Security Enhanced Weighted Double Cluster Head based Routing Scheme for Efficient Routing in MANETs

S. Aruna, Dr. A. Subramani

Abstract— The primary objective of ad hoc network routing protocols is to construct an efficient route between source and destination nodes, with the intention that the messages may be delivered on time without any delay. Therefore, route construction must be done with less routing overhead and bandwidth consumption. One way to reduce routing control traffic is to divide the network into clusters. In most MANET clustering protocols, the leader node (cluster head) acquire on a special role in managing routing information. Due to highly mobility, the cluster head may move often, that leads to frequent re-clustering. This in turn, agitates the stability of the whole network. To enhance the network stability and bandwidth consumption, we introduce a new cluster-head election scheme to reform the cluster. This scheme is based on providing an alternative clusterhead (SCH) for each primary clusterhead (PCH). This SCH is an ordinary member node, which is identified and elected by its PCH to be the future leader of the cluster. When the PCH is no longer being a cluster head, the SCH will be triggered to be the PCH, by the former PCH. Since the SCH is known by all member nodes, the cluster leadership is transferred efficiently without affecting the performance of the network. Also, our proposed protocol (SD-CBRP) aims at improving quality of service with security. The performance of the proposed scheme is evaluated with NS2 simulator and shows better performance in terms of the packet delivery ratio, throughput and delay when compared to a weighted cluster based protocol (CBPMD).

Index Terms— MANET, Primary cluster head (PCH), Secondary cluster head (SCH), Stability, Security.

1 INTRODUCTION

THERE are two types of wireless networks: Infrastructured networks, and Infrastructure less networks. Infrastructured networks are referred to as "managed" wireless networks, as it consists of one or more access points (known as gateways or wireless routers) connected to the network. Ad hoc wireless networks are also referred to as "unmanaged" wireless networks, as it consists of each device connecting directly to each other. That is , its a decentralized type of wireless network.

The types of ad hoc networks are as follows: Mobile ad hoc networks (MANETs), vehicular ad hoc networks (VANETs), Internet based mobile ad hoc networks (iMANETs), Intelligent vehicular ad hoc networks (InVANETs). [1]

MANETs has no fixed routers; all nodes are capable of movement and can be connected dynamically in an arbitrary manner. Nodes of these networks function not only as an end system, but also as a router to discover and maintain routes to other nodes in the network. Example applications of mobile ad-hoc networks are: emergency search-and-rescue operations, Conventional meetings in which persons wish to share information, and data acquisition operations on inhospitable environment.

Due to the limitations of power, transmission range and node mobility, path failures are very frequent in this type of networks. To accommodate frequent path failures, special routing protocols are necessary [4].

Routing Protocols in MANET can be broadly classified as proactive, reactive, and hybrid. In proactive or table-driven protocols, each node maintains a routing table, containing routing information on reaching every other node in the network. All the nodes update these tables so as to maintain a consistent and up-to-date view of the network. DSDV (Destination-Sequenced Distance Vector), is one of the popular proactive routing protocols.

In reactive or on-demand routing, all up-to-date routes are not maintained at every node. Instead, the routes are created as and when needed. When source wants to send data to the destination, it invokes a route discovery mechanism to find the path to the destination. DSR (Dynamic Source Routing), AODV (Ad hoc On-Demand Distance Vector Routing), are some of the popular reactive routing protocols.

Hybrid protocols combine the benefits of both proactive and reactive routing and overcome their shortcomings. Normally, hybrid routing protocols for MANETs exploit hierarchical network architecture. That is, proactive and reactive routing approaches are exploited in different hierarchical levels, respectively [4]. That is, if the mobile nodes in MANET are assigned different roles and functionalities, the network topology is said to be hierarchical.

In cluster-based hierarchical routing, nodes are hierarchically organized into clusters or groups based on their relative proximity to one another. It greatly increases the scalability of routing in ad hoc networks by increasing the robustness of routes. Example: Cluster Gateway Switch Routing (CGSR) [5].

1.1 Applications of MANET

With the increase of portable devices, ad hoc network is gaining its importance with large number of widespread applications. They include:

- Military battlefield: Military equipments now a days routinely contain some sort of wireless equipments. Ad hoc networking can be effectively used in military to maintain information between soldiers, their vehicles and with their head quaters.
- Commercial sectors: ad hoc networks can be used in emergency rescue operations for disaster relief efforts. For example, fire, flood or earth quake etc.,
- Social sectors: ad hoc network can be used with laptop computers or palmtop computer to share the information among others academic environments like virtual classrooms, virtual conferencing, etc., and other civilian environments like sports stadium, taxicob, and aircrafts and many more.

1.2 Objectives of clustering in MANET

Clustering technique is one of the most important techniques that help to provide resource management in MANET [6]. In this technique, the nodes in the network can be either grouped into a number of overlapping or dis-joint clusters. The cluster-based MANET defines three types of nodes as shown below:

1. Cluster head (CH): It acts as a coordinator within its group or cluster.
2. Cluster member: It is ordinary nodes that communicate only with its CH.
3. Gateway node: It is a node that is within the transmission range of more than one cluster [7].

1.3 Problem Definition

One of the key challenges of a cluster based routing protocol is the appointment of a proficient cluster head. The cluster head can be elected either by considering single performance metric or multiple performance metrics. Multiple metrics based clustering schemes performs better than single metric based clustering scheme hence it takes multiple parameters such as node's degree, mobility, energy, bandwidth, etc. Therefore, in our proposed clustering protocol, we take multiple performance factors for the election of primary and secondary cluster head.

Another important issue of cluster based routing is to reduce the routing overhead. During the route discovery phase, the cluster heads and gateway nodes are flooded with route request (RREQ) and route reply (RREP) packets. Therefore, due to the nature of high mobility of ad hoc networks, any intermediate CH or gateway may move during the route reply process. So, in order to reduce the routing overhead and to address the cluster head mobility, we propose a double cluster head based protocol to facilitate route discovery and maintenance and to improve network stability.

The rest of the paper is organized as follows: In Section –II, summary of previous related works was presented. Section-III consists of the overview of the proposed solution and the estimation of metrics that are chosen for the proposed clustering protocol was discussed. Section-IV shows the performance evaluation of our proposed work. Section V concludes the paper and gives directions for future scope.

2 Literature Review

In this section, we broadly classify the literature study into two sections namely: attacks in MANETs and secure routing.

2.1 Attacks in MANETs

In snooping, the nodes misuse the inherent trust between nodes to eavesdrop on packets to obtain packet payload data and routing information.

In flood storm attacks, malicious nodes flood the network with route requests and route replies, effectively paralyzing the network.

In tampering attacks, the intermediate nodes modify the packet content or change source and destination address. Data packets are prevented from reaching node and also nodes are prevented from sending data packets in denial of service attacks.

In rushing attacks, a malicious node establishes routes through it.

In blackhole attack, malicious nodes advertise them as having shortest route to destination node, thus all traffic is forwarded toit and the node does not forward any traffic at all.

A wormhole attack creates a tunnel called, wormhole tunnel, between two nodes [11]. A wormhole tunnel diverts packets to some random node in the network rather than the intended destination.

2.2 Secure Routing

Zapata et al., [11] presented an overview of various approaches to secure routing protocols in MANETs. An extension of AODV, secure AODV was proposed which provides security features to the routing protocol. Features like digital signatures and hash chains were incorporated to secure the AODV messages. Digital signatures are used to authenticate the non-mutable fields of the messages and hop count information is secured using hash chains. The route error messages generat-

ed by a node are signed using digital signatures and forwarded. Neighbor nodes verify the signature before forwarding.

Deng et al.,[11] performed a study on the security issues in particular about black hole attacks when routing is performed in a MANET and also proposed a solution for AODV routing protocol. The authors discussed the routing security issues in a MANET and give an overview of current security schemes proposed for MANETs in the literature. To mitigate the black-hole attacks, it was proposed to disable the ability of the intermediate nodes to reply and all reply messages can be sent from the destination node only, but the routing delay increases considerable to make it infeasible. A more workable solution was proposed where using one more route to the intermediate node that replies the RREQ message to chek whether the route to the destination exists or not and also use the method only when there were suspected node in the network. Their simulation results showed that the proposed method was able to secure AODV from blackhole attack and achieve increased throughput.

In [12], authors attempted to detect the malicious node in AODV protocol under different density of node with number of attacks. They compare normal AODV with AODV affected by malicious nodes which shows that there is degradation in performance of normal AODV due to malicious nodes.

In RCBRP [12], route discovery is done by inter-cluster on-demand and intra-clsuter table-driven routng, which increases only throughput but not other QOS paramenters [desktop-9].

3 PROPOSED SOLUTION

3.1 Overview

Our proposed protocol, which is named "Weighted Double Cluster-head Based Routing Protocol" (WDCBRP) is a double cluster head based routing, in which, primary & secondary CH will be elected for each cluster. WDCBRP aims at improving route stability by reducing frequent path failures through primary & secondary CHs.

- *S. Aruna is currently pursuing her PhD in Anna University, Chennai, and working as Associate Professor in MCA department, Sona College of Technology, Salem, Tamil Nadu, India, PH-9842826484. E-mail: aruna_subram@yahoo.co.in*
- *Dr.A.Subramani is currently working as Professor&Head in MCA Department, KSR College of Engineering, Thiruchengode, Tamil Nadu, India, PH-9842506919. E-mail: subramani.appavu@gmail.com*

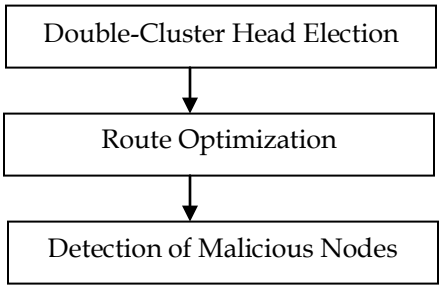

Fig-1: Overview of proposed work

3.2 Cluster Formation

The following assumptions are made before cluster formation:

i. Each mobile node joins exactly with one cluster-head.
ii. The optimal number of nodes in the cluster is assumed to be 'n'.
iii. The co-efficient values used in the weight calculation of nodes assume the following: w1=0. 3, w2=0. 3, w3=0. 2, w4=0. 2. The sum of these co-efficient is 1. These co-efficient values are used to normalize the factors such as mobility, link quality, residual energy and bandwidth efficiency of the mobile node, during node weight calculation.

1. PCH and SCH Selection

Initially, each mobile node broadcasts a beacon message to notify its presence to its neighbors. The beacon message contains the state of the node. Each node builds its neighbor list based on the beacon messages received. The cluster-head election is based on the weight values of the nodes and the node having the highest weight is chosen as a primary cluster-head. And, the node with second highest weight is chosen as secondary cluster-head.

Based on the following algorithm, each node computes its weight value:

1) Broadcast a beacon signal to all its neighbor nodes in the transmission range.

2) Process the beacon signals received from the neighbor nodes in the network and form the connection matrix 'A'.

3) Compute the average speed for a mobile node until the current time T. This gives the measure of the mobility M, based on the X-co-ordinate and Y-co-ordinate of the mobile node at all previous time instance't'. [11], using equation (1)

$$M_{v=} \frac{1}{T}\sum_{t=1}^{T}\sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2} \quad (1)$$

4) Compute the link quality LQ, ie., stability of the mobile node by finding the ratio of first signal and last signal received,using equation (2)

$$MD_A = \frac{1}{N}\sum_{i=1}^{N} D_{A,i} \quad (2)$$

5) The energy consumption is assumed to be more for a cluster-head when compared to an ordinary node. Because, cluster-head is periodically sending beacon signals to its member nodes, and routing the packets to its neighbor clusters, using equation (3)

$$LQ_A = MD_t - MD_{t-1} \text{ [10]} \quad (3)$$

6) Bandwidth efficiency can be calculated by finding the difference between channel capacity of the mobile node and its utilized bandwidth, using the equation (4).

Available Bandwidth (BW) =
Channel Capacity - Utilized Bandwidth [2] (4)

7) The combined weight value W_v for a node is calculated based on the following formula:

$W_v = (W1*LQ + W2*R_S + W3*BW) / (W4*M_v)$,

Where LQ is the link quality, R_s is the residual energy, BW is the available bandwidth and M_v is the mobility of the mobile node.

8) Broadcast W_v to all its neighbor nodes.

9) Process the signals received from the neighbor nodes and identify the weights of its neighbors.

10) Compare the weights of its neighbor nodes with its weight W_t (V).

11) The node with the highest W_v is elected as primary cluster head.

12) The node with second highest W_v is elected as secondary cluster head. All the neighbors of the chosen primary and secondary cluster heads are no more allowed to participate in the election process.

13) All the above steps are repeated only for the remaining nodes, which is not yet elected as primary or secondary cluster head or assigned as a cluster member to a cluster group.

An example of three overlapping clusters with PCH, SCH and gateway nodes are shown below:

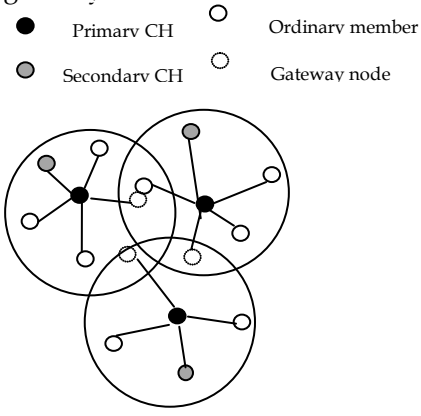

Fig. 3. Cluster formation in MANET

3.2 Cluster Maintenance

It is the second phase of our cluster algorithm. If the moving node is a member node, it will not affect the cluster structure. If the moving node is a primary or secondary cluster head, the cluster structure has to be reorganized by invoking our proposed clustering algorithm to elect cluster heads.

But, in our proposed clustering algorithm, the primary & secondary CH has been chosen based on the combined metrics such as mobility, link quality, residual energy and bandwidth. Therefore, cluster head movements would not happen frequently. But, due to high mobility, cluster heads may move. If the primary cluster head is about to move from its boundary, it signals the secondary cluster head, and secondary CH would take the role of primary cluster head, thus avoids path failure & improves cluster stability.

1. Detection of Malicious Nodes

During the transmission of packets from source to destination, the intermediate node which does not participate in routing process is considered as malicious nodes. The malicious node leads to several attacks. The security algorithm that we proposed below helps in isolating the malicious nodes thus by preventing packets from wormhole, black hole and Denial of Service (DoS) etc.,

2. Proposed Secure routing scheme

Quality of service requires security mechanism to ensure appropriate service assignment. In our proposed double cluster head based secure routing scheme, se implement a security mechanism which starts with data protection like cryptographic process. In cryptographic process, Diffie-Hellman algorithm is used for encrypting and decrypting the data. It is an asymmetric key cryptography which is used for key exchange. The source and destination nodes create a session key to share the information.

3. Elliptic curve digital signature algorithm

After cryptographic process, the secret signature is inserted by this Elliptic Curve Digital Signature Algorithm [12] along with session key and forwards to destination. The intermediate node simply forwards the packets. The destination node matches the signature, if it matches the information be decrypted. If it does not match, the destination node cannot be able to access the information. Thus, elliptic curve digital signature algorithm provides authentication and security. Thus high level of security is implkemented along with the QoS.

4 Simulation Results

4.1 Simulation Model and Parameters

The Network Simulator (NS-2) [12], is used to simulate the proposed architecture. In the simulation, mobile nodes are randomly deployed in 750 meter x 750 meter region for 50 seconds of simulation time. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in Table-1.

Number. of Nodes	100 to 500
Node Speed	5m/s to 25m/s
Area Size	750 X 750m
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 Sec
Traffic Source	CBR
Number of CBR connections	10
Packet Size	512
Rate	50kb
Initial Energy	20 Joules
Transmission Power	0.660
Receiving Power	0.395

Table-1 Simulation settings

4.2 Performance Metrics

The proposed SD-CBRP is compared with the CBPMD protocol. The performance is evaluated mainly, according to the following metrics.

- **Packet Delivery Ratio**: It is the ratio between the number of packets received and the number of packets sent.
- **Delay**: It is the average end-to-end delay measured in seconds.
- **Throughput**: It is the average number of packets received per second.

4.3 Results

1. Based on Node Speed
   The speed of the mobile node is varied from 5m/s to 25m/s for 100 nodes.

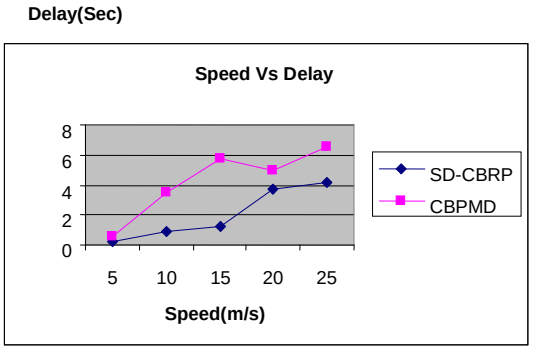

Fig 2. Speed Vs Delay

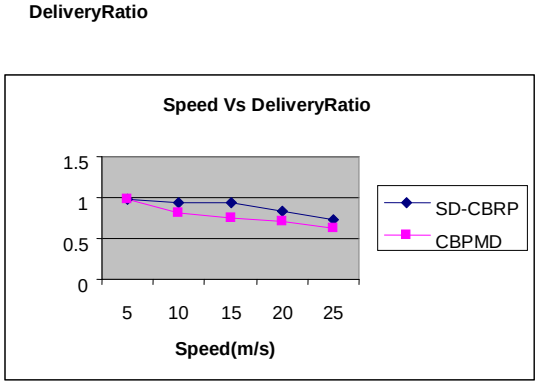

Fig 3. Speed Vs Delivery ratio

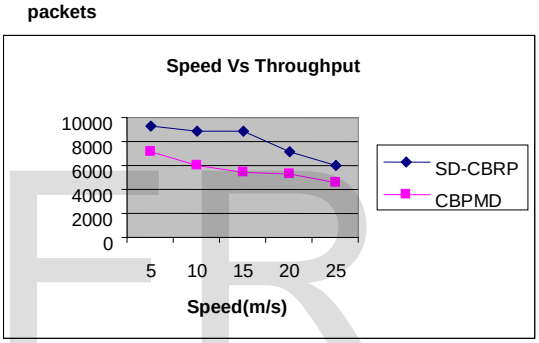

Fig 4. Speed Vs Throughput

5 Conclusion

Mobility of nodes cause frequent route failure. Therefore, it is evident from the simulation results that, our proposed protocol SD-CBRP avoids frequent cluster re-affiliation and gives better results in terms of increased throughput and packet delivery ratio when compared to CBPMD. Also, it adopts a secure routing scheme to ensure appropriate service assignment. As a result, the average end-to-end delay is reduced and by designating double cluster heads, link breakages are avoided.

6 References

[1]. Dr. Mohammad U. Bokhari, Hatem S.A. Hematite, Shams TabrezSiddigui, "A Review of Clustering Algorithms, as Applied in MANETs", *International Journal of Advanced Research in Computer Science and Software Engineering*, volume 2, Issue 11, November 2012, ISSN: 2277 128X pp. 364-369.

[2]. N. Sumathi, Dr. C.P. Sumathi, "Energy and Bandwidth Constrained QoS Enabled Routing for MANETs", *International Journal of Computer Networks & Communications (IJCNC)* Volume-5, No. 2, March 2013, pp. 37-46

[3]. Rathish Agarwal, Roopam Gupta, Mahesh Motwani, "Review of Weighted Clustering Alogirthms for Mobile Ad Hoc Networks", *GESJ: Computer Science and Telecommunications*, 2012, No. 1(33), ISSN: 1512-1232, pp. 72-77.

[4]. S. Aruna, Dr. A. Subramanian, "Comparative Study of Weighted Clustering Algorithms for Mobile Ad Hoc Networks", *International Journal of Emerging Technology & Advanced Engineering (IJETAE)*, ISSN: 2250-2459, Volume 4, Issue 5, May 2014, pp. 307-311.

[5]. Mohammed Abdullah Naser, "Study analysis and propose enhancement on the performance of cluster routing algorithm in a Mobile Ad hoc Network", *Journal of Advanced Computer Science and Technology Research*, Vol.4 No.1, March 2014, pp. 12-2.

[6]. Naveen Chauhan, Lalit Kumar Awasthi, Narottam Chand, Vivek Katiyar, Ankit Chugh, "A Distributed Weighted Cluster Based Routing Protocol for MANETs", *Scientific Research Journal of Wireless Sensor Network*, 2011, No. 3, pp. 54-60.

[7]. Fereydoun Ramezani, Zangi Sajjad mavizy, Javad Badali, "A Stable Distributed Clustering Algorithm For Mobile Adhoc Networks", *IJCSI International Journal of Computer Science Issues*, Vol. 9, Issue 5, No 3, September 2012 ISSN (Online): 1694-0814, pp. 245-250.

[8]. Ayman Bassam Nassuora, Abdel-Rahman H. Hussein, "CBPMD: A New Weighted Distributed Clustering Algorithm for Mobile Ad hoc Networks (MANETs)", *American Journal of Scientific Research*, ISSN 1450-223X Issue 22(2011), pp.43-56.

[9]. S. Muthuramalingam and R. Rajaram, A Transmission Range Based Clustering Algorithm for Topology Control Manet", *International Journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC)* Vol.2, No.3, September 2010.

[10]. Ankit Verma, A.K. Vatsa, "Optimized Stable and Reliable Routing (OSRR) Mechanism in MANET", *International Journal of Science and Technology*, Volume 1 No. 9, September 2012, ISSN: 2049-7318, pp. 466-475.

[11]. Manikandan. S.P, Manimegalai. R, "Survey on Mobile Ad Hoc Network Attacks and Mitigation using Routing Protocols", *American Journal of Applied Sciences*, 2012, ISSN: 1546-9239, Volume 9 No. 11, pp. 1796-1801.

[12]. Nandhini. J, Dr. D. Sharmila, "Security Based Weighted Cluster Routing in MANET", *Journal of Theoretical and Applied Information Technology*, 2014, ISSN: 1992-8645, Volume 64 No. 1, pp. 102-106