branch, else abandon the GRPH message.

Node K initially receives a GRPH message from node B and then defines that the hop to the group leader in the GRPH message is fewer than that in multicast routing table. Node K updates the tinier tree branch and exchanges node E with node B as the fresh upstream node. The littler tree branches can reduce control traffic and average delay. Furthermore, node H, node I and node J disjointedly add backup branches in their backup routing tables. Lacking damaging the tree structure, the addition of backup branches improves stoutness of the network and certifies the network performance.



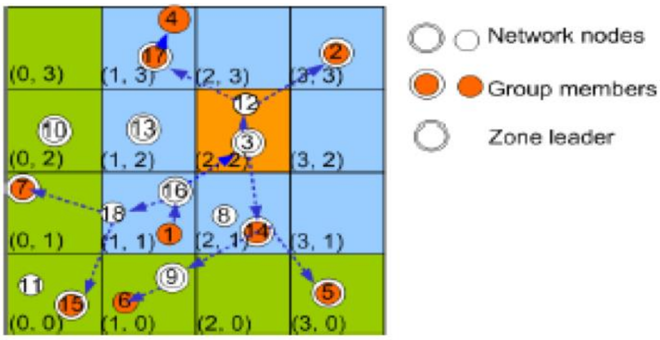
2. Architecture Diagram



First of all, a Mobile node is generated to initiate the process. a connection is creating between the created mobile node and the server mode. When the mobile node is created, it is verified by using Certification authority. Server mode establish a connection with connected relay. The data which are going to send through this network is stored in Data Collected and Stored. Then Handshaking using JCE algorithm is used to secure the data stored. Then the authentication process taken place. The data is viewed using Data View. For Additional security purpose the data control access is given to a certification authority. Then using Randomized Algorithm to view the Analysis of the Result. The Final output is generated by using Connected Relay in the form of Graph. After all the connections are made and verified using certification authority the data can be downloaded.

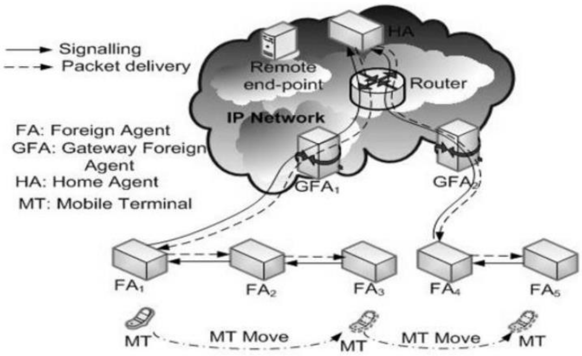
3. List of Modules

A. Mobile Relay



- Relay nodes do not transport data.
- decrease the transmission costs.
- Optimal solution , moving is beneficial

B. SINK



- Point of contact
- Translates the question into multiple queries

C. Tree Optimization

- Sub problem of finding the optimal positions of relay nodes.
- Fixed topology.

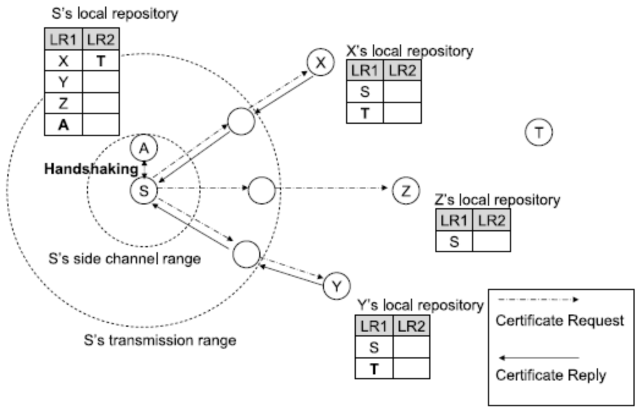
D. Attack While Data Transfer

- Zone structure
- Member node

E. Node Assumption

- Two local certificate repositories (LR1 and LR2) and stores acquired certificates in the repositories.
- All nodes share the same secure hash function Hash (), digital signature generation Sign () and verification Sign Ver () functions.
- Each node has its own public/private key pairs.

4. Running Proposed System



5. Algorithm

begin

1) $u \rightarrow v$: $ID_u|pub_u$;
2) $v \rightarrow u$: $ID_v|pub_v$;
3) u: verify ID_v and derive r_v = Hash($ID_v|pub_v$);
   v: verify ID_u and derive r_u = Hash($ID_u|pub_u$);
4) $u \rightarrow v$: σ_u = Sign($ID_u|ID_v, prv_u$);
5) $v \rightarrow u$: σ_v = Sign($ID_v|ID_u, prv_v$);
6) u: check SignVer($ID_v|ID_u, \sigma_v, pub_v$) = 1;
   v: check SignVer($ID_u|ID_v, \sigma_u, pub_u$) = 1;
7) u: generate $Cert_v = r_v|ID_v|ID_u|pub_v|\sigma'_u$ and store $Cert_v$ in LR1 repository;
   (σ'_u = Sign($r_v|ID_v|ID_u|pub_v, prv_u$))
   v: generate $Cert_u = r_u|ID_u|ID_v|pub_u|\sigma'_v$ and store $Cert_u$ in LR1 repository;
   (σ'_v = Sign($r_u|ID_u|ID_v|pub_u, prv_v$))

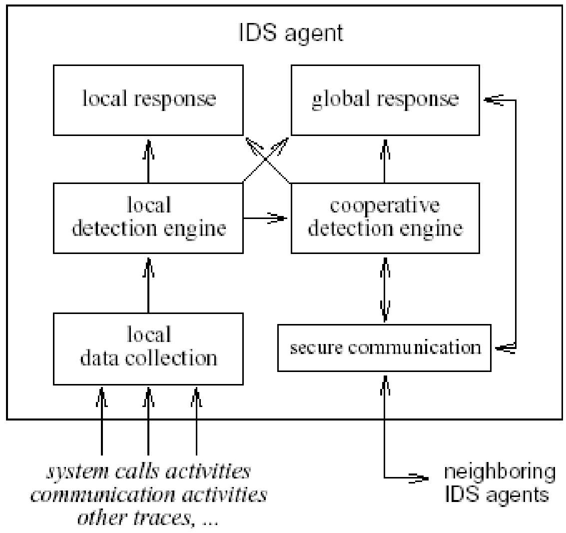
end

III. RESULTS AND DISCUSSION

1. Algorithm Explanation

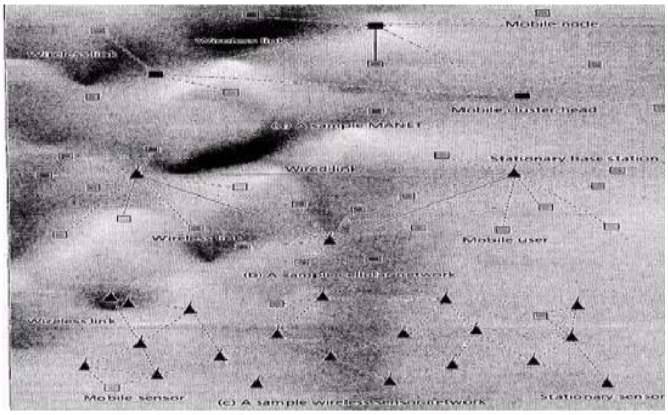
- Distributor gets 'S' request or 'R' from agent, gives requested data to agents.
- Distributor creates fake object
- Create a six-digit fake object- first two digits are the random Number and the next four digits specify the agent identity. Distributor checks the agents, who have received data.
- Leaked file-distributor compares the Leaked tuple, which contains allocated data for every agent. Then he Identifies the target.
- unique fake objects.
- Estimate the probability value for guilt agent.

2. Algorithm Works



3. Existing System

- many challenges
- traditional mechanisms



Disadvantage

- Single sensor.
- Redundancy.
- More time.
- High Cost.

4. Proposed System

- Mobile relays-Low – cost
- reduce energy consumption.
- Lows-cost
- mobile sinks or data-reduce communication delays

Advantages

- Launches only passive attacks.
- Attempts to observe.
- Threat can be countered by encrypting the packets.

IV. CONCLUSION

Data Server has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Data Server is the result of the evolution and adoption of existing technologies and paradigms. The goal of Data Server is to allow users to take benefit from all of these technologies. Data Server generally, and SaaS in particular, is a rapidly growing method of delivering technology. The Server distribution and optimization techniques resulted the definition of the minimal manageable IOT Server that is capable of updating and configuring its IOT machine. The result reveals that the introduced technique significantly decrease the deployment time of IOT Server is based on the deployment systems.

V. REFERENCES

[1]. Internet Engineering Task Force (IETF), Mobile Ad H oc Networks (MANET) Working Group Charter 2006, http://www.ietf.org/html.charters/ manet-charter.html.

[2]. Conti M, Giordano S. Multihop Ad hoc networking: the theoryJ. IEEE Communications Magazine, 2007, 45 (4): 78-86.

[3]. Luo Junhai, Ve Danxia, Xue Liu and Fan Mingyu, "A survey of multicastrouting protocols for mobile ad-hoc networks," IEEE Communications Surveys & Tutorials, vol. 11, no. 1, pp. 78-91, 2009.

[4]. Soni S.K. and Aseri T.Ci, "A review of current multicast routing protocol of mobile ad hoc network," in Proc. Second Int. Conf. Computer Modeling and Simulation ICCMS' 10, vol. 3, pp.207-211, 2010.

[5]. K. Viswanath, K. Obraczka, and G. Tsudik, "Exploring mesh and tree based multicast routingprotocols for manets," vol. 5, no. 1, pp. 28-42,2006.

[6]. E. M. Royer and C. E. Perkins, "Multicast ad hoc on-demand distance vector (maodv) routing," draft-ietf-manet-maodv-OO.txt, 2000.

[7]. W. S. Vunjung Vi Sung-Ju Le and M. Gerla, " On-demand multicast routing protocol (odmrp) for ad hoc networks," draft-ietf-manet-odmrp-04.txt, 2002.

[8]. Hua Chen, Zhengxiang. Van, Baolin Sun, Vue Zeng, Xianying He, An Entropy-Based Longlife Multicast Routing Protocol in MAODV.2009 ISECS International Colloquium on Computing, Communication, Control, and Management, 2009, Page(s): 314 -317.

[9]. Mingyang Zhong, Vunqing Fu, Xinqiang Jia. "MAODV multicast routing protocol based on node mobility prediction ", E -Business and E -Government (ICEE), 2011 International Conference, June, 2011.

[10]. Baolin Sun, Hua Chen, and Layuan Li, "A Reliable Multicast Routing Protocol in Mobile Ad Hoc Networks", In Proceedings of the 16th International Conference on Computer Communication (ICCC2004), Beijing, China, September, 2004, pp. 1123-1129.

[11]. CheeOnn Chow, Hiroshi Ishii. Video multicast over mobile ad hoc networks: Multiple-Tree Multicast Ad Hoc On-demand Distance Vector Routing Protocol (MT -MAODV). The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile R adio Communications (PIMRC07). Sept. 2007.

[12]. Hong Tang, Fei Xue, Peng Huang. MP-MAODV: a MAODV-Based Multi-path Routing Algorithm. IFIP International Conference on Network and Parallel Computing. 2008 , Page(s): 296- 301.

[13]. Xiaohua Chen, Qiu Zhong, Danpu Liu, An Improved MAODV Based on Mobility Prediction and Self-pruning Flooding, In Proceedings of IEEEICCMC -2009, China, Jan, 2009, pp.127 -131.

[14]. The Network Simulator - NS-2: http://www.isi.edu/ nsnam/ns.