Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

e-EPSAR: Enhanced Efficient Power Saving Adaptive Routing Algorithm for Mobile Ad-hoc Networks

Gaurav Banga
ECE Department, ISTK,
Kurukshetra University
Kurukshetra, Haryana, INDIA

Shakti Kumar
ECE Department, ISTK,
Kurukshetra University
Kurukshetra, Haryana, INDIA

Amar Singh
CSE Department, ISTK,
Kurukshetra University
Kurukshetra, Haryana, INDIA

Abstract- Mobile ad-hoc networks (MANETS) are formed by a set of mobile nodes that have the ability to make a communication network without help of any fixed infrastructure. due to the character of these networks, routing protocols play a distinguished role in their measurability and overall performance. because of restricted radio transmission range, multiple hops is also needed so as to exchange information among the act nodes. So, a key demand of any efficient routing protocol is to seek out a route between 2 communicating nodes quickly and with low bandwidth overheads, reliability play major role on selection of a node for packet forwarding. in this paper we have a tendency to projected a brand new approach to for the selection method of next node. The projected algorithmic rule is novel, as a result it selects the next node which is farthest, reliable and efficient when both source and destination nodes are present in same cluster but for inter cluster communication it uses clusters heads to make path at the same time with minimum computation requirement.

Keywords-- MANETS, e-EPSAR, Clustered Based Routing, Efficient Routing, Reliable Path Selection Algorithm.

I. Introduction

Wireless network is a growing new technology and has replaced approximately all wired network due to its heavy advantages. Wireless Networks are classified in two classes - infrastructure network and infrastructure less (ad-hoc) networks. In these, the ad-hoc networks works without any pre-existing infrastructure. They are easy to deploy and set up at any place and time, hence it has decreased the dependence of the infrastructure. So ad-hoc networks became a very important technique these days because of its features. Quality of service is the ability to assign different priority to different applications, users, or information flows, or to ensure a certain level of performance to a data flow. Routing is the main constraint within the working with ad-hoc network. Routing is the integral part of any kind of the network as it not only exchanges the data but also control the information in the form of packets with its respective connected nodes in its range. There are varieties of routing protocols available in the area of the mobile ad-hoc networks. Due to the popularity of these networks, it is important to improve the quality of service for these networks. There are many parameters on which the quality of service depends. With rapid development of wireless technology, the Mobile Ad Hoc Network (MANET) has emerged as a new type of wireless network. MANET is a group of wireless mobile nodes (e.g. laptops) that dynamically function as a network without the use of any existing infrastructure and centralized administration. In MANETs each node operates not only as an end system but also as a router to forward packets for other nodes. [11], [12], [13], [18]

Since the nodes in MANET move around, the connections between them break and re-establish frequently. Most of mobile nodes are having limited resource in computing capability and battery power. In order to work with MANETs there are some predefined routing strategies through which we can pursue our communication i.e. active routing (on demand), proactive routing (table driven). Rest of these there is one more routing strategy known as pre-emptive routing (works on the bases of signal strength and age of path) all these strategies have their own pros and cons. All these protocols have some wonderful features if we intermix the selected features, particularly offer additional stress on signal strength that acts as threshold and distance to define inter/intra cluster communication. We could found a routing path that is extremely efficient in terms of power conservation. [14], [15], [17]

II. Previous Work

[1] A certificate based protocol named ARAN is proposed to reduce security threats to AODV and DSR and avoid all identified attacks.

[2] A new protocol MOCA (mobile certificate authority) based on PKI (public key infrastructure) and CA (certificate authority) proposed for efficient communication.

[3] For multi-hop network a new mobile intrusion detection system (MIDS) is proposed, which efficiently detect the misbehaviour, packet drop and delay by appointing a special node (monitor) in the network.

[4] An integrated network architecture is designed for multiple MANETs accessing cellular IP and an integration routing protocol to connect cellular IP to MANETs is also proposed.

[5] Briefly discuss the MANETs functionality and beautifully listing the architecture and limitation of MANETs for the past decade.
[6] An efficient power saving protocol (p-MANET) is proposed to reduce the power consumption and transmission latency by offering new foundation (MAC) layer power saving protocol.
[7] A novel algorithm is proposed for selecting best neighbour node in multicast MANETs named BNNSA (best neighbour node selection algorithm).
[8] An excellent, multicast efficient routing protocol named MOMENTAP is proposed.
[9] A new algorithm (FRENSA) is designed for next node selection to enhances the quality of next node selection method for MANETs.
[10] An new version of FRENSA, efficient power saving adaptive routing protocol (EPSAR) is proposed to reduce the overheads.

In this paper a new algorithm is designed for next node selection to enhances the performance of MANETs. For packet forwarding the proposed algorithm select the next node with respect to its distance from sender node, power backup and reliability for intra cluster communications and for inter cluster communication data packets sent through cluster heads, which reduces the overall communication head and improves the reliability of communication.

III. Proposed Work

Before elaborating the proposed algorithm first discuss some pre-required arrangements / Processes. Network manages some tables and formats in the process of selecting next node.

A Cluster Head Awareness Table

Cluster heads maintains a table with current time stamp; this table contains the information about the member nodes of their clusters collected from Hello_request packets received from nodes present in the specified area of that cluster and information about other neighbour cluster heads collected from Hello_request packets received from cluster heads present in the outside area of that cluster.

ID	Node Status
192. 168. 0. 5	Member
192. 168. 1. 4	Member
192. 168. 1. 7	C.Head
192. 167. 1. 6	Member
192. 158. 2. 8	Member
192. 168. 4. 7	Member
192. 168. 7. 5	Member
192. 168. 6. 9	C.Head
192. 148. 3. 1	C.Head

Table 1. Shows the CHATts

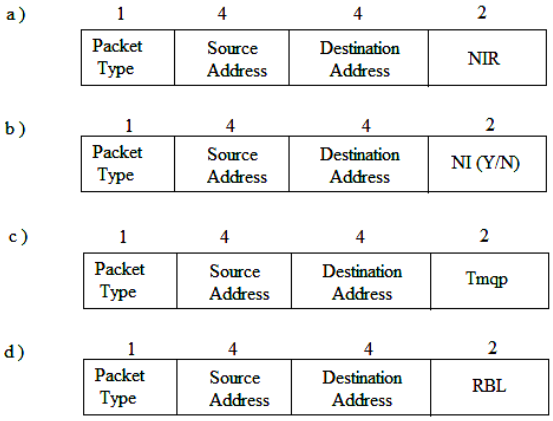

Fig.1: Shows the packet header of a) beacon_request1 packet, b) beacon_reply1 packet, c) beacon_request2 packet, d) beacon_reply2 packet.

B. Beacons call

In MANETs whenever a node wants to communicate it first release a beacon_ request packet to all the nodes within its radio range and the recipients reply with a beacon_reply packet. Here initially In beacon _request1 packet with source and destination address additional NIR field (node information required field) is sanded to their cluster head which demands the cluster head to supply the required information (first time it demands to supply the information that weather the destination node is present in their cluster on not) and beacon_reply1 packet reply with the NI field (Y/N: e.g. yes or not) to show the source node and destination node are in same cluster or not. Then beacon_request2 packet is broadcast by source node to all the nodes within their radio range with source address, destination address and additional Tmqp (Threshold minimum qualifying power) is sanded which demands to supply the remaining battery duration of the nodes that are having RBL > = Tmqp and beacon_reply2 packet reply with the RBL field (remaining battery life, e.g. in seconds) to show the remaining time of charged battery of the node.

C. Network awareness Table

Sender node maintains a network awareness table within their cluster with current timestamps; this table contains the information about the neighbor nodes collected from beacon_reply2 packet. The nodes are arranged in the decreasing order of their distance from the sender node (distance is estimated by the signal strength of beacon_reply2 packet). Generally weakest the signal means farthest the distance. For each communication the sender node defines Threshold

minimum qualifying power value (Tmqp) depends on the length of the transmitting data and communication duration required. Sender node defines the value of the Tmqp, means the next node (selection) battery power should be higher than defined Threshold minimum qualifying power value (Tmqp). The NATts table enrols only that nodes having RBL > =Tmqp .

Table 2. Shows the NATts format (Ports number are arranged in decreasing in distance from sender node)

Table 2. Shows the NAT

Neighbour Node ID	Port Number	RBL (In Seconds)
192. 168. 1. 272	2001	427
192. 168. 1. 239	2002	702
192. 168. 1. 213	2003	1210
192. 168. 1. 187	2004	912
192. 168. 1. 155	2005	227

D. RnR Table

A reliable/unreliable table (RnR) is maintained, which is having the list of reliable and unreliable mobile nodes with their IP address and port number. When a node experience multicast, multi-hop communication the behavior of node travels during packet transmission is reported in RnR table. The reliable node information is recorded in R column and information about unreliable is stored in nR column which is further communicated to the nodes of its multicast group.[9]

Table 3 shows the format of RnR

R (Reliable Node)		nR (Unreliable Node)	
ID	Port Number	ID	Port Number
192. 168. 0. 5	1102	192. 164. 7. 33	1279
192. 168. 1. 4	3214	188. 165. 3. 57	2621
192. 168. 1. 7	1456		
192. 167. 1. 6	1654		

E. CVP (certificate verification packet)

For a node (not found in RnR table) a special packet is transmitted to the node for providing the off line verification certificate and the new node supplies the verification certificate generated by its parent node. This certificate provides the guaranty of geniuses and reliability of that node and RnR table is updated with the new node. Otherwise two cases are formed in case-a when node generates a unreliable proof, that node is enrolled in nR column of RnR table and in case-b when node fails to provide certificate/ timeout, for both the cases the current node is left and the next highest node from NATts table is selected to check the reliability. [9], [10]

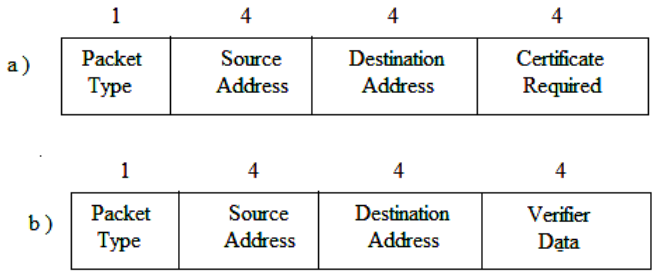

Fig.2: a) shows the format of certificate verification packet and b) shows the certificate verifier packet.

F. Data seen table (DST)

Each node maintains a DST which contains the log of packet forwarded. It reduces the duplicate packet forwarding because when a node receives a packet it check the information to its DST if information is found then it discard the packet otherwise information is inserted to DST and packet is forwarded. [9]

Table. 4 shows the format of DST

Packet ID	Multicast ID	Source ID

IV. Enhanced Efficient Power Saving Adaptive Routing (e-Epsar) : The Proposed Algorithm

A new approach is proposed which selects the reliable and efficient node for packet forwarding. Firstly it has been checked that both source and destination node are in same cluster or not, if both are in same cluster (Intra cluster communication) then table of neighbor nodes within that cluster is arranged with respect to their distance from the sender node. The nodes having less remaining battery life then Threshold minimum qualifying power value (Tmqp) are not the part of NAT. Then select the highest node and search it from RnR table to check its reliability if the node is in R column of RnR table then that is next node for forwarding the packet (Reliable and Efficient Node is Selected) and if the node is listed with nR column that means that is an unreliable node we cannot trust on this node so leave that node and select the second highest node from NAT table and check out its reliability from RnR table. If the node does found in RnR table then off line certification is demanded to its parent node/multicast group by sending CVP (certificate verification packet). If source and destination node are in different clusters (Inter cluster communication) then data is passed to the source node's cluster head and source node's cluster head send that data to destination node's cluster head and after reception of data by cluster head of destination node it act as source and send data to destination node (After reception of data at destination node's cluster head communication will take place as intra cluster communication)

A. Cluster Head Awareness Table (time stamp) Maintenance Algorithm

Input // Hello_request packet received //
Output // Generating cluster head awareness table CHATts with node status //

Hello_request packet received with IP address and node status

1. Received Hello_request packet with IP and node status

2. If (IP && node status ! = CHATts)

3. Then insert IP, Node status in CHATts

4. Else
   Leave that packet
   Select next hello_request packet
   go to 1.

B. Network Awareness Table (time-stamp) Maintenance Algorithm

Input // Beacon_reply2 Packet Received //
Output // Generating network awareness table NATts with port number (Max to min in distance from sender node) //

Beacon_reply2 packet received with IP address and Port number

1. Received beacon_reply packet with IP and Port number

2. If (IP && Port number ! = NATts)

3. Then insert IP, Port number in NATts
   And
   Arrange Port number's in descending distance order

4. Else
   Leave that packet
   Select next beacon_reply2 packet
   go to 1.

C. Reliable/Unreliable Table Maintenance Algorithm (RnR)

Input // Node selected from NATts table //
Output // Update for reliability/unreliability in RnR table //

1. Set i = Top of NATts

2. Check RnR

3. If
   i found in R column
   Then
   Reply with " The respective Node is Reliable"
4. If
   i found in nR column
   Then
   Reply with " The respective Node is Unreliable"
   & go to 1, & i++
5. If
   i not found in RnR table or time out
   Then "Call to parent node for offline verification certificate"

6. If it provide unreliable certificate / Timeout
   Then go to 4.
7. If
   Gives reliable certificate, update RnR
8. Stop

D. Enhanced Efficient Power Saving Adaptive Routing Protocol (e-EPSAR)

The actual mechanism of e-EPSAR as follows:

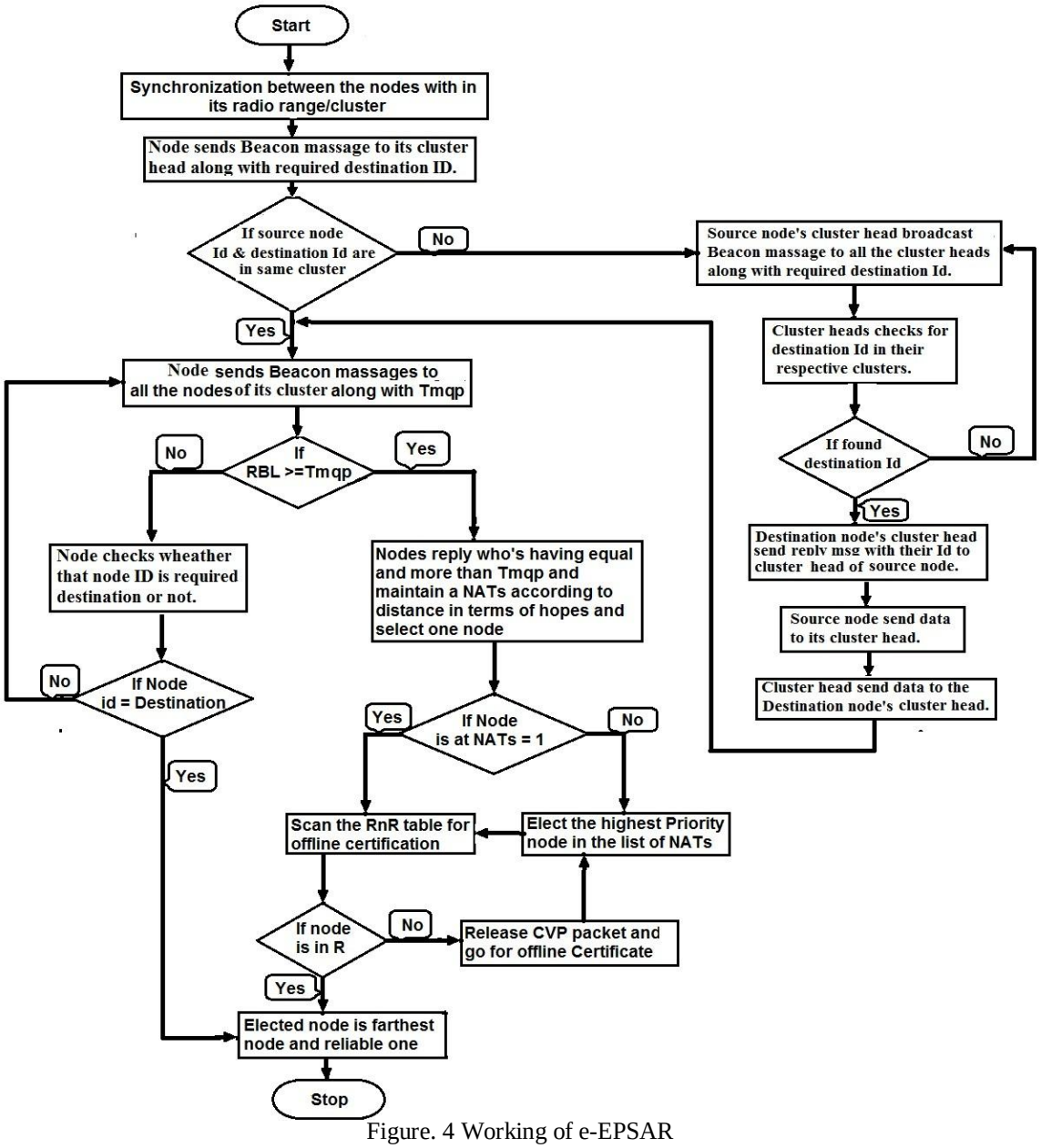

Figure. 4 Working of e-EPSAR

V. Conclusion

Reduction on overall communication head, selecting best reliable node for packet forwarding low power consumption and less processing always challenge the performance of Mobile ad hoc networks. The proposed e-EPSAR (Enhanced Efficient Power Saving Adaptive Routing) algorithm selects the node which can efficient enough and reliable in behavior directly when there is intra cluster communication required. For inter cluster communication cluster heads are used as clustering increases the system capacity; it does in the way that the information is stored once on the cluster head, which facilitates the spatial reuse of resources. Efficient characteristics nature may reduce the dynamic nature of routing (fast communication) and reliable node selection may provide a good quality of service (QoS) and after the topological changes, the cluster structure helps in decreasing the transmission overhead incurred for the updating of routing tables.

References

[1] Kimaya sanzgiri, Bridget dahill, Brain neil Levine, Clay Shields and Elizbeth M.Belding-Royer "A secure routing protocol for AdHoc Networks" Proceedings of 10th IEEE International Conference on Network Protocols (ICNP'02), 2002.

[2] Seung Yi, Robin Kravets "MOCA: Mobile Certificate Authority for Wireless AdHoc Networks" University of Illinois at Urbana-Champaign Urbana,IL61801, {seungyi,rhk}@ cs.uiuc .edu

[3] S.Madhavi, Tai Hoon Kim "An intrusion detection system in mobile adhoc networks" international journal of security and its applications vol.2 no.3, ju;y 2008.

[4] Fekri M.Abduljalil, Shrikant K. Bodhe "Integrated routing protocol (IRP) for integration of cellular IP and Mobile AdHoc Network" proceedings of the IEEE international conference on sensor networks, ubiquitous and trustworthy computing (SUTC'06) 2006.

[5] Marco Conti, Silvia Giordano "Multihop Ad-Hoc Networking:The theory" IEEE Communication magazine April 2007.

[6] Chiung-Ying Wang, Chi-Jen Wu, Guan Nan Chen & Ren- Hung Hwang "p-MANET : Efficient power saving protocol for multi-hop mobile ad-hoc networks" Proceedings of the third international conference on information technology and application(ICITA'05) 2005.

[7] A.K.Sharma and Amit Goel "Best Neighbor Node Selection Algorithm for MANET " journals of institution of engineers, Jan2005.

[8] A.K.Sharma,and Amit Goel "Moment to Momant Node Transition Awareness Protocol (MOMENTAP)" international journal of computer application (IJCA) special issue. IASTED, Vol.27/1 jan 2005.

[9] Priyanka, Komal Kumar Bhatia, Ajay Jangra "FRENSA: Farthest, Reliable and Efficient Node Selection Algorithm for Mobile Ad-hoc Networks (MANETs)" in IJCST International Journal of computer Science and Technology Vol. 1 Issue 2 December 2010

[10] Ajay Jangra, Nitin Goel, Chander Kant and Priyanka, "An Efficient Power Saving Adaptive Routing (EPSAR) Protocol for Mobile Ad Hoc Networks (MANETs)" © Springer-Verlag Berlin Heidelberg 2011, International Conference, HPAGC 2011, Pages. 638–646, July 2011.

[11] Gaurav Banga, Saranjeet Singh, Rakesh Kumar, Shrishtansh Pathak,"Quality of Service (QoS) on Queuing Disciplines", National Conference on Emerging Trends in Electronics & Communication Engineering, ETECE-11. April 2011.

[12] Gaurav Banga and Ankur Singhal, "Performance Evaluation of Queuing Principles", International Journal of Applied Engineering Research,Vol.6 No.18. Pages 2283-2287, November 2011.

[13] Sahil Gupta, Sunanda Arora, Gaurav Banga, "Simulation Based Performance Comparison of AODV and DSR Routing Protocols in MANETS", International Journal of Applied Engineering Research,Vol.7 No.11. Pages 2028-2031, November 2012.

[14] Ankur Gupta, Gaurav Banga, Saranjit Singh, "Effect of Variation in Packet Size on Throughput of Mobile Ad-hoc Network", GGGI Journal of Engineering & Technology,Vol.1 No.2. December 2012.

[15] Gaurav Banga, Shakti Kumar, Amar Singh "Impact of Node Density and Mobility on Reception of Packets for AODV Protocol in MANETS Using NS-2",Proceeding of IETE, ETECH-2013 August 23-24, 2013..

[16] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhanng, "Security on Mobile Ad Hoc Networks: Challenges and Solutions" 1536- 1284/04/IEEE Wireless Communications Feb., 2004

[17] C.Siva Ram Murthy & B.S Manoj, "Mobile Ad Hoc Networks- Architectures & Protocols", Pearson Education, New Delhi, 2004.

[18] http://www.routingprotokolle.de/Routing/routing_sbr.htm

