TEST Engineering & Management

March - April 2020
ISSN: 0193-4120 Page No. 14539 - 14544

Fuzzy based Reliable data Gathering Routing in Mobile Ad Hoc Networks

Dr.S.Mohana,Associate Professor,Department of CSE, Saranathan College of Engineering,Trichy.
V.Kalpana,Asst.Professor,Department of CSE,K.Ramakrishnan College of Technology,Trichy.

Article Info
Volume 83
Page Number:14539 - 14544
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 22 April 2020*

Abstract:

Ad hoc network plays a vital role in the wireless networks. Mobile ad hoc network is a kind of ad hoc network where the nodes are communicated without access point. There was no static topology followed in ad hoc networks. Data gathering is one of biggest challenge in ad hoc environment. In this research work, Fuzzy based Data Gathering Routing Protocol (FDGRP) is proposed to improve data gathering ratio among the mobile environment. It contains three phases. In first phase, multicast routes are discovered and cluster is formed based on reliable links. In second phase, data gathering algorithm is followed to ensure high packet availability. In third phase, fuzzy decision rules are applied to provide more gathering ratio. The simulation results are evaluated using network simulation tool.

Keywords: Minimum 7 keywords are mandatory, Keywords should closely reflect the topic and should optimally characterize the paper. Use about four key words or phrases in alphabetical order, separated by commas.

I. INTRODUCTION

Due to dynamic nature of ad hoc environment, the nodes may be compromised by the attackers. If any dropping attacks are present, information may be reached at the destination efficiently. The concept of fuzzy decision rule is used for finding the reliable nodes as well as links. Data gathering ratio is improved based on packets observation by the mobile nodes. In this research work, fuzzy based data gathering routing protocol is established to attain balancing between energy and data availability.

II. PREVIOUS WORK

Anonymous Multicast Routing scheme [1] was introduced for reducing delay and the malicious nodes were blocked for efficient data transmission. Packets are divided into segments which are transmitted through multiple routes. The nodes were compromised by the attacks to observe the data transmission between the nodes. This scheme identifies the undetectable paths in the network. But there was no protection of data in the network during data transmission.

Security based energy model [2] was based on erasure coding to attain balance between reliability of paths and energy of nodes. The estimation of packet quantities and optimal path determination are the key challenges in the network. The security algorithm was established based on alert procedure and hierarchical zone installation in the routes. Multiple erasure coding was used for the data transmission.

The classification methods on intrusion detection [3] were examined in ad hoc network. There were five classifiers used for investigation of attackers in these methods. The classification error and weighted classification error were developed for obtaining the network performance. The performance of network was affected by the unknown affects.

Published by: The Mattingley Publishing Co., Inc.

The different categories of attack, mobility scenarios and clock intervals covered the dataset of the network.

The watchdog and path rater mechanism [4] were introduced based on intrusion detection system. The nodes were permitted for relay transmission within the time frame. If it violates, the nodes are considered here as misbehaving nodes. The tag communication was sent based on node trustworthiness and reliable routes.

The trustworthy based routing scheme [5] was explored based on node trust values. The existing schemes were implemented to detect the fake id nodes based on optimal value. This scheme provided quality of service metrics and compared to existing schemes.

A semi distributed scheme [6] was proposed based on the intrusion detector and source routing protocol to improve the network security. The characteristics of reputation were disturbed based on human behavior. A distributed scheme was implemented based on observation to assign the node priority. The true relationship was protected by this scheme.

Signature based multi-layer intrusion detection [7] system was developed. A new signature based ID was launched using mobile agents. The rule based signatures were used for small to large database systems. The database was updated based on the detection of new signature.

A Trust based Multipath Security Scheme [8] was developed for the data transformation to incorporate packet dispersal in the network. The information dispersal algorithm was used in conjunction with multiple paths. The eigen trust calculation was estimated to route packets. Based on node recommendation and node's capacity value, the trust value was determined.

Fuzzy based Intrusion Detection System [9] was introduced to find intrusions based on threshold values and category of attackers. The intrusion was found based on detection of black hole and gray hole attacks. The significance of causes was found based on various aspects.

An innovative approach [10] was developed for estimating the energy and security and providing balancing between them. The reliable routes were established to remove least remaining energy of nodes. The intelligent approach was captured based on dynamic nodes behaviors.

A watchdog technique [11] was presented to detect the misbehaving nodes with fake reports. A table was maintained to record the number of packets during transmission and reception. Based on the receiving packets, the checksum error was found. Immediately the misbehaving nodes are reported to the source nodes.

III. PERFORMANCE OF FDGRP

In this section, Fuzzy based Data Gathering Routing Protocol (FDGRP) is introduced based on scheduling algorithm. The algorithm gives priority to nodes and packets. Cluster formation is done based on group of nodes with stability metrics. There are two categories of node used here in the cluster group i.e. static node and dynamic node. The data gathering scheme is implemented based on time division multiple access. Figure 1 illustrates the cluster formation based on cluster head and cluster members. Due to high density of mobile nodes, cluster formation will be implemented based on node mobility and energy. The selection of Cluster head (CH) is done based on node stability, activity of node in the routing history and data gathering ratio. During information gathering, the energy consumption of nodes becomes more. The network energy is optimized to balance the power between transmission and reception.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 14539 - 14544

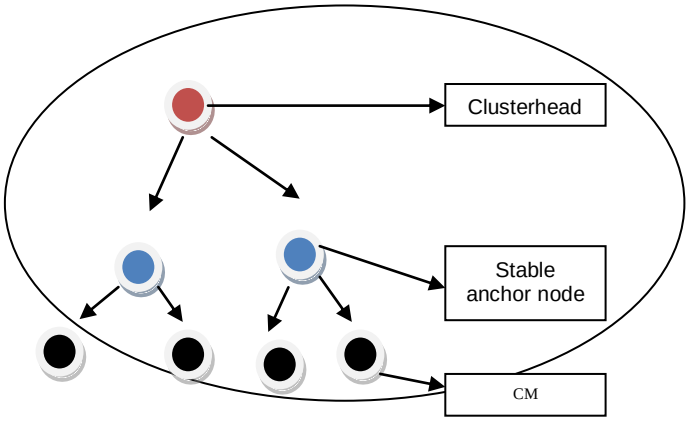

Fig.1. Cluster Formation

Data Gathering Algorithm

The cluster members are deployed and the route reliability is established to propose the fuzzy data gathering routing protocol based on network environment scenarios. The following assumptions are made to establish the stable network model.

1. Cluster Head (CH) records the random location of cluster members.
2. Cluster members are distributed randomly in the cluster network environment.
3. Static nodes are located except cluster head and cluster members.
4. The power limited nodes are not allowed by cluster head during node deployment and route discovery scheme.
5. Received Signal Strength Indicator (RSSI) is used to differentiate CH and Cluster member.
6. Cluster network environment is established without access point whereas CH has high power and more handling capacity with high reachability.
7. The transmission energy between transmission and reception is adjusted by the distance.
8. Data transmission is required during symmetric radio communication.
9. If energy is depleted, the cluster member will not be present in cluster region.
11. Anchor node computes the activity of mobile nodes and report will be received by the cluster head.
12. According to network scenarios, the count of CH is varied.
13. Data gathering can be done on sink node only.

Mobility model

Cluster members in mobility model use the random way point mobility model. Nodes are randomly located in the 1200 x 1200 sq.m region. Cluster head communicates the cluster members inside the coverage area. Unknown node is allowed to join the cluster region after the approval of cluster head.

Fuzzy decision model

In this phase, fuzzy inference engine is used for providing high data gathering ratio. Input parameters are taken as stability of node, data observation factor and route reliability. The node stability is determined how well the node behaves in high mobility scenarios. The data observation factor is used to identify the node which observes the information in a short span of time. The route reliability is estimated based on link expiry time and node quality. These parameters are taken as crisp values. The output of fuzzy inference engine isdata gathering ratio. If anyone of input crisp values is below threshold value, the value of gathering ratio will become less.

Stable routes are found based on link quality. The location of mobile nodes based on minimum hop count and accuracy of node location. Based on trilateration method, location of node is found. Gathering ratio of node is obtained through next hop neighbor node. It will be updated in the routing table. Data gathering ratio is improved based on the following steps.

1Cluster Head (CH) computes the packet forwarding ratio before transmission.

2After joining the cluster group, cluster members will receive the data packets.

3The routing table is updated based on gathered packets.

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 14539 - 14544

4 CH checks the link quality and try to improve the data gathering.

5 If node is found with maximum packet loss, it will be immediately isolated from the network.

IV. SIMULATION RESULTS

Fuzzy based Data gathering routing protocol is simulated using network simulation tool (NS2.34). Number of nodes used here is 200 nodes. The Medium access channel is 802.11. The network traffic used here is constant bit rate.

Table 1. Simulation and Setting Parameters of FDGRP

No. of Nodes	200
Area Size	1100 x 1100 sq.m
Mac	802.11
Radio Range	200 meter
Simulation Time	100 sec
Traffic Source	Constant Bit Rate
Packet Size	80 bytes
Mobility Model	Random Way Point
Protocol	MAODV

The following QoS metrics are used for simulation.

Data gathering ratio: It is defined as the number of packets gathered to the total number of packets during transmission.

Processing delay: It is defined as the delay of packets during the propagation from cluster head.

Packet dropping ratio: It is defined as the number of packets dropped to total available packets.

Network lifetime: It is defined as the number of epochs gathered during the node lifetime.

Control overhead: It defines the presence of excessive control packets in the link.

Figure 2 shows the performance of FDGRP over existing schemes in terms of data gathering ratio. The proposed scheme achieves high ratio than existing schemes.

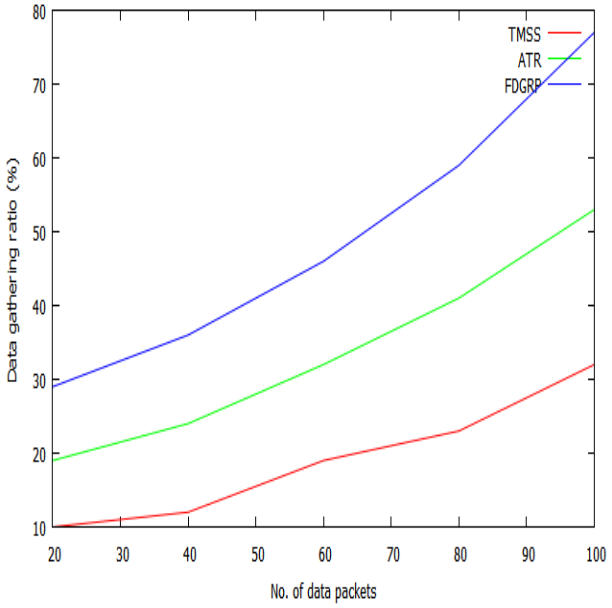

Figure 2. Data gathering ratio Vs No. of data packets

Figure 3 shows the analysis of process delay while varying simulation time in x axis. The delay of FDGRP is less compared to compared to existing schemes.

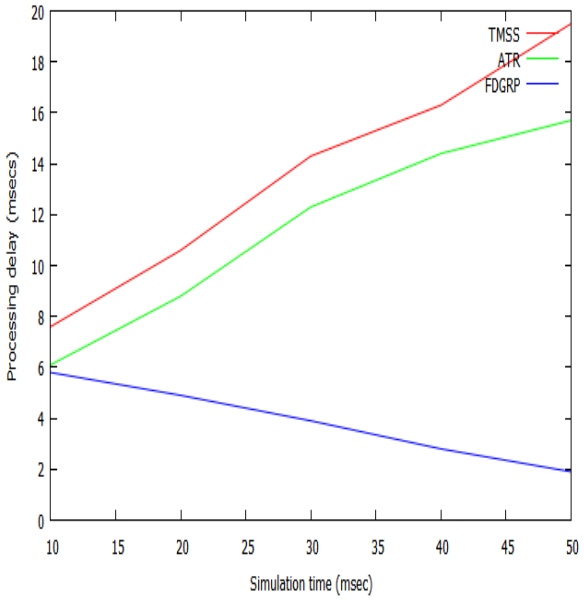

Figure 3. Processing delay Vs Simulation time

Figure 4 illustrates the performance of packet dropping ratio while varying number of nodes in x axis. From the results, it is seen that

Published by: The Mattingley Publishing Co., Inc.

March - April 2020
ISSN: 0193-4120 Page No. 14539 - 14544

FDGRP achieves less dropping ratio than existing schemes.

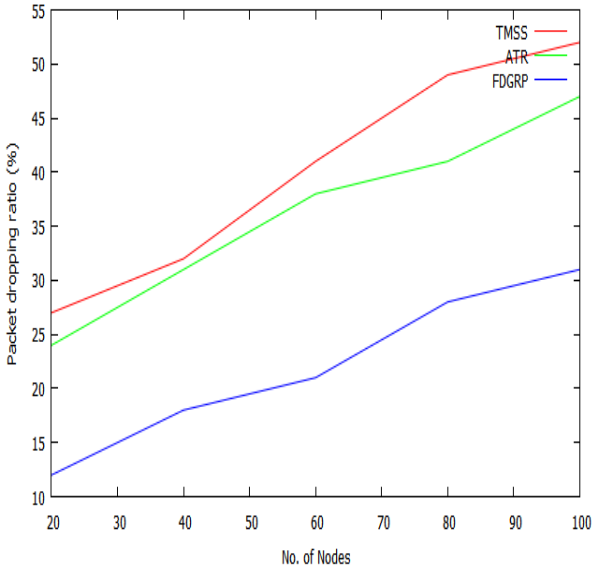

Figure 4. Packet dropping ratio Vs No. of Nodes

Figure 5 illustrates the performance of Network lifetime of FDGRP while varying the number of routes in x axis. The proposed scheme achieves high network lifetime than existing schemes..

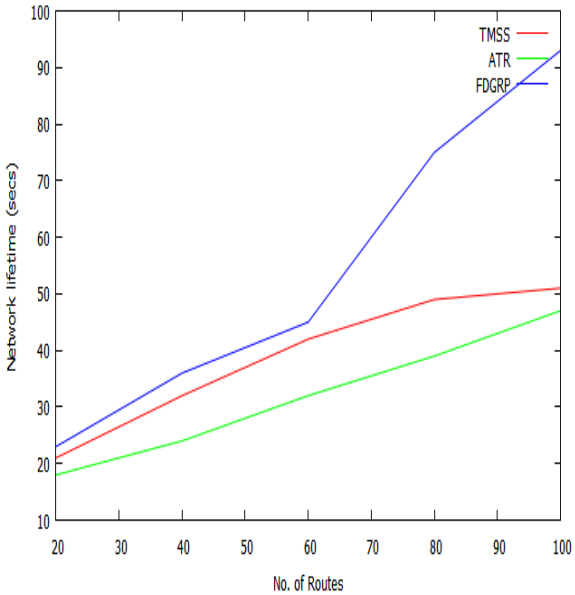

Figure 5. Network lifetime Vs No. of routes

Figure 6 shows the results of control overhead while varying time in x axis. It is seen that overhead of FDGRP is less compared to existing schemes.

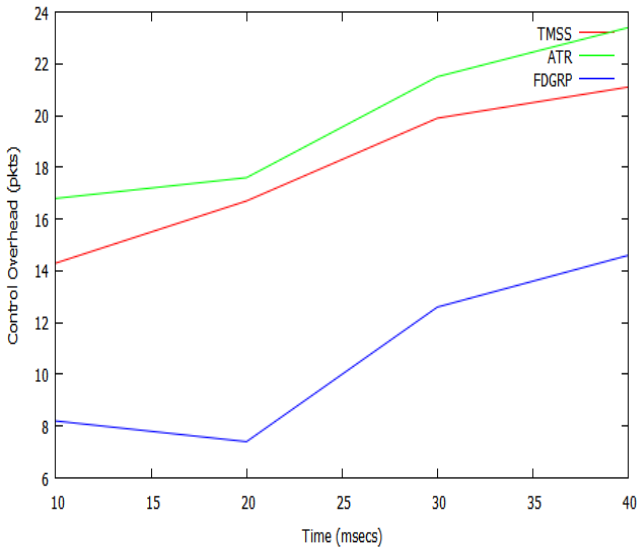

Figure 6. Control Overhead Vs Time

V. CONCLUSION

MANET contains mobile nodes where the links are dynamic. Due to dynamic links, the packets may be dropped. In this scenario, data gathering ratio is the biggest challenge in ad hoc environment. In this research work, Fuzzy based Data Gathering Routing Protocol is proposed to improve data gathering ratio based on fuzzy decision mechanism. In first phase, cluster is formed to support the network connectivity. In second phase, data gathering algorithm is introduced to reduce packet loss and provide stable routing. In third phase, fuzzy model is introduced to attain balance between data gathering ratio and energy. In future, it is planned to MAC based Reliable data gathering scheme to provide high packet arrival rate.

REFERENCES

[1] "Efficient Anonymous Multicast Routing Protocol in MANET", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, No. 3, 2014, pp.187-193.

[2] Sethulekshmi and Manoj Kumar, "Energy Efficient Secure Routing in MANET Based on Multipath Erasure Coding", International Journal

Published by: The Mattingley Publishing Co., Inc.

of Engineering and Computer Science, Vol.4, No. 10, 2015, pp. 14717-14724.

[3] Aikaterini Mitrokotsa, Christos Dimitrakakis , "IntruMadhumitha and S. Kirubakaran, sion detection in MANET using classification algorithms: The effects of cost and model selection", , Elseiver, Vol. 2, No.5, 2012, pp.1-12.

[4] Charlie Obimbo, Liliana Maria Arboleda-Cobo, "An Intrusion Detection System for MANET", Communications in Information Science and Management Engineering, Vol.2, Issue.3, 2012, pp.1-5

[5] Sridhar and Baskaran, "Ant Based Trustworthy Routing in Mobile Ad Hoc Networks Spotlighting Quality of Service", American Journal of Computer Science and Information Technology, Vol.3, Issue 1, 2015, pp.64-73.

[6] Animesh Trivedi, Rajan Arora1, Rishi Kapoor, Sudip Sanyal and Sugata Sanyal, "A Semi-distributed Reputation-based Intrusion Detection System for Mobile Ad hoc Networks", Journal of Information Assurance and Security, Vol.4, No.3, 2006, pp.265-274.

[7] Mueen Uddin, Azizah Abdul Rehman, Naeem Uddin, Jamshed Memon, Raed Alsaqour, and Suhail Kazi, "Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents", International Journal of Network Security, Vol.15, Issue 1, 2013, pp.79-87.

[8] Shyamala, Niveda Ashok and Bhavya Narayanan, "Trust-based multi-path Security Scheme for Ad-hoc networks", International science, Vol.8, Issue 15, 2015, pp.1735-1742.

[9] Anusha, Jayaleshwari , Arun Kumar and Rajyalakshmi, "An Efficient And Secure Intrusion Detection Method In Mobile Ad hoc Network Using Intuitionistic Fuzzy", International Journal of Engineering and Technology, Vol.5, Issue 3, 2013, pp.2575-2584.

[10] Kumuda, Usha and Venkatraman, " An Approach for Energy based Secure Routing Protocol", International Journal of Computer & Mathematical Sciences, Vol.4, Issue 12, 2015, pp.11-14.

[11] Nidal Nasser and Yunfeng Chen, "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks", IEEE Communications, 2007, pp.1-6