Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130514

Enhancing Network Duration by Secured Node Disjoint Clustering for Mobile Adhoc Network

K. Senthil Prakash[1,*] *and T. Guna Sekar*[2]

[1] Department of ECE, Velalar college of Engineering & Technology, Erode, Tamilnadu, India.
[2] Department of EEE, Kongu Engineering College, Erode, Tamilnadu, India.

Received: 26 May 2018, Revised: 20 Jul. 2018, Accepted: 20 Sep. 2018
Published online: 1 Sep. 2019

Abstract: Mobile Adhoc Networks (MANETs) are dynamic networks due to their node mobility and may be employed as multi-hop networks. Major research spotlight in data aggregation is directed towards conserving power. Additional research problems contain increasing the security level in data transmission and aggregation, managing tradeoffs in data aggregation i.e. tradeoffs among dissimilar objectives such as data accuracy, latency, improving quality of service in terms of throughput, end delay and power consumption. Security problems created by sensor networks constitute a big field for research issues like constructing routing protocols with inherent security aspects, cryptography technique for sensor networks, designing safe data aggregation protocols, designing intrusion finding method and multimedia sensors security. In this research work, Security-Enabled Cluster Head Node Disjoint Power Aware Clustering (SENDPAC) method is proposed to modernize MANET security aspects endlessly when forwarding information from source node to destination node.

Keywords: Node –disjoint, Power, Security, Clustering, MANET, Cluster Head

1 Introduction

In recent years, Mobile Adhoc Networks (MANETs) [1] has become one of the popular technology for low power wireless communication. In most of the MANET applications, a large number of sensor nodes are deployed to gather based on application domains. MANET can be deployed in various domains and applications such as health care, military surveillance industrial control, wild life monitoring, agriculture and environmental sensing, security [2], home automation etc. Fast growth in MANET has leaded to construct many new routing protocols [3]. All of these routing protocols considered QoS [4] as the ultimate objective in order to prolong the whole network lifetime. QoS has been defined as a set of service requirements to be fulfilled when transmitting a stream of data packets from one place to another. Currently developing routing protocols are focused to bring specific quality of service (QoS) requirements like throughput [5], packet loss, end-to-end delay, and energy [6]. The proposed research scheme should aim for one or more aspect of the following: minimizing the total energy spent in the network, minimizing the number of data retransmissions, maximizing the number of alive nodes over time or balancing the energy dissipation among the sensor nodes in the network, provision to discharge the exclusive failure nodes from the network.

2 Literature review

Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for wireless sensor networks with cluster-based manner implemented as an extensively-recognized and stylish clustering algorithm, by choosing the cluster heads in each round. LEACH is an accepted power proficient flexible clustering algorithm that shapes the clusters based on the obtained signal quality and uses the local cluster head as a router to reach the destination. While information transmission to the base station uses high power, each sensor node in a cluster get turns with the transmission by revolving the cluster heads. This brings reasonable power consumption of all nodes, and extends the duration of the whole network.

Another well-known energy efficient clustering method is Hybrid Energy-Efficient and distributed

[*] Corresponding author e-mail: prasenrose@yahoo.co.in

(HEED) clustering method [7] for ad hoc network. HEED modified by Younis & Fahmy (2004) is a scattered clustering method which was recommended through four most important goals as follows:

1. Selecting highly - distributed cluster head and dense cluster
2. Concluding the clustering method inside a regular number of iterations
3. Reducing control overhead
4. Extending network duration by distributing power usage.

HEED occasionally chooses cluster heads based on a mixture of two clustering factors: The main factor is the remaining power of all sensor nodes and the secondary factor is the cost of intra- cluster communication as a role of neighbour nearness or cluster compactness. The main factor is implemented to probabilistically choose an early set of cluster heads as the secondary factor is implemented for breaking ties.

The Two-Phase geographical Greedy Forwarding (TPGF2) system constructs multiple node-disjoint paths to raise the node utilization. It does not accept face routing to avoid holes which construct it dissimilar to other techniques. Ni's On-demand geographic routing scheme (briefed as NI3) allows a source to forward information through two paths not including some routing details. The routing system is constructed with the concept that the sensor nodes are attentive of their location. It first situates a permanent rectangular prohibited region between the source and the sink, its breadth being two times the broadcast range and extent smaller than the remoteness among the source and the sink. It effectively unites two non-nosy paths, but the nodes in the paths are permanently arranged such that they cannot alter until a small number of nodes are lifeless.

Shiva Murthy et al (2012) suggested the secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) [8]. This protocol implements the various paths from source node to destination node according to minimum energy spending and the waiting line length of each node. It gives protection adjacent to the attacks similar to the sinkhole, and careful forwarding in wireless sensor networks [3]. This protocol offers high protection, implementing the digital signature crypto scheme that related the RSA algorithm and the MD5 hash function. They consider that use of nodes is arbitrary, and wireless sensor network is similar to an undirected graph.

3 Objectives of the proposed work

The main objectives of the proposed research work are

- To increase the network capacity by diminishing the path cost generated by path invention technique and path safe guarding methods.
- To increase the network lifetime [9] by distributing the traffic among multiple paths available in wireless sensor networks.
- To discover multiple cluster head node-disjoint paths between the source and the sink nodes.
- To obtain minimum end-to-end delay, minimum power requirement, high throughput and high PDR.

4 Proposed research work

The most important aim of this research is to inspect the power efficient methods for cluster-based mobile adhoc network. That power efficient method must try to reduce the total power used in the network, reduce the number of data transmissions, increase the number of living nodes and equate the power dissipation between the sensor nodes in the network. This research utilizes some methods such as power awareness, cluster head node disjoint clustering [10], Multi hop communication, discharging of failure nodes from the network with the purpose of increasing network security.

We propose SENDPAC with improved security, when forwarding information from transmitting node to receiving node. The key target of proposed SENDPAC algorithm is to search cluster head-based node-disjoint routes which are readily available [11] among transmitting node - receiving node pair to get a path with minimum routing cost. Following three different segments are implemented in this protocol to achieve this target.

(A) Path detection segment
(B) Path assortment segment
(C) Path safeguarding segment.

A. Path detection segment:

By certifying a routing table for the next-hop in the track of receiving node, a transmitting node is equipped to dispatch a bit of data. The data packet is transmitted to the next hop if any helpful entry for the receiving node is available in assigned routing table [12]. The path invention segment begins if there is no helpful entry for the receiving node. Following two types of control messages are used to construct routes to reach the receiving node:

(i) Route request messages
(ii) Route reply messages

In mobile adhoc network transmitting node sends the RREQ message to all available nodes. When receiving this RREQ message, all intermediate nodes ensures whether it is a copy of another message or original by checking all the entry in the seen table. The following two entries are recorded in this table:

1. Source IP address
2. RREQ flooding ID

It is considered as a copy of RREQ message if an entry is already specified in the seen table for the received RREQ.

SOURCE IP ADDRESS	FLOODING ID	SEEN FLAG
——	——	——

Fig. 1: SENDPAC Seen table structure

TYPE	R	A	RESERVED	PREFIX SIZE	HOP COUNT
DESTINATION IP ADDRESS					
DESTINATION SEQUENCE NUMBER					
SOURCE IP ADDRESS					
SOURCE SEQUENCE NUMBER					
BROADCASTING ID					

Fig. 2: SENDPAC RREP structure

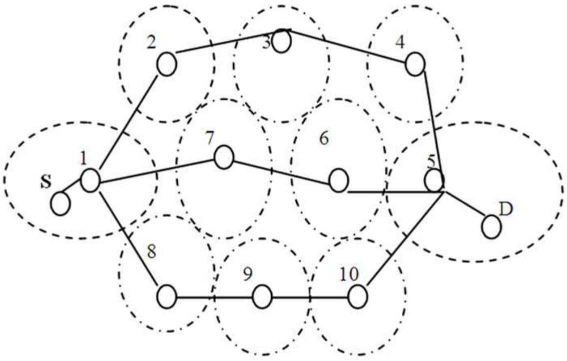

Fig. 3: Cluster head-based node-disjoint paths discovery Process

If not, this will be informed to its routing table earlier than transmitting the RREQ message. In this protocol, only the destination can transmit RREP based on reception of a RREQ. The intermediate cluster head nodes are not allowed to transmit RREPs when they comprise an active route to destination node. This is completed in order to obtain the cluster head node-disjoint routes. In SENDPAC, the destination must transmit RREP information for all RREQ messages already accepted, even if the RREQ message is a reproduction of another one.

At seen table, a newly added extra field shows the status of seen flag. This flag is fixed to FALSE at the initial stage, i.e. One separate broad cast ID is assigned for each RREP message by receiving node in SENDPAC method. To find out cluster head-based node-disjoint paths path discovery segment is executed. Receving node generates the RREP message when they obtain a RREQ. The receiving node generates the second copy of the flooding ID from the obtained RREQ message. This can be used as a new broadcast ID field of transmitted the RREP message. This unicast RREP message is forwarded in the direction of the originator of the RREQ by using reverse path. The receiving node completes this repeated task for each RREQ message obtained from every transmitting node. The seen flag status is verified by intermediate nodes in the back path to forward the RREP to the originator. This seen flag status in FALSE condition indicates the initial RREP on the back path in the direction to the transmitting node. Due to this condition, in-between nodes start to forward the RREP to the transmitting node and change the value of seen flag. According to seen flag status [13], the transmitting node rejects the RREP message as soon as the in-between node obtains a RREP for the same RREQ it received previously. Because of this rejection of duplicate RREP message, the in-between nodes can only join in any route from the available multiple paths to the destination.

B. Path assortment segment:

When a source node gets information packets to transmit and there is no existing route in routing table, the node starts the route invention method. Immediately source node initiates information broadcast and obtains the first route to reach the destination called as the primary route [14]. In the routing table inferior routes are recorded from all other cluster head node-disjoint routes. Any other path is not permitted in the routing table later than entering of primary route and few inferior routes. Other invented routes are put back as secondary paths when they contain lower hop count to reach the receiving node. In all time period this method is useful to select a suitable route for information broadcast. So, constant allotment of the primary route is available for data broadcast in the path assortment segment. Existing secondary paths with the minimum hop count [15] are used when the primary route is not energetic.

C. Path safeguarding segment:

A new route invention task like this can reduce the routing overhead due to finding and maintaining multiple paths. As in this case, one RREQ message is employed to discover all existing node disjoint routes as evaluated to one RREQ message needed for each route. In second route preservation technique, the source begins the route invention procedure immediately when it discovers that there is one active path left behind in the routing table. In this method, the source node gets routes to reach the destination node at any time. Delay induced by rerouting provision which is activated by a route smash [16] is strongly reduced by the implementation of path safeguarding segment. At the same time this constantly raises the overall network routing overhead.

5 Security provision in SENDPAC

The essential organization and previous association of the MANET is short, thus there is a variation in security concern than in predictable network. The MANETs are forced to extra risk of attacks by the wireless connections. For the intruders, it is easy to listen to the secret data and entering or leaving a wireless network is also easy since there is no necessary physical link. For fake packet insertion or taking off a node and removing communication, they can be able to openly hit the network. These break the aim of network of accessibility, reliability, certification, and non negation. In the future method, we provide safety to schemes at the same time the broadcasting of information from starting node to receiving node and also the connection breakdown may happen in middle of the link during the communication. In this system, consequently as the route detection with route detection stage and later than detection of the pathway, the intermediate distinctive node path is ready to allow the data. In this condition if the unexpected failure of connection happens in communication, the data is missing in the meantime earlier than reaching to the receiving node. In this condition, initially the primary path gets recovered or else from the backup table it moves to the secondary path as quickly as the basis gets damaged. The system protection is provided prior to move to an alternating path. The discharging of exclusive nodes does not take place in the existing work and there is a possibility to take away the data from the intermediate node to another network. This provision has been included in the proposed system to prevent data theft from the failure intermediate nodes and cluster heads. Thus an additional data security provision is achieved in the mobile adhoc network.

6 SENDPAC algorithm

This algorithm demonstrates the method used by a node subsequent to obtaining RREQ message from the transmitting node.It ensures its routing table for all available active routes to reach the information receiving node when a transmitting node has an information packet to transmit through the intermediate nodes. If an active route available, the information packet is transmitted to the next hop in the direction to reach the destination node. With this activity it makes an entry in information sent table. This is very useful to prevent re-sending of RREQ message before getting the RREP message from the intermediate nodes for the previously-transmitted RREQ message. Prior to transmitting the RREQ message, all nodes update its seen table to stop duplicating transmissions of the same data which increases the routing overhead. This algorithm verifies every node in the network whether the node is a transmitting node, cluster head intermediate node or receiving node when a RREQ is obtained. A RREP message will be transmitted from a receiving node when it gets the RREQ message, and it also takes the broadcast ID from received RREQ message. Handling of RREQ message from the transmitting node is in the identical way when it is obtained by a source node or cluster head intermediate node. Several routes are created by receiving node to give responses to all RREQ messages forwarded from several nodes in the network.

```
T = Transmitting Node
R = Receiving Node
T Address = IP Address of Transmitting Node
R Address = IP Address of Receiving Node
B id = route request message broadcast id
F id = route reply message flooding id
ICH= Intermediate cluster head Node
NN= Network Node
S flag = FALSE
n routes
X= FALSE //Seen flag status assigned in seen table
Count = 0
if T =1// Transmitting Node has data to send
if R=1 // Receiving Node has primary route
Initiate information broadcast ()
else
insert RREQ // Initiate route request
insert S() //Make an entry in seen table
start RREQ flodding ()//Flood the route request via all the nodes
if NN =1 // Any node in the network receives a RREQ message then
if $NN \equiv S \vee NN \equiv ICH$ then
X = check S ()
if X = 1 // duplicate route request messages are captured
discard ()
otherwise
relay()
else
if NN is the receiving node
B id =F id// When Broadcast ID =Flooding ID
initiate RREP ()
end if
```

This algorithm is implemented for route invention when a node obtains RREP to determine several cluster head node-disjoint routes. Type of the node is confirmed by obtained RREP message. Status of the seen flag is verified from seen table when RREP message is received by an intermediate node. The initial RREP message collected by a network node is pointed out by a FALSE status of seen flag. At this time, algorithm embraces this path as the primary path to transmit the information. Subsequently, this intermediate cluster head node transmits another RREP to the next hop node in the path of transmitting node. The path is considered as a secondary path when status of seen flag is set to TRUE.

```
if NN receives RREP
X = check () //verify the content of seen table
if NN /= S
relay () // Forward RREP message to the next hop node
insert primary ()
```

```
change () // To detect duplicate RREPs, reset the seen
flag
else
discard ()
else
X= confirm seen flag ()
if NN /= S
modify seen flag ()
add primary route()
else
Count = count ()
if Count ¡ n routes
add secondary route ()
discard RREP()
```

Additionally, this method provides the protection when the information is broadcast from source node to the destination node. An intermediate cluster head node is not released when path failure happens. These nodes have all information about the earlier transmission of the network. So these nodes are not released till removing of all data that it is previously restrained. Frequent link crash takes place due to random movement of all nodes including transmitting node with intermediate cluster head node and receiving node. Due to this, information protection is a critical problem in the MANET.

7 Simulation results and discussions:

The proposed method is simulated in network simulator (NS-2) and the performance is contrasted with recognized various routing protocols. Network testbed has been setup for different number of nodes within the restricted area of 1000 * 1000 m^2. In the different circumstance's performance metrics like PDR, end-to-end delay and control overhead ratio are evaluated for different multipath routing protocols. From the simulation results we can understand our proposed protocol SENDPAC gives less end-to-end delay, control overhead ratio and high PDR compared to other well-known routing protocols.

8 Conclusion

From the performance comparison results of various routing schemes, it can be concluded that the cluster head node disjoint-based multilevel hierarchical routing with security provisions for data aggregation has proven overall efficiency in various aspects. Future work may be focused on wireless energy transfer by means of diverse mechanisms like laser beam, piezoelectric principle, radio waves, microwaves, inductive coupling and electromagnetic resonance. Developing a combination of WSN-MANET will make possible cross network communication with small latency in various fields of IoT that can be considered as a future work. These integrated models will maintain heterogeneous networks and will develop the capacity and coverage of upcoming wireless

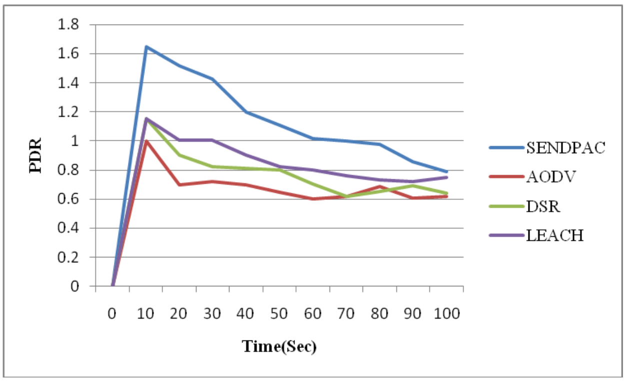

Fig. 4: Comparison of PDR variation between PAC, AODV, DSR and LEACH

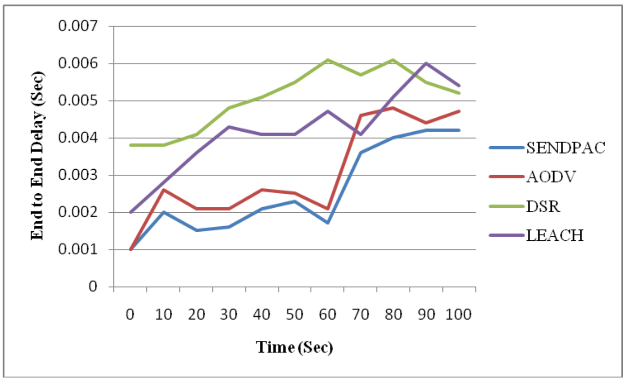

Fig. 5: Comparison of End to End delay variation between PAC, AODV, DSR and LEACH

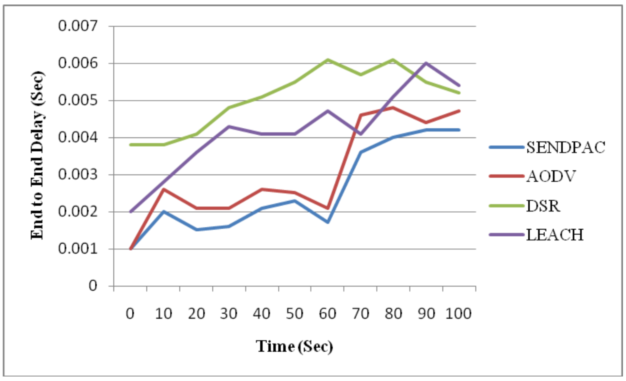

Fig. 6: Comparison of control overhead variation between PAC, AODV, DSR and LEACH

networks. Hence there is a wide scope for future research in the domain of mobile adhoc sensor networks.

References

[1] Baskaran.S, Arputha Vijaya Selvi .J & Sarma Dhulipala V. R, Trust Based Cluster-Energy Efficient Multicast Routing In Mobile Adhoc Networks, Applied Mathematics & Information Sciences, Vol.12, pp.421-429 (2017).

[2] Prasanna, S & Rao, S, An Overview of Wireless Sensor Networks Applications and Security, International Journal of Soft Computing and Engineering, Vol.2, pp.538-540 (2012).

[3] Hamdy H. El-Sayed, Shortest Paths Routing Problem in MANETs, Applied Mathematics & Information Sciences, Vol.10, pp.1885-1891 (2016).

[4] Rishiwal, V., Verma, S. and Bajpai, S.K., QoS Based Power Aware Routing in MANETs, International Journal of Computer Theory and Engineering, Vol.1, pp.47-54 (2009).

[5] Ramchand, V & Lobiyal, DK, Throughput Analysis of power control B-MAC protocol in WSN, International Journal of Wireless & Mobile Networks, Vol.4, pp.155-167 (2012).

[6] Heinzelman, W, Chandrakasan, A & Balakrishnan, H, Energy-Efficient Communication Protocols for Wireless Microsensor Networks, in Proc. Hawaii Conference on System Sciences, pp.584-598 (2000).

[7] Younis, O & Fahmy, S, HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks, IEEE Transactions on Mobile Computing, Vol.3, pp.366-379 (2004).

[8] Shiva Murthy G, Robert John D Souza & Golla Varaprasad, Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks, IEEE Sensors Journal, Vol.12, pp.941-2949 (2012).

[9] Ali Ahammed. G.F & Pavithra .N .S, Increasing Network Lifetime by Using SecureClustering With Reliable Node Disjoint Multi-path Routing in Wireless Sensor Networks, International Journal for Research in Applied Science & Engineering Technology, Vol.4, pp.401-407 (2016).

[10] Abhishek Bande and Mr. Gaurav Deshmukh, Node Disjoint Multipath Routing Approach for Controlling Congestion in MANETS, Global Journal of Computer Science and Technology Network, Web & Security, Vol.12, pp.39-45 (2012)

[11] Hoda Rafiee Pour, Marjan Kuchaki Rafsanjani & Hamid Saadat, A New Zone Disjoint Multi Path Routing Algorithm to Increase Fault-Tolerant in Mobile Ad Hoc Networks, Applied Mathematics & Information Sciences, Vol.9, pp.433-444 (2015).

[12] Lee, SH, Lee, S, Song, H & Lee, HS, Gradual Cluster Head Election for High Network Connectivity in Large-Scale Sensor Networks, in Proc. International Conference on Advanced Communication Technology, pp.168-172 (2011).

[13] Senthilprakash Kuppusamy and Mahendrakumar Subramani, Improving congestion control performance and fairness in multihop ad hoc network, International journal of Networking and Virtual Organisations, Vol.9, pp.86- 101 (2011).

[14] Senthil Prakash K and MahendraKumar S, Stable And Energy Efficient Routing For Mobile Ad-Hoc Networks Using Backbone Nodes, International Journal of Advanced Research in Computer Science, Vol.3, pp.303 -308 (2012).

[15] Senthil Prakash K and MahendraKumar S, Wireless Congestion Control Protocol For Multihop Ad Hoc Networks, International Journal of Computer Science and Information Security, Vol.7, pp.25 -31 (2010).

[16] Senthil Prakash K and MahendraKumar S, Congestion control performance and fairness in multihop ad hoc network, International Journal of Networking and Virtual Organisations, Vol.9, pp.86-101 (2011).

K. Senthil Prakash received his Bachelor degree in Electronics and Communication Engineering from Bharathidasan University, Tiruchirappalli in 2003 and his Master degree in Communication System from Kumaraguru College of Technology, Coimbatore in 2009. He is currently working in Velalar College of Engineering and Technology as a Associate Professor of Electronics and Communication Department since 2009.Currently he is pursuing Ph.D in Anna University ,Chennai. His area of interest includes mobile communication and ad hoc network. He has published 4 papers in International journals in the field of ad hoc networks. He is a Life Member of ISTE.

T. Guna Sekar received his B.E in Electrical and Electronics Engineering from Bharathair University, Coimbatore and M.E. in Power System Engineering from College of Engineering, Guindy, Anna University, Chennai, India. He has published 10 papers in International journals and conferences. His areas of interest include Power Systems, Power Quality Engineering, Active filters and Electrical Machines.