Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURITY BASED WEIGHTED CLUSTER ROUTING IN MANET

[1] Mrs.J.NANDHINI, [2] Dr.D.SHARMILA, [3]K.DHIVITHRA, K.S.BALASUGANYA, D.GOWRI

[1]Associate Professor, Department of ECE, Jay Shriram Group of Institutions, Tirupur
[2]Professor & Head, Department of EIE, Bannari Amman Institute of Technology, Erode
[3]Students, Department of ECE, Jay Shriram Group of Institutions, Tirupur

ABSTRACT

In close to future computing atmosphere, usually expected the recent progresses and advances in computing and communication technologies. Mobile Adhoc Network (MANET) is one of the promising fields for analysis and development of wireless network. Routing in wireless MANET has to be economical and saving of resources. One in every of the approaches to understand these items is completed by dividing the network into clusters and every cluster have a Cluster Head (CH) that's answerable for the nodes associated among the cluster. Due to the dynamic atmosphere and random topology, the CH election technique has to be done per applicable criteria. This paper aims at weight based cluster routing with the improvement of QoS along with security. Here CH is chosen with relevance to weighted parameters like bandwidth, energy efficiency and link quality thereby giving higher QoS and elliptic curve digital signature algorithm which provides security from attacks by victimization Network Simulator-2. On scrutiny with CBRP protocol, this weight based cluster routing protocol achieves the QoS in economical and efficient manner.

Keywords: *MANET, CBRP protocol, Security, Clustering, QoS.*

1. INTRODUCTION

MANET simply stated, are unplanned, self-organizing networks composed of mobile nodes that utilize networking principles for interconnectivity. Nodes in the network should be able to sense and discover with nearby nodes. Due to limited transmission range of the node, multiple hops may be needed in exchanging data between the communication parties. Each node acts both as router and as a host. MANET are useful for different purposes. Example: military operation to provide communication between squads, medical control etc., Routing protocol plays an important role in implementation of MANET. The different types of routing protocols are i) Table Driven, ii) On-Demand, iii) Hybrid Protocols.

MANET exhibits unique characteristics such as node mobility, unpredictable link properties, dynamic topology, limited bandwidth and limited energy resources. Now-a-days real time applications using wireless links is getting more attention. Such applications demand specific characteristics on QoS such as throughput, delay, jitter and error rate. The characteristics of MANET make the provision of QoS for real time applications very challenging.

The process of dividing the network into interconnected substructures called clustering and the interconnected substructures are called clusters. The aggregation of nodes into clusters are controlled by a Cluster Head (CH) provides a convenient framework for the development of important features such as code separation, channel access, routing and bandwidth allocation. For the election of CH in Mobile Networks include the Highest degree, the Lowest identifier, Distributed Clustering Algorithm, Weighted Clustering Algorithm (WCA).

A closed Ad-hoc network is at a greater risk by allowing the extended presence of malicious nodes, but more likely to have preinstalled security mechanisms to detect these malicious nodes.

2. RELATED WORK

Researchers have proposed several clustering algorithms and security mechanisms. However these algorithms achieve limited QoS and security.

In [1] authors designed Flexible QoS Model for MANET (FQMM) which classifies nodes such as ingress, egress and interior nodes for forwarding packets and provisioning is done by per-class and per-flow provisioning methods and it

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

controls traffic by conditioning mechanism. In complex cases, effective link capacity is not determined and it is only suitable for medium size MANET.

In [4] authors introduced CBQR(Cluster Based QoS Routing) protocol for MANET, which not only deals with bandwidth requirement over the wireless network but also takes care regarding the routes, storage overheads and limited battery power. Since it is table-driven routing protocol that consumes more power.

In RCBRP, route discovery is done by inter-cluster on-demand and intra-cluster table-driven routing which increases only throughput but not other QoS parameters [9].

Malicious node is responsible for several attacks which leads to loss of information. It is detected by a trust based packet forwarding scheme using routing layer information and security is provided by link layer using CBC-X mode of authentication and encryption [5].

In [2] authors proposed MSRP uses pre-determined cryptographic certificates that guarantees end-to-end authentication, thus it restricts the attacks. It does not require any intermediate node to perform cryptographic operation or have a prior association with the end nodes.

In [10] authors suggested SCEEP divide MANET into 2-hop cluster where each node belongs to at least one cluster. It uses weight based leader election model to balance resource consumption and Diffie-Hellman key exchange protocol for secure communication.

In [11] authors presented mechanisms for avoiding cluster head re-election process. It is mainly concerned with mobility and no geographical, distance and speed information are required. They provide heuristic weight function and king bonus mechanism for cluster head which avoids re-election process.

A cluster based routing protocol was proposed which has weight group, so that the speed of the cluster formation increases and the network services are more accessible. Here routing is done quickly, because routing depends on the address of cluster head [3].

A distributed weight based clustering algorithm which solves the problem of node density that increases the stability of the cluster, also the load of the network is balanced [8].

In [13] 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.

3. PROPOSED WORK

Clustering is an important concept for MANET because clustering makes it possible to guarantee basic levels of system performance, such as throughput and delay, in the presence mobility and large number of nodes.

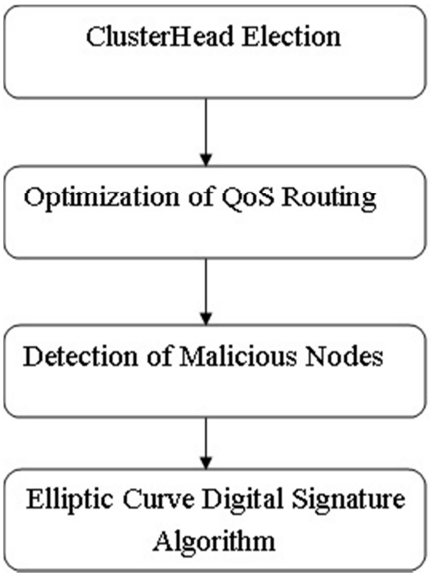

Figure 1: Block Diagram

A. Cluster head Election

In MANET, the nodes with different energy levels are grouped together to form a cluster. Each node in the cluster has unique identification number. Each cluster has several nodes in the transmission range. After formation of cluster, CH is elected based on weight based parameters such as Bandwidth, Energy Efficiency, and Link Quality. The node with highest weight value is chosen as CH. The node with former highest weight value is chosen as Sub Head (SH).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This SH acts as a CH if the existing CH moves away from the cluster. This avoids cluster re-election process.

B. Optimization Of Qos Routing

The packet delivery fraction of QoS_WCA protocol is apparently higher than that of WCA. This attributes to effectiveness of node disjoint paths algorithm used in QoS_WCA.

*Packet Delivery Ratio = Ratio of packets received to packets sent PDR = (PR/PS)*100 %*

When network topology change speed up, the success rate of the local repair declined in WCA protocol and lead to cache data packet loss. The backup paths in AODV protocol is intersecting and the broken place is likely to the public mode of two paths, thus this lead to larger failure probability of data packet. But QoS_WCA protocol can quickly find alternate paths to arrive the same destination node, so the probability of packet discarded is small. At the time of discovery link open QoS_WCA protocol can find alternate paths of non-existent public node. Further because of considering the maximum residual energy of each node in selecting path, the chance of path broken is smaller, so the packet delivery fraction is increased.

It can be seen that with the acceleration of the network topology changing average end-to-end delay of two protocols all increased but the average end-to-end delay of QoS_WCA is lower and smoother than that of WCA. In particular, with the network topology change intensified the differences between QoS_WCA protocol and WCA. When a node maximum movement speed is to 15m/s, the delay of QoS_WCA protocol is low to nearly 70% than that of AODV protocol and lower compared with the WCA protocol. This is mainly because QoS_WCA protocol can use alternate routing in link broke so then reduced delay of source node rerouting. Moreover, QoS_WCA protocol adopts minimum hops path in selecting node dis-joint path to be great influence on end-to-end delay.

Average end-to-end delay(AD) = Delay spent to deliver each data packet AD = TD/PR.

It can be seen that with the acceleration of the network topology changing the average throughput of two protocols all increased, but the average throughput of QoS_WCA is higher and smother than that of WCA.

*Throughput = No. of bytes received * 8 / (end time – start time)*

C. Detection Of Malicious Nodes

During the transmission of packets from source to destination, the intermediate nodes which does not belong to path of the route is considered as malicious nodes. The malicious nodes leads to several attacks. This security algorithm isolates malicious nodes preventing packets from wormhole, black hole, Denial of Service(DoS), and modifier attacks.

D. Security Mechanism

QoS requires security mechanism to ensure appropriate service assignment. Inappropriate service level selection can leak extra information but clever manipulation of QoS parameters might even help to reduce the leaking of information.

In our paper we implement security mechanism which starts with data protection like cryptographic process. In cryptography process, Diffie-Hellman algorithm is used for encrypting and decrypting the data. It is an asymmetric key cryptography which is used for key exchange. Here the source and destination create a session key to share the information.

Elliptic curve digital signature algorithm:

After cryptographic process, the secret signature is inserted by this Elliptic Curve Digital Signature Algorithm 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 implemented along with the QoS.

4. SIMULATION AND RESULTS

In this section, we evaluate the proposed routing protocol and compare it with WCA routing protocol via simulation. For this purpose, we

Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

implemented the proposed algorithm on the NS-2 simulator.

Packet Delivery Ratio:

Figure 2 shows comparison for packet delivery fraction of QOSWCA and WCA under different node movement speed.

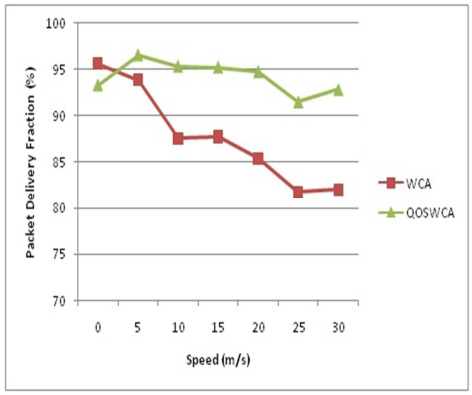

Figure 2: PDR Vs Speed

Average throughput:

Figure 3 shows comparison for average throughput of two protocols under different node movement speed.

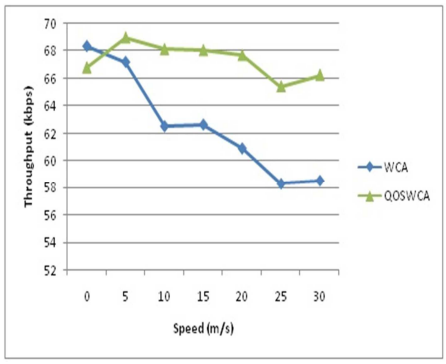

Figure 3: Throughput Vs Speed

Average End to End Delay:

Figure 4 shows comparison for average end to end delay of two protocols under different node movement speed.

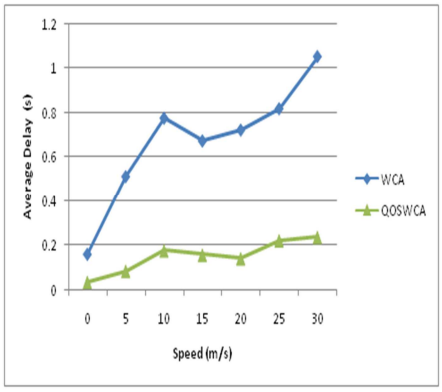

Figure 4: Average Delay Vs Speed

Effect of Malicious nodes:

Figure 5 illustrates the reduction of packet delivery ratio in the presence of malicious nodes.

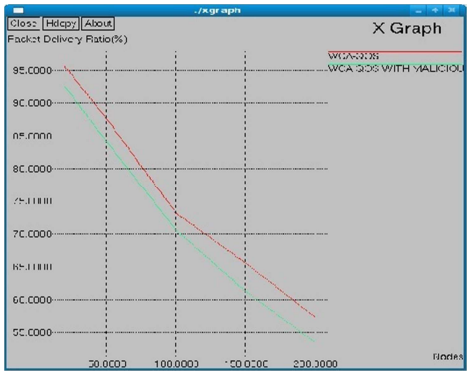

Figure 5: Packet Delivery Ratio Vs No. of nodes

Figure 6 illustrates the increase of delay in the presence of malicious nodes.

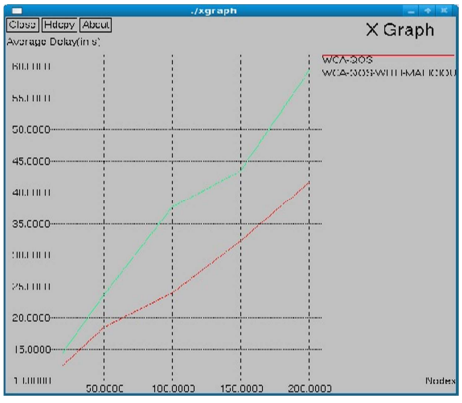

Figure 6: Average Delay Vs No. of nodes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CONCLUSION

Our QoS_WCA is a On-demand (Reactive) cluster based routing protocol for MANET. In our method, QoS_WCA avoids the cluster re-election by choosing SH along with CH thereby achieving QoS parameters. QoS requires security mechanisms to ensure appropriate service assignment. The leakage of information in this method is overcome by Elliptic Curve Digital Signature Algorithm. Simulation results demonstrate significant improvement in Packet Delivery Ratio (PDR), throughput, and reducing delay over traditional routing protocol and better performance than other routing protocols.

6. REFERENCES

[1] Hannan XIAO, Winston K.G. SEAH, Anthony LO and Kee Chaing CHUA, "A Flexible Quality of Service Model for Mobile Adhoc Networks," In proceedings of the IEEE Vehicular Technology Conference, Tokio, Japan, 2000.

[2] Li Zhitang and Shi Shudong, "A Secure Routing Protocol for Mobile Adhoc Networks," 6th IEEE/ACIS International Conference on Computer and Information Science, 2007.

[3] M. Rezaee, M.Yaghmaee, "Cluster Based Routing Protocol for Mobile Ad Hoc Networks", 2009.

[4] Prof. P.K. Suri, Dr. M.K.Soni, and Parul Tomar, "Cluster Based QoS Routing Protocol for MANET", International Journal of Computer Theory and Engineering, Vol.2, No.5, 2010.

[5] A.Rajaram and Dr.S. Palaniswami, "Malicious Node Detection System for Mobile Adhoc Networks,"International Journal of Computer Science and Information Technologies, vol.1, 2010.

[6] S.Karunakaran and P.Thangaraj, "A cluster Based Service Discovery Protocol for Mobile Adhoc Networks," American Journal of Scientific Research, Issue 11, 2011.

[7] Huang Lu, Jie Li, Senior Member, and Mohsen Guizani, "Secure and Efficient Data Transmission For Cluster-based Wireless Sensor Networks," IEEE Transactions On Parallel And Distributed Systems, 2012.

[8] Fereydoun Ramezani Zangi, Sajjad mavizy, Javad Badali, "A Stable Distributed Clustering Algorithm For Mobile Adhoc Networks", International Journal of Computer Science and Issues, Vol.9, 2012.

[9] Yuvraj Kumbharey, Suwesh Shukla, and Sushil Chaturvedi, "Renovated Cluster Based Routing Protocol for MANET," International Journal of Advanced Computer Research, Vol.3, No.1, Issue 8, 2013.

[10] Shobana M and Suresh S, "Secure Clustering and Energy Based Routing for Mobile Adhoc Networks," International Journal of Emerging Technology and Advanced Engineering, Vol.3, Issue 3, 2013.

[11] Mr.V.V.Sunil Kumar and Dr. Ash Mohammed, "A Hierarchical Weighted Clustering Algorithm Optimized for Mobile Networks," International Journal of Advanced Research in Computer Science And Software Engineering, Vol.3, Issue 6, 2013.

[12] Xiaoyong Li, Feng Zhou and Junping Du, "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks," IEEE Transactions On Information Forensics And Security, 2013.

[13] Priyambada Sahu, Sukant Kishoro Bisoy, Soumya Sahoo, "Detecting and Isolating Malicious Node in AODV Routing Algorithm", International Journal of Computer Applications, Vol.66, 2013.

[14] Network Simulator 2, http://www.isi.edu/nsnam.