ESMCH: An Efficient And Secure Model For Data Transmission Using Malicious Cluster Head In Manets

P. Vinodhini[1], Dr. S. Lakshmi Prabha[2]
[1]Dept of Computer Science
[2]Assistant Professor, Dept of Computer Science
[1, 2] Government Arts College for Women, Salem-636008

Abstract- *Mobile ad hoc networks (MANETs) are wireless networks made up of a number of autonomous mobile devices that are momentarily linked together by wireless media. MANETs have emerged as one of the most popular fields of study in recent years. The most difficult problems with MANETs are resource constraints, energy efficiency, scalability, and security. MANETs are more susceptible to malicious assault due to their deployment nature. The safe routing protocols execute just the most basic security tasks, which are insufficient to defend the network. An Efficient and Secure Malicious Cluster Head (ESMCH) is presented in this article, which incorporates security considerations into the clustering method to achieve attacker detection and categorization. To make the network more attack resistant, a cooperative approach based on Byzantine agreements is employed for attacker detection and categorization. ESMCH used to address this problem by requiring nodes that are completely surrounded by malicious neighbors to dynamically change their belief and unbelief levels. The suggested approach chooses the most secure and energy-efficient cluster head to serve as a local detector while incurring no cost on clustering performance.*

Keywords- MANET, CH, ESMCH, RREP, RREQ

I. INTRODUCTION

Mobile Ad Hoc Networks (MANET) varies from traditional networks in many ways, including node mobility, limited capacity, and rapid changes in network architecture. MANETS are self-motivated networks with no specified mode of transportation. Fixed cable systems are more secure than wireless networks [1]. Attacks may come from any direction and target any node. They encountered many challenges when the wireless mobile technology was introduced. Engineers devised many solutions over time [2]. A base station (BS) in a given region serves as a transreceiver. When someone want to communicate and is close to the BS, nodes will find it simple to transmit signals straight to the BS. If the nodes are too far apart, the ideal option is to use BS to create a straight line of sight. If nodes are too far apart, they will be unable to transmit any data to the BS, resulting in no communication [3]. To address these issues, energy-efficient methods that create clusters rather than individual nodes are proposed The MANET architecture as shown in Figure 1.

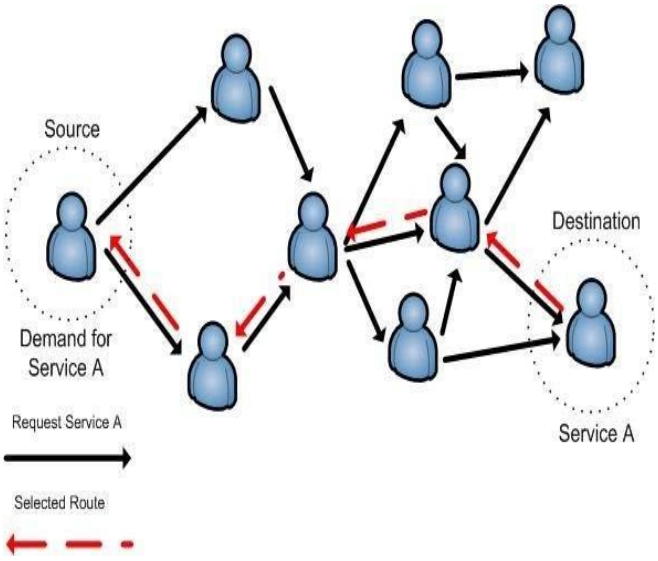


Figure 1: MANET architecture

A network in MANET Cluster architecture is split into Clusters, which are groups of self-managed nodes. Clustering divides a network into virtual groups based on a set of criteria known as protocols. The primary aim of their work is to create mobility and scalability in big networks [10]. Cluster-based routing is used to handle node heterogeneity and to restrict routing knowledge that persists in the network, increasing routing life time and decreasing routing control overhead. Cluster nodes are classified into three types: Cluster Heads, Cluster Members, and Cluster Gateways. The clustering algorithm is divided into two sections. The first is Cluster Formation, and the second is Cluster Maintenance. In the Cluster creation process, the Cluster Head is chosen from among the cluster nodes initially, as illustrated in the figure below. When there are node moves, Cluster Maintenance comes into play. As a result, it asks that re-affiliations be performed alongside regular nodes and cluster chiefs.

During the selection process, one node each cluster is chosen as the CH, taking into account the energy restriction

and processing. Multiple clusters inside a single cluster cause cluster reformation, routing problems, and complex Quality of Service (QOS) concerns [6].

This paper remaining as follows, section II represents the background study about existing MANET Routing protocols, Section III represents the proposed system model, section IV represents the results and discussion and finally presented the conclusion in section V.

II. BACKGROUND STUDY

(Guruswamy et al. 2016) [4] Proposed a method for rebroadcasting based on a proficiency factor known as delay, as well as a route repair mechanism for connection failures. This method also focuses on distributing neighbor scope information among nodes with the explicit aim of keeping a strategic distance from the RREQ packet duplication problem.
Kritika Sood et al. (2013) [5] have investigated several clustering methods in a mobile ad hoc network the clustering method describes the unique features of MANETs and organizes their structure in a hierarchical way. Clustering problems, such as cluster structure stability, control overhead, and energy consumption maintenance of mobile nodes, have been investigated. These problems have been investigated using different cluster-related statuses and traffic load distribution in clusters in order to behave as a cluster head. However, no steps are being done to improve data security.
(Ramanna Havinal, et al. 2016) [6] suggested an energy-efficient MANET routing system based on advanced graph theory this concept generated a debate regarding an actor, namely zone availability for data transfer. This paradigm provides a clear perspective on the network model and leads to an efficient routing strategy that ensures energy efficiency.
Sunil Pathak & Sonal Jain (2016) [7] has created a Weight Based Clustering technique for efficient MANET routing. For creating cluster and cluster head in WBC, two variables, namely node degree and bandwidth requirements, were taken into account. The WBC procedure joins two clusters that are close together to form a single cluster. When there are two cluster heads, one cluster drops out and the other takes up the job. For connecting the two clusters, an enhanced cluster maintenance method was used. This results in reducing the process of cluster changing

(Shivashankar, et al. 2014) [8] By improving the current DSR protocol, we presented a power-aware routing method. The protocol chooses the most energy-efficient routes for routing, which minimizes the energy used per data packet, increases network lifespan, and lowers node costs.

Xiang et al. (2011) [9] Efficient Geographic Multicast Protocol has been introduced (EGMP). To provide effective membership management and multicast delivery, an EGMP network-wide zone-based bidirectional tree has been developed. Then, based on the location information, zone structure construction, multicast tree construction, and multicast packet forwarding have been guided. The usage of zone depth has aided in improving the efficiency of the routing protocol, while the use of zone structure has helped to manage the empty zone issue. EGMP reduces routing costs and latency while increasing data packet delivery.

III. ESMCH SYSTEM MODEL

This method has divided the nodes into several clusters, such that each node belongs to more than one. Concentrate on a single cluster of m or n nodes. All of the data in the cluster nodes that are not aware of each other's data should be aggregated (including the aggregator). The aggregated data may be obtained from any source. Two nodes may be used to provide a single-hop or multi-hop network connection path for an overlay.

The sensitive specifics of the node (e.g., age, location, earnings, etc.) are best left until the initial state. However, when the number of nodes on the network is large, aggregated data only contains all node figures. Consider real-time meters that gather energy usage for management reasons as an example of the benefit of how smart meters help to service controls.

3.1 DATA AGGREGATION

More nodes in a network imply more anonymity, but also more complicated node monitoring: Use two keys to avoid detection while looking for problematic nodes. The condition of the first node is half of its dimension, and it is transmitted to two of two others. Extra noises are created throughout this procedure to be incorporated into the original condition for the privacy of the house. For a moment, consider developing rules for nodes to monitor and discourage misbehavior. It is used to monitor immoral nodes and improve aggregation accuracy.

3.2 Neighbor Monitoring

When a new neighbor is found, this method asks an available node to keep an eye on it. A node near node j searches for information using the three criteria listed below: based on the information that is currently available the update is a routine procedure, and the noise decreases dramatically as the process progresses. In c2, node states are restricted to

guarantee that they remain true, keeping each part of the network honest, while in c3, node states are approximated to preserve the original form of the other isolated Node created as shown in figure 2.

Two adjacent sets of data are required to guarantee that the deceiving node can identify the changing values of its noise process.

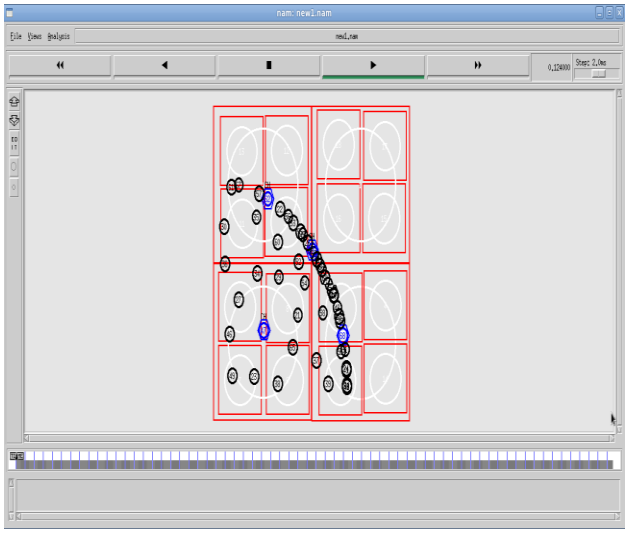


Figure 2: Node creation.

Figure 2 shows Creation 0-70 nodes using NS2 Simulator for data transfer.

3.3 Energy Aware Path Selection

The utilization of energy is predetermined (in the sense that the maximum energy level that can be used is specified beforehand). With RREQ, the usual scenario is that the node's useable power exceeds the required power. A malicious cluster head that is both efficient and secure (ESMCH) for an effective adversarial usage model, many attack sites have been proposed. Selecting for neighbor node is illustrated **as** figure 3. On the node, the transport protocol is forwarded via a variety of ways. Assume that improvement is desired; therefore it is suggested as an improvement. The path between nodes is determined by multiplying a formula factor by the number of nodes to provide a useful route between them. This element's impact is determined by the routes and hops' expiry dates. To improve network lifespan, the authors chose the route with fewer hops and more resources in the comparison. The intermediate nodes are chosen based on the degree of originality in the method that has been proposed. The extended- selection stage is the last step of route collecting, and hop count is one of two components of the route's lifespan.

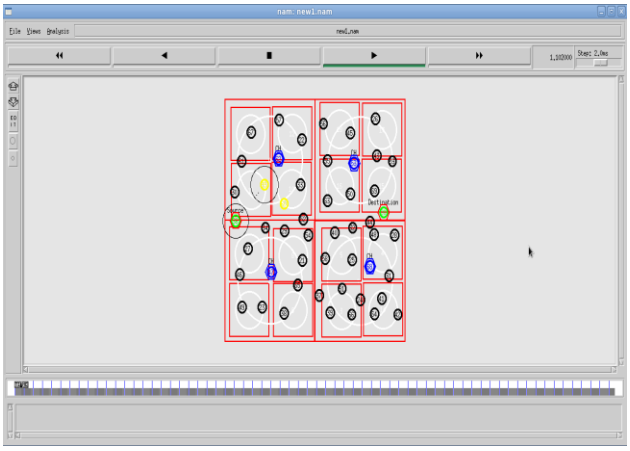


Figure 3: Selecting neighbor node.

As shown in Figure 3 shows selecting neighbor nodes for data transfer from source to destination The source and destination is mentioned in green color and cluster head is mentioned as blue color. The black color indicates as normal node and yellow color is mentioned as neighbor node checking. Finally the malicious node is represented by blue color as shown in figure 7.

3.4 REACTIVE ROUTING

Based on the signal strength received from the sender, estimate the propagation area surrounding each node. These zones are known as the inner, middle, and exterior regions. This categorizes the packets. The network topology of MANETs is complicated due to the movement of nodes. The proposed routing flow diagram is mentioned in figure 6**.** To address this issue, avoid using outside nodes; since this will assist prevent network partitioning by identifying which nodes are critical to the overall system. To reduce search engine latency, the inner zones inside acquired signal intensity values may be ignored; it refers to middle nodes, which implies concentrating on nodes here. Choose the lower and higher ranges of the computed single-strength limitations to balance the number of utilized single-strength nodes between the inner and outside areas.

The Route Reply packet (RREP) is sent by the node; the ROUTE with the greatest RPS value is transmitted along the route with the highest energy. There is a route in the routing table's destination table. It computes the average value and compares it to a previously saved value. Acceptance is granted if the new RREQ value is larger than the old RREP. Otherwise, it will be returned. When a backup route is discovered, the source node may store a duplicate of it in memory in case of disaster. The path selection is shown in figure 4.

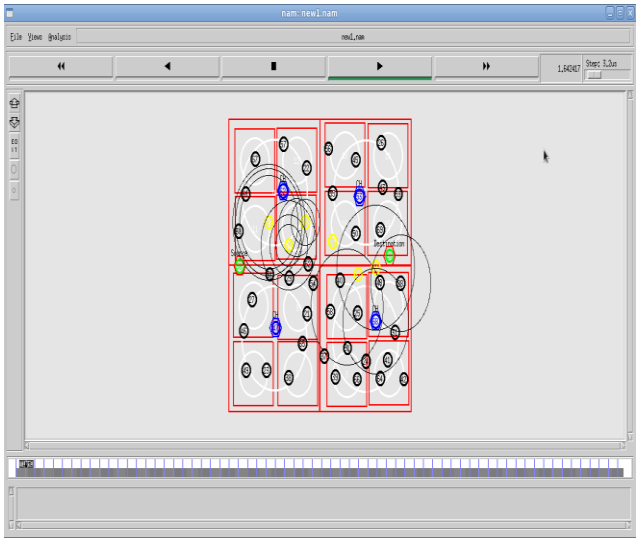


Figure 4: Selecting primary path.

As shown in Figure 4 shows selecting primary path for data transfer from source to destination.

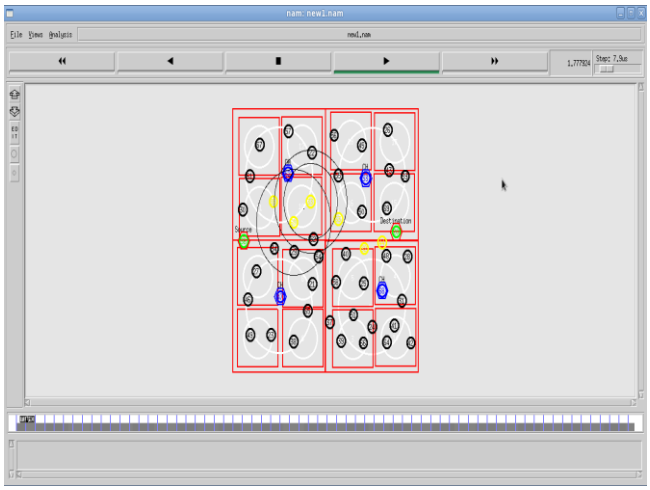
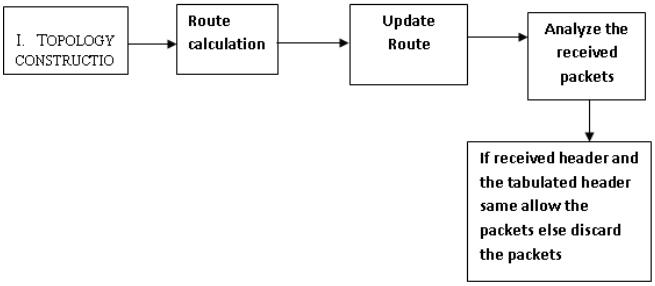


Figure 5: data communication.

Figure 5 shows data communication from node to node in cluster head 1.

3.5 RECEIVED SIGNAL STRENGTH

Residual power is allocated to the middle nodes and the bottom ones throughout the network routing operation. When a route request reaches the intermediate node, the energy calculated for the direction is stored in the routing table. Then it waits for some time of time T to prepare for all requests to be sent to arrive before acting. If the new path's average energy is greater than the old one, the new node is rejected. As the amount of Time passes, the node can apply the N Residual Energy to the RREQ. In path exploration, the middle-value threshold values will be expanded by evaluating the requested RREQ values' average path length; the dynamic delay is applied to the active hop count and communication is denoted as figure 5. The delay values depend on the path's average energy. The total energy of the route tends to decrease as the delay period increases. Nodes that are close to the sender can reduce the packet transit time. Traditionally, an arbitrarily delayed in AODV; however, the latency computation has been refined in Sites.



System 6 Flow Diagram for Route optimization

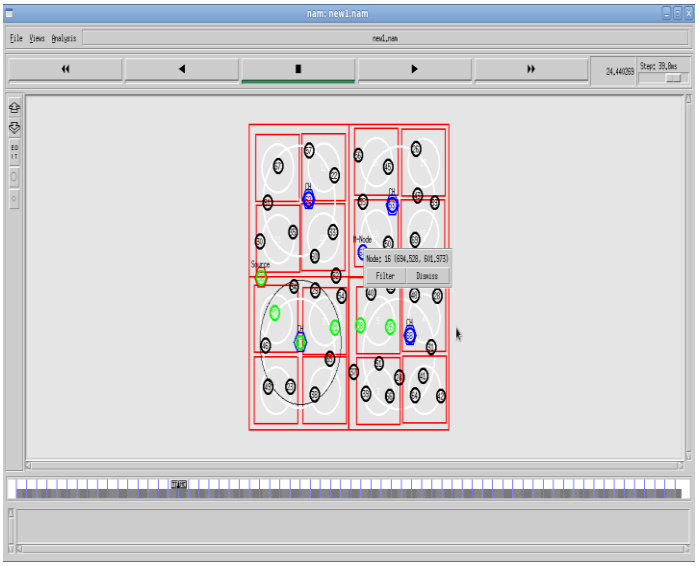


Figure 7: Identified malicious node

Figure 7 shows node 16 is identified as malicious node in cluster head 2.

Algorithm 1: Neighbor Node Selection algorithm

1. Identify the neighbors of every node v (that is to say, the nodes inside its transmission range). This provides the node's degree d_v.
2. Calculate the running average of the speed for each node. This provides the quantity of mobility and is signified by Mv.
3. For each node, calculate the summation of the distance

$$dv = \sum \sqrt{((x_2 - x_1)^2 + (y_2 - y_1)^2)}$$

$$D_v = d_v - M_v$$

4. Calculate the degree-difference Dv For each node v, here dv is known as the node degree of every node, and Mv is called the mobility where node goes arbitrarily.
5. Calculate the Time, Tv, of a node v for the duration of which it plays as a cluster head. Tv specifies the battery power utilized.
It is presumed that battery power utilization is high for a cluster head compared to an ordinary node and produced arbitrarily.
6. Compute a combined weight For every node v. the coefficients C1, C2, C3, C4 are the weighing factors for the related system parameters.
7. Select the node with a minimum Iv to be the cluster head. Every neighbor of the selected cluster head could no longer take part in the election algorithm.
8. Do again Steps 2 to 7 for the residual nodes in a cluster

Algorithm 2: ESMCH Data Forwarding:

Require Packet output from the upper layer.
Ensure: Packets inserted to MAC queue.
Get group list N from the group table
for node n in group list N do
for multicast region r in 4 quadrants regions R do
if n 2 r, then
Add n into r.list
end if
end for
end for
for r € R do
if *r.list* is non-empty then
Duplicate a new packet p
Add ESMCH header (TTL, checksum,r.list)to p
Insert *p* to MAC queue
end if
end for

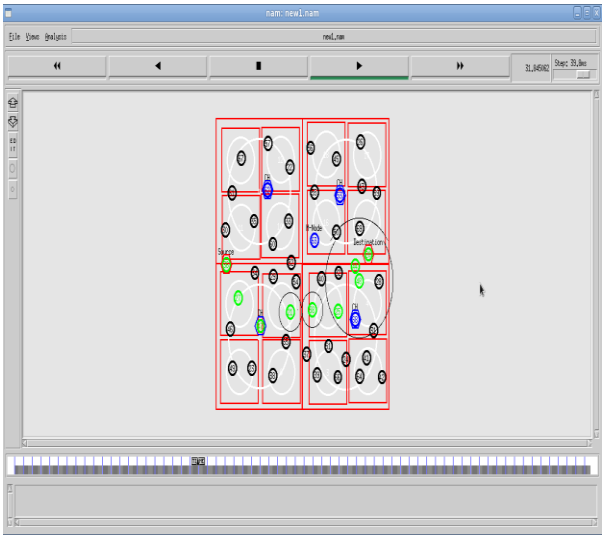


Figure 8: data transfer.

Figure 8 shows data transferring on the secondary path.

Cluster head security mechanisms first scan the packet's header to see whether the checksum is correct before accepting it. Whether it's not in the delivery field, it loses the envelope. Within the radio range, the forwarding zone is closer to the sender than the destination. The malicious node is identified as shown in figure 7.

Once a node detects a forged malicious packet, it looks up the collection of destinations in the ESMCH header. If this is inside the array, it strips the lower layers' packages and transfers them to the following protocol. If the TTL is less than 0, it lowers the packet. If there are no malicious subdomains or virtual nodes in the destination list, then the safe cluster nodes and virtual cluster node lists are restored. Otherwise, malicious nodes and virtual nodes are measured, and new packets are created. The individual packages are then sent to the MAC queue (for each of which is a malicious cluster member head region). Finally the data transferring is shown in figure 8.

ESMCH Data receiving algorithm:

Require: Packet input from the lower layer
Ensure: Forwarded packets inserted to MAC queue
Calculate checksum. Drop packet if error detected
Drop packet if not in Forwarding zone
Get destination list D from the packet header
for node d in destination list D do
if I am *d* then
Duplicate the packet and input it to the upper layer
Remove d from list D
end if
end for
if TTL in header = 0 then
Drop the packet
return
end if
for d € D do
for secure malicious cluster head region r in 4 quadrants regions R do
if d € r then
Add d into r.list
end if
end for
end for
for r € R do
if r.list is non-empty then
Duplicate a new packet p
Add ESMCH header (TTL - 1, checksum; r.list)to p
Insert p to MAC queue

end if
end for

IV. RESULTS AND DISCUSSION

The Existing model is ESMR- Energy-aware and Secure Multi hope Routing, and the proposed model is ESMCH- Efficient Secure Malicious Cluster Head. The below figures show a comparison of the ESMR method and ESMCH model in NS2.

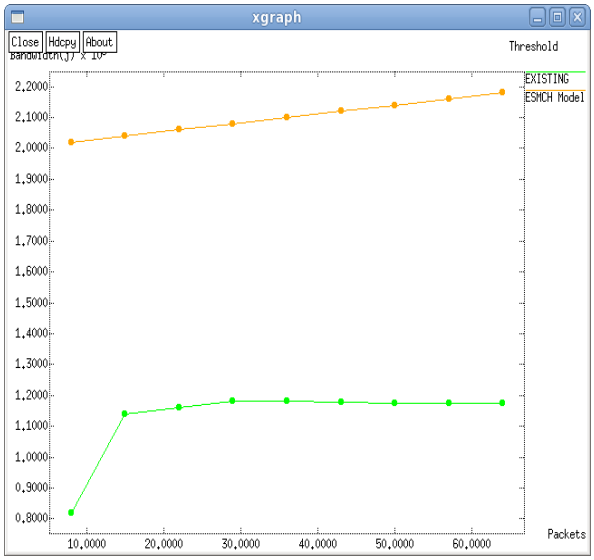


Figure 9: Comparing Threshold in Existing model and ESMCH model.

Figure 9 shows comparing threshold values in the Existing model ESMR model and ESMCH model. In this figure, the x-axis represents packets, and the y-axis represents bandwidth.

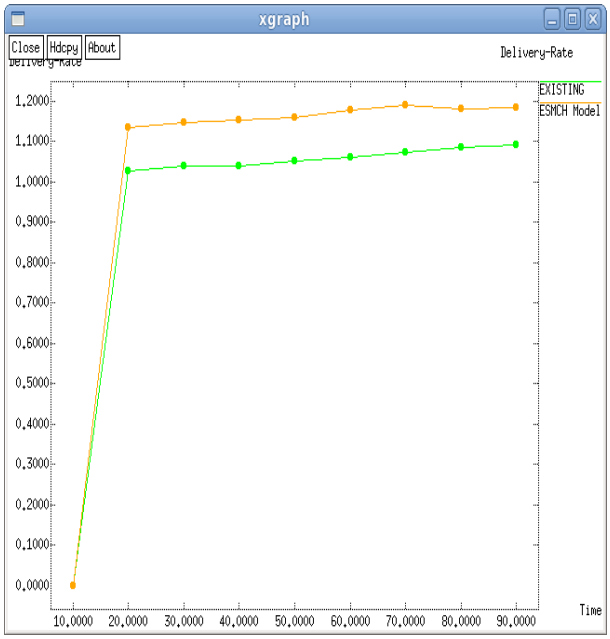


Figure 10: Comparing Delivery-Rate.

Figure 10 compares the delivery rate in the Existing model and the ESMCH model. In this figure, X-axis represents the Time, and Y-axis represents the Delivery rate.

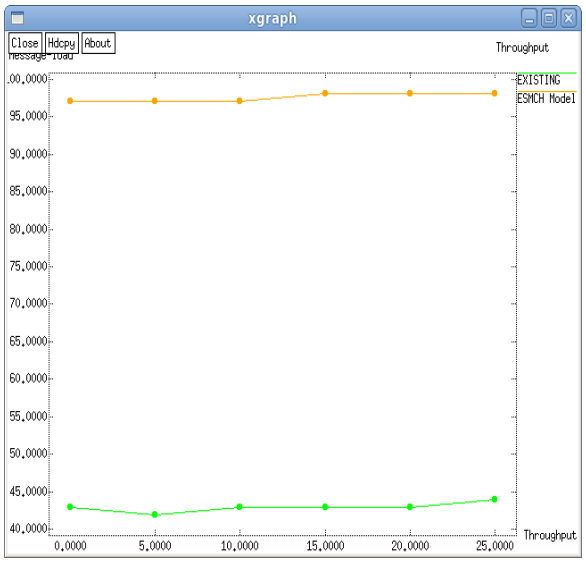


Figure 11: Throughput comparison.

Figure 11 shows a comparison of throughput in the Existing model and ESMCH model. The X-axis represents throughput, and Y-axis represents Message Load.

Figure 12: Energy comparison.

Figure 12 compares the Energy in Existing model and ESMCH model. The X-axis represents Delay, and Y-axis represents energy.

Figure 13: Attack detection.

Figure 13 shows Attack detection in the Existing model and ESMCH Model. The X-axis represents Time, and Y-axis represents detection rate.

V. CONCLUSION

There are several protocols available today that choose cluster heads based on a variety of characteristics, mostly energy, as well as other factors such as random selection of weight or priority parameters, which may result in network loss or reduction in network life time. There may be a variety of causes for these losses, such as inappropriate and unbalanced energy use, or nodes becoming dead or energy-depleted at any point of the network. The old algorithm did not take network security into account. The node's status was not verified prior to data transfer. The attacker node is located using the node status, and before selecting the cluster head, it is determined if the node is trustworthy or not. So, in this suggested work, a new protocol ESMCH is presented, in which the node state is specified, as well as characteristics such as energy and bandwidth. The results and assessment indicate that our method is more efficient and requires the least amount of resources for cluster head selection. The MANET lifespan is extended significantly with the assistance of our suggested protocol. We also test our method in many situations with varying data rates for critical assessment and fair cluster head.

REFERENCES

[1] Anubhuti Roda Mohindra, Charu Kumar, 2013, "A Stable Energy- Efficient Location-Based Clustering Scheme for Ad Hoc Networks", Quality, Reliability, Security and Robustness in Heterogeneous Networks, Springer, vol. 115, pp. 75-85

[2] Chand, KK, Bharati, PV & Ramanjaneyulu, BS 2012, 'Optimized energy efficient routing protocol for lifetime improvement in wireless sensor networks', Proc. Int. Conf. Adv. Eng., Sci. Manage. (ICAESM), pp. 345-349.

[3] Drugan, OV, Plagemann, T & Munthe Kaas, E 2015, 'Dynamic clustering in Sparse MANET', Computer Communications, Elsevier, vol. 59, pp. 84-97.

[4] Guruswamy, Madhumita Chatterjee," A Novel Efficient Rebroadcast Protocol for Minimizing Routing Overhead in Mobile AdHoc Networks", International Journal of Computer Networks and Applications (IJCNA), Vol. 3, Issue 2, March – April 2016.

[5] Kritika Sood & Anuj, K, Gupta 2013, 'A Survey on Load Balanced Clustering Algorithms', International Journal of Innovative Technology and Exploring Engineering , vol. 2, no. 5, pp. 50-56.

[6] Ramanna Havinal, Girish V. Attimarad, M. N. Giri Prasad, 2016, "MECOR: Minimal Energy Consumption with Optimized Routing in MANET", Wireless Personal Communications, pp. 1-21

[7] Sunil Pathak & Sonal Jain 2016, 'A novel weight based clustering algorithm for routing in MANET', Wireless Networks, Springer, vol. 22, no. 8, pp. 2695-2704.

[8] Shivashankar, G. Varaprasad , S. H. Narayanagowda, 2014, "Implementing a new power aware routing algorithm based on existing dynamic source routing protocol for mobile ad hoc networks", IET Networks, vol. 3, no. 2, pp. 137 – 142

[9] Xiang, X, Wang, X & Yang, Y 2011, 'Supporting Efficient and Scalable Multicasting Over Mobile Ad hoc Networks', IEEE Transactions on Mobile Computing, vol. 10, no. 5, pp. 544-559.

[10] Zhaowen Xing, L. Gruenwald and K. Phang, 2010, "A Robust Clustering Algorithm for Mobile Ad-hoc Networks", Handbook of Research on Next Generation Networks and Ubiquitous Computing, Editor Samuel Pierre, IGI Global.