A Hybrid Cluster based Multicast Routing Approach for detecting active attacks in MANET

Dr. N. Suma[1], Dr.N.Shanmuga Vadivu [2], Dr.L. Jubair Ahmed[3] , Mr. S. Mukunthan[4], Ms. M. Sathia Priya[5]

[1,5] Department of ECE, Karpagam Institute of Technology, Tamilnadu, India.
[2]Department of ECE, RVS College of Engineering and Technology, Tamilnadu, India.
[3]Department of ECE, Akshaya College of Engineering and Technology, Tamilnadu, India.
[4]Department of ECE, Dhanalakshmi Srinvasan College of Engineering, Tamilnadu, India.

[1]suma.ece@karpagamtech.ac.in

Abstract *- Mobile Ad hoc Network (MANET) is one of the wireless networks where the access point is not present. Due to absence of administrator, the nodes may be comprised by the attackers. In the presence of active attackers, network may be damaged and out of connectivity. In the absence of passive attackers, information about the network may be disclosed to unauthorized agent. Compared to passive attackers, active attackers are most vulnerable to network. To detect and avoid this attacker, there is a need of reliable routing and intrusion detection system. In this work, Hybrid Cluster based Multicast Routing Approach (HCMRA) is introduced and implemented to detect and isolate the malicious attackers i.e. active attackers. In first stage, optimal path is identified through metrics of path to smooth packet delivery. In second stage, cluster is formed and cluster head is chosen based on energy and stability. Here sub CH is maintained to monitor routing, energy conservation etc. In third stage, trust aware routing is established in cluster region to identify the attackers based on reliability value. The work is simulated with various parameters like path reliability rate, end to end delay, packet delivery ratio, control overhead and energy efficiency.*

Keywords - Malicious node detection, optimal path discovery, trust aware routing, cluster formation and cluster head election.

1. Introduction

Nowadays nodes are connected in wireless scenarios. The replacement of cabling was done in 20 years back and communicating via signals. In the presence of access point, node can be easily tracked and identify any issues in the network. Mobile ad hoc network is a special kind of network where it was first launched in military applications. It contains wireless mobile nodes without access point. Due to that, node may be easily comprised by the attackers and attack the network communication. It may lead to network dis-connectivity.

To overcome such issues, nodes must be controlled through trust routing and reliable path maintenance schemes. To withstand attackers, several schemes were developed to protect the data and ensure effective transmission. In some cases, the enhanced on demand routing [1] was developed to isolate attacks in the network. Here authors implemented two algorithms which are used to detect the attacks and monitor the routing performance. In first algorithm, the flood based routing is implemented to monitor the congestion through attackers and each node stores route request made by the intermediate nodes, and record it in the routing table. If any node floods the unlimited route requests or duplicate packets it will be discarded from the network. Based on threshold vector, the activity of routes was monitored and isolates the malicious nodes. Security model [2] using triple factor algorithm was used to improve packet arrival rate and defend against malicious attacks. Here nodes are having mobility and goes out of the zone. Due to absence of administrator, nodes may be comprised as misbehaving nodes. Cryptographic routing mechanism was implemented to balance data integrity and delivery ratio. Secure transmission path was built to defend against black hole attackers. In some scenario, the concept of Swarm based MAC layer routing protocol [3] to improve the energy efficiency through priority scheduling approach. The secured lazy processing model was used to identify and isolate the malicious nodes. The on demand protocol was modified to support security and protect nodes against attackers. Ant colony optimization model was used to ensure secure routing and increase the network throughput. The concept of weight based coding approach [4] was introduced to isolate the malicious attacks in VANET. In active attacks, the wormhole attacks are the vulnerable and difficult to detect. The route analysis and round trip time was used to detect the attacks and instruct the nodes to check the identity of packets and duplication before transmission. The delay was reduced due to maintenance of round trip time and path.

2. Literature Review

In [5], author introduced the high performance intrusion detection scheme for detecting black hole and gray hole attacks. The information about the identified nodes was recorded in the routing table of source node. The concept of connected domain set was used to balance energy and trust in the network. The nearby connected domain sets were identified through localization model. The information about packet forwarding was retrieved at source node to secure node against attackers.

In [6], reliable on demand routing protocol was adopted to ensure network integrity in the network. Here the route contains energy factor, reliability value and authentication management in the network. Nodes were aware of reliable routes and forward the packets through reliable neighbor nodes. In each transmission process, threshold vector is maintained to detect and isolate the attackers. Route reliability was improved using message digest algorithm to ensure data transmission between source and sink node. The pause time was increased to identify the malicious activity present in the network.

In [7] author introduced the acknowledgement based approach for identifying wormhole attacks in the network. The issue of tunnelling approach due to the attackers make packet grasping in one location and drops in another location. In route reply phase, the packet collision may be produced in the intermediate phase. The approach was simulated using advanced network simulator tool and analysed through QoS metrics.

In [8], author explored the trust factor model and swarm optimization routing to ensure secure routing in the network. The concept of fuzzy model was used to make system as decision model to ensure reliable routing. Only secure paths are chosen for packet forwarding instead of shortest path to protect packets from attackers. The secured paths were identified through trust factor model. Optimal paths were found using optimization technique. The path with high reliability value was identified as secure path for packet forwarding. The detection rate was improved to reduce delay and overhead through secure routing mechanism.

In [9] author implemented enhanced trust aware routing algorithm to balance energy and reliability in the network. The on demand routing protocol was adopted to support routing to produce minimum overhead and delay. Reliable routes were used to increase the energy efficiency during sleep mode. The network performance was improved and compared with existing works periodically.

In [10] author implemented enhanced trust aware routing algorithm to balance energy and reliability in the network. The on demand routing protocol was adopted to support routing to produce minimum overhead and delay. Reliable routes were used to increase the energy efficiency during sleep mode. The network performance was improved and compared with existing works periodically.

In [11], the secured on demand routing protocol was used to avoid black hole attack and denial of service attack. The route hop count was increased due to the presence of malicious node. Route request packets were used to support network stability through reliable and secure data transmission. Based on secured crypto routing, the vulnerability of attackers was reduced to improve data throughput.

In [12], author explored the identification system for detecting and isolating the misbehaving node in VANET. The reliable paths were found for effective data transmission. In route maintenance, the history of routing in source routing table was recorded and analyzed to choose the primary path as reliable path. Least packet dropping rate and less delay was the key parameters to choose the reliable node. The key management system was deployed to manage the key for ensuring data protection.

In [12], reliable and stable multi-hop routing protocol was introduced to improve the path reliability and stability for packet transmission. Every source node forwards packet to neighbour node in least hop fashion based on location information of nodes. Here two metrics were considered i.e sink node selection and weight node connectivity to obtain stable route from source to sink node. The concept of self-chosen was adopted to reduce the control overhead in network congestion period.

In [13], safe routing approach was introduced to identify and listen the attackers who make packet dropping during data transmission period. In route discovery process, the approach was able to find the dropping rate. In order to defend the attackers, recognition system was implemented for protecting the properties of controller network. The advised approach was used to examine the nearby attackers and forwards to reliable node through secured path. Based on packet arrival rate, the path will be chosen as primary on for routing the packets based on strength metric of node to improve network lifetime and reduce overhead.

In[14]. Optimal route selection approach was implemented to choose best routes with least hop and minimum energy consumption. This is to ensure the failure of routes and to extend the network lifetime. Optimal cluster head was chosen to ensure reliability in the network and to improve the packet arrival rate. The multicast routes were discovered to ensure the quality of service and reduce the transmission cost in the network. Optimal paths were identified depends on the node energy, number of hops and reliability factor.

In [15], the concept of reliability antecedent packet forwarding approach was deployed to implement reliable route between source and sink node. In this method, flooding nodes are avoided. The existing communication is stored if the interference is present in communication time. The advanced path mechanism is designed to provide interference free routes to track the flow of packets and delivery at sink node. Due to the store routing concept, the data lost can be avoided and breakdowns can be easily dropped as well as solution can be provided immediately.

In [16], secure routing mechanism was implemented with least energy conservation to provide high data security and less energy consumption. The proposed scheme was categorized into two major approaches. In the first approach, the cluster head was found, and in second approach, reliable routes were identified for secure communication. Through packet forwarding information, the reliable value was computed to identify and remove the malicious nodes.

In [17], the trust model was formed based on cluster structure and reliability based model secure routing. The efficiency of node reliability determination was improved using hierarchical cluster structure. There were two nodes maintained in the network i.e. reliable agent node and reliable management node to manage node dependability with high confidentiality. Reliability based routing was adopted to manage reliability, and safe route, and data transmission.

In [18], fuzzy based zone routing protocol was presented to choose the optimal value of zone radius. Here the zone radius was obtained based on residual energy and node mobility. The radius value of zone was tuned to provide high network lifetime and less delay based on remaining energy and overhead. Here the node was automatically adapted to meet the network conditions. The approach was analyzed with various mobility models.

In [19], Mobility-Based Optimized Multipath Routing Protocol was introduced to minimize link failure and improve the QoS performance. It was also used for ensuring efficient route discovery and maintenance process to avoid traffic nodes and idle nodes. The latency was also reduced to extend the network lifetime. Each node has a right to assess the many routes for packet forwarding. The address of the sink was discovered based on neighbor node discovery. The scalable and efficient data transmission was ensured to improve the performance of QoS.

In [20], the selfish node aware reliable and optimized cluster routing was adopted to improve cluster reliability. Authentication mechanism was used to authenticate node and detect misbehaving nodes. The attacks are isolated through effective authentication model. The optimal cluster nodes were identified and used for ensuring packet delivery at sink node.

The work is categorized into five sections. In first section, introduction about MANET and detection of attackers is given. In second section, various detection schemes, trust mechanisms and reliable routing approaches were discussed. In third section, the proposed work is illustrated and justified through trust model. In fourth section, simulation results are provided with discussion. In final section, conclusion and future work is given to justify the proposed work and extension of trust model in future work.

3. Materials and Methods

In this phase, the cluster formation is initialized to select the Cluster Head (CH) and optimal routes were identified using Path finding mechanism. The proposed work consists of three stages. In first stage, optimal path is discovered to support cluster mechanism. In second stage, cluster is formed and CH is elected based on energy metric, reliability metric and communication cost among the nodes. In third stage, detection of malicious node is done to ensure malicious free network. The stages are described as below.

3.1.1 Optimal Path Finding stage

The optimal path is determined based on various metrics i.e. path energy, path capacity and path reliability. The methodology was suggested to choose optimal paths based on maximum remaining energy and least hop between the nodes. It is not required to choose the path using specific approach if various approaches were used. The optimal path is discovered based on high energy of path, capacity and reliability. The optimized multiple paths are located based on high remaining energy. If the path is broken or failure, alternative path will be chosen for packet transmission. The computation time was also reduced using the algorithm.

The algorithm focuses on selecting the congestion free route and traffic reduction. The path chosen is accomplished by considering the minimum residual energy available in the path. There are two major metrics considered to ensure congestion free optimal route i.e. sequence number of cluster member and packet transmission ID. The proposed path find approach is used to ensure an original and reliable route based on response rate, delivery rate, jitter and path tolerance rate.

The round trip time RT_{τ} is evaluated based on consuming time for sending packets and receiving corresponding acknowledgements. It is calculated as,

$$RT_{\tau} = RT_{pr} + BER_{\tau}$$

where RT_{pr} is round trip time with propagating transmission data rate and BER_{τ} indicates bit error rate with respect to time.

If there is any modification in path time, the data transmission rate DTR is measured as,

$$DTR = \frac{\Delta AR}{\tau}$$

where *AR* refers to arrival rate and τ indicates time. *AR* should be less than threshold value and τ should be greater than exact arrival rate.

The path reliability is based on packet delivery rate and maintaining the data confidentiality.

Algorithm 1 : Optimal path finding

```
Step 1: CH sends a Route Request (CH_RREQ) to cluster members. CH_RREQ contains packet ID, sink address, source address, hop count, sequence number, path reliability (pR), path capacity (pC) and path energy (pE).
Step 2: pE is updated if the energy level of node is greater than current pE; otherwise pE is maintained as constant.
Step 3: Keep monitoring until CH_RREQ reaches its final target value
Step 4: Energy efficient route is chosen based on various CH_RREQ collected from various paths.
Step 5: If (pE=high, pC= high, pR=high && path hop_count=low), choose the optimal path
Step 6: Sink node send CH_RREP to join the path
Step 7: Packet is sent through newly discovered path.
```

Algorithm 2: Packet transmission through Optimal Path

```
Step1: Deploy node randomly in the network.
Step 2: Discover optimal path to sink node
Step 3: Collect the geographical position of node based on node ID
Step 4: Determine the distance between nodes
Distance = $\sqrt{((x1-x1)^2+(y1-y1)^2)}$
Step 5: Choose the high reliable path based on
$R_p = \min(\{pR, pE, pC \mid M_i, M_j \in Q, M_i \rightarrow M_j\})$S
tep 6: If (distance<coverage region)
  {
     Choose the optimal path to forward packets
  }
End
```

3.1.2 Cluster Head Election Algorithm

In this algorithm, cluster is formed based on node centrality, node stability and high residual energy nodes (N_r). The node centrality (N_c) is used to ensure the communication capacity between hub and neighbor nodes. Node stability (N_s) is determined based on capability of node to receive packets and forward to neighbors without dropping many packets. High residual energy nodes are chosen to ensure more network lifetime. Here the cluster head is elected based on reliability metric and node's residual energy. If the node has good stability, high residual energy and centrality, it will be chosen as CH. In such case, the other following nodes are taken as alternative CH. In high mobility cases, two CHs are basically deployed. If the primary CH is failed, the secondary CH will be automatically chosen for packet forwarding and monitoring the packet transmission in the cluster region. CH backups the routing history of previous data transmission and forward the packet to neighbor CH which is located in the nearby cluster region. The cluster head election algorithm is given below. It is used to improve the network lifetime and reduce the time delay for packet transmission from CH to CM or CM to CH.

Algorithm 3: Cluster Head Selection Algorithm

```
Step1: Find CH among nodes based on $N_c$, $N_s$ and $N_r$
Step 2: Broadcast packets to cluster members and it joins by replying CH_RREP
Step 3: Determine node centrality and choose the primary CH.
Step 4: Choose the alternate CH based on calculation of CM<ACH<CH
Step 5: When primary CH fails, alternate CH maintains energy of cluster members, distance and node reliability metric
Step 6: Forward the packets from primary CH to cluster members through optimal path based on available energy of node and least hop distance between nodes.
```

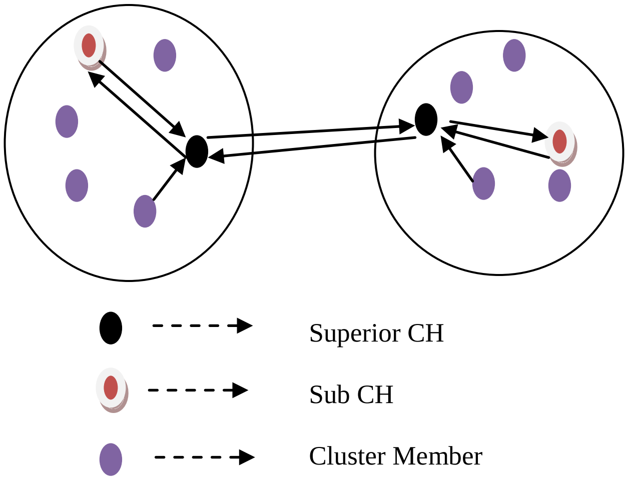

Figure 1. Cluster formation and cluster head election

In Figure 1, the cluster formation and selection of cluster head is illustrated. If primary CH i.e. superior CH is failed, sub CH will be chosen as primary one.

3.1.3 Reliable system for malicious node

detection system

In this stage, malicious node is identified by tracking a node when it becomes a director intermediate node of any node present in the network. The reliable vector is calculated based on packet dropping rate (PDR) and node energy (nE). The value of threshold reliable vector is 0.8. If any node goes below the threshold reliable vector, it will be marked as malicious node and it will be immediately isolated from the network.

Let $\{Rv_1, Rv_2\ldots\}$ be the reliable vectors of the cluster members $\{CM_1, CM_2\ldots\}$ along the optimal path OP1 from CH to CM.

At initial stage, cluster member does not contain reliability of neighbor node. CH forwards the packets to sink CM or CH then it will send a reply to source through optimal path and verified its digital signature. The digital signature of node is verified through its ID and its sequence number by source CH. When source CH verifies digital signature of all nodes and it becomes successful, reliable vector is increased to 1 or else it will be decremented. It is given as below

$Rv_k= Rv_k+1$

Or if the verification is failure then,

$Rv_k= Rv_k-1$

If energy of node is get depleted due to packet dropping, then the node will be marked as malicious node. Residual energy of node is go out of the threshold value, then the node is considered as misbehaving node. The reliable vector includes node residual energy and node stability. For any node or CM, if it falls below the threshold value, it is identified as malicious node and it will be isolated from participating in the network.

3.1.4 Packet format

Superior CH ID	Sub CH ID	Hop count	Path reliability	CRC
2	2	1	2	2

Figure 2. Proposed packet format

In figure 2, the packet format of proposed work is shown. First two fields occupied by superior CH and Sub CH. Third field is Hop Count that occupies 1 byte. Path reliability is the fourth field of packet format and it occupies 2 bytes. Last field is the Cyclic Redundancy Check used for error detection and correction.

4. Results and Discussion

In The work is simulated using Network Simulator tool (NS2.34). The language used in the tool is C++ and Tool Command Language (TCL). The basic routing protocol used is Dynamic Source Routing (DSR) which is a reactive protocol that provides less overhead and high energy efficiency. Table 1 shows the simulation parameters of proposed work.

Table 1. Simulation settings

No. of mobile nodes	300
Setup Area	1200 X 1200 m^2
Mac	802.11
Radio Range	250 m
Pause time	100 sec
Traffic Source	CBR
Packet Size	64 bytes
Mobility Model	Random way
Protocol	DSR

Parameters:

Energy Efficiency: It is the ratio of energy consumed to the total energy supplied. It should be kept high.

End to end delay: It is the delay consumed for packet transmission from source to destination.

Control Overhead: It the excessive of packets traveling in the path. It should be kept low.

Path reliability rate: It is the rate at which number of reliable paths to the total number of paths available in the network.

Packet delivery ratio: It is the ratio of packets arrived at sink to number of packets sent during route maintenance.

Detection efficiency: It is the accuracy for detecting malicious node to the total number of nodes present in the network.

Figure 3 illustrates the analysis of packet delivery ratio. From the graph, the proposed work HCMRA provides high packet delivery ratio 95-59% than existing schemes due to the presence of reliable path selection and cluster head election.

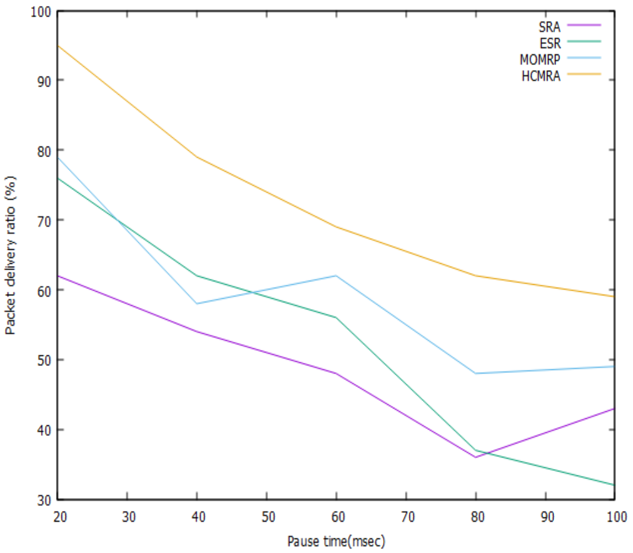

Figure 3. Packet delivery ratio Vs Pause time

Figure 4 shows the performance of end to end delay for proposed and existing works. It seems that HCMRA consumes less delay 4.8-10.1 msecs due to trust aware routing. Trust threshold vector allows node to consumes less delay for packet transmission.

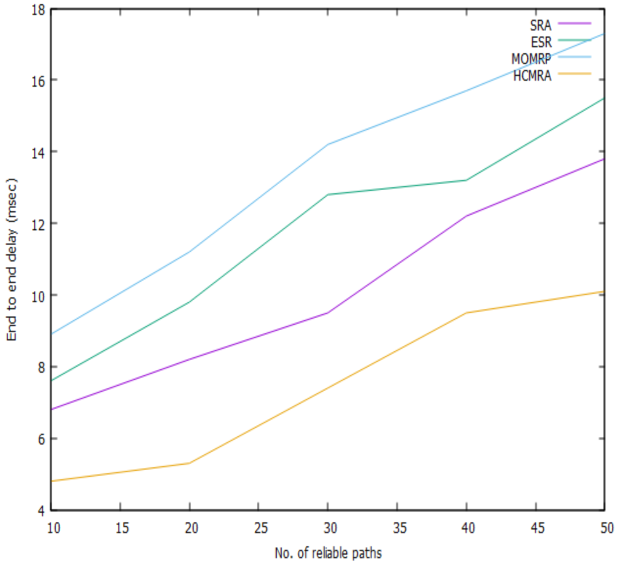

Figure 4. End to end delay Vs No of reliable paths

Figure 5 illustrates the performance of path reliability ratio. It is seen that HCMRA achieves high path reliability rate (19-192) packets/sec than existing schemes. It is because of selection of optimal path and trust enhanced routing scheme. While varying pause time, the HCMRA produces high ratio than existing schemes.

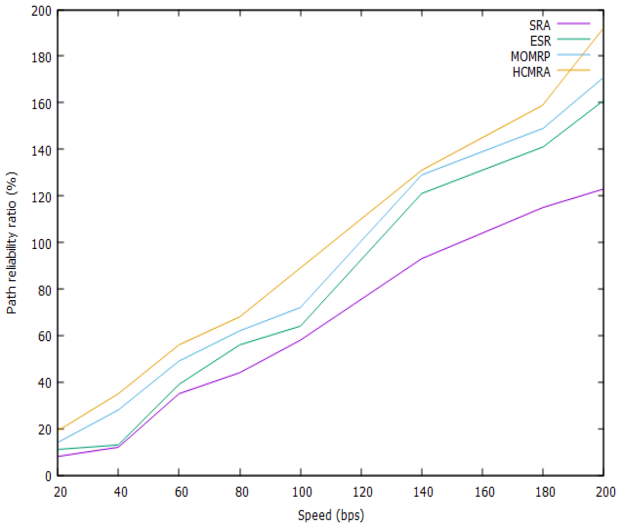

Figure 5. Path reliability rate Vs Speed

Figure 6 show the performance of control overhead for proposed and existing work. From the analysis, the proposed work HCMRA has less overhead (10.8-5.6) packets than existing schemes. It is because of trust aware routing and cluster management scheme.

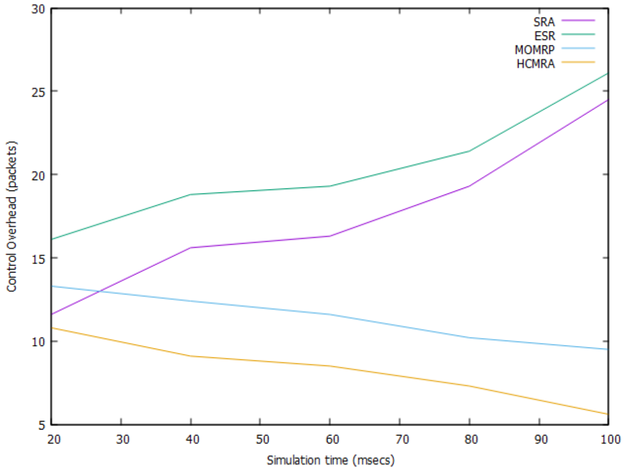

Figure 6. Control Overhead Vs No. of Nodes

Figure 7 illustrates the performance of energy efficiency 24.4 – 15.7 joules of proposed and existing schemes. The proposed work consumes less energy due to the presence of trust aware routing and cluster management scheme.

Figure 8 shows the detection efficiency of malicious nodes for proposed and existing work comparison. HCMRA achieves 94-78% efficiency than existing works due to the implementation of trust aware routing scheme.

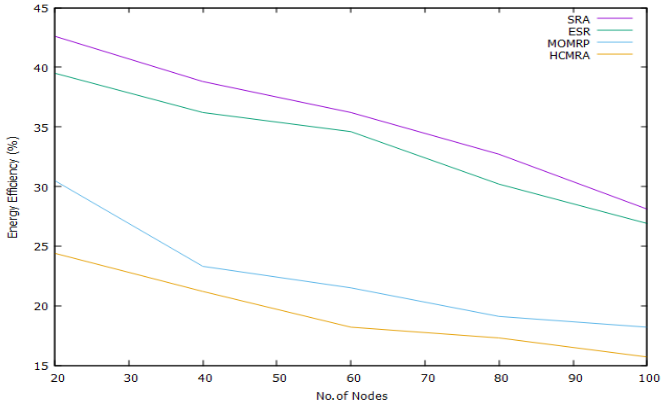

Figure 7. Energy Efficiency Vs Mobility

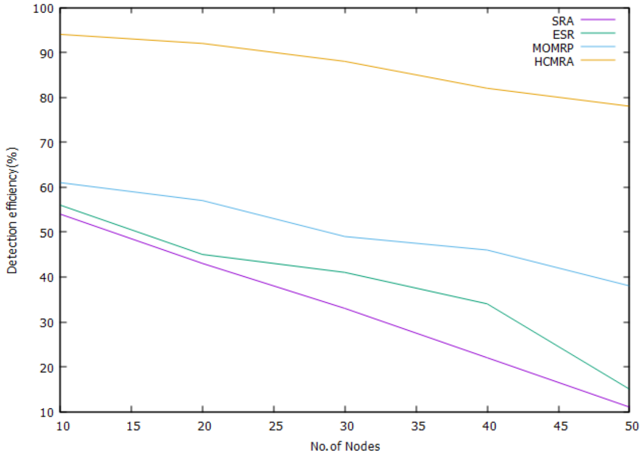

Figure 8. Detection Efficiency Vs No. of Nodes

5. Conclusion and Future Work

Detecting malicious attackers is a challenging task in MANET. To detect and isolate the attackers, trust enhanced cluster aware routing is established in the proposed work. Due to the discovery of optimal path, packets are arrived at quick arrival time and reliable path can also easily maintained without consuming excessive energy for packet transmission. Installing cluster is good approach to maximize the network lifetime. Here there are two cluster heads nominated i.e. superior CH and sub CH. Superior CH is elected based on high residual energy and stability. If it falls below energy level, sub CH can be automatically deputed as superior CH. Using trust aware routing, malicious nodes are identified and proposed work achieves 93% of detection efficiency compared to existing schemes i.e. SRA, ESR and MOMRP. In future, it is planned to implement advanced optimization technique for enhancing network lifetime through energy model.

References

[1] Mahmoud Abu Zant and Adwan Yasin, “Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol”, *Security and Communication Networks*, 2019, pp.1-13.

[2] Mohammad Riyaz Belgaum, Shahrulniza Musa, MazlihamMohd Su’ud, Muhammad Alam, Safeeullah Soomro and Zainab Alansar, “Secured Approach towards Reactive Routing Protocols Using Triple Factor in Mobile Ad Hoc Networks”. *Annals of Emerging Technologies in Computing*, vol. 3, no.2, 2019, pp. 32-40.

[3] Nazia sulthana and Virendra kumar sharma “Evaluation of Enhanced Swarm Based Mac Layer Protocol Over Secured Lazy Receiver Processing in MANETs”, *International Journal of Computer Trends and Technology*, vol. 67, no. 8, 2019, pp.81-86.

[4] Mohammed Gouse Galety, Mohammed Nuru, Tigist Adam, “WCBAODV: An Efficacious approach to detect Wormhole attack in VANET using CBAODV Algorithm”. *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 2, 2019, pp.20-25.

[5] Zulfiqar Ali Zardari , Jingsha He , Nafei Zhu, Khalid Hussain Mohammadani , Muhammad Salman Pathan , Muhammad Iftikhar Hussain and Muhammad Qasim Memon, “A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs”, *Future Internet*, 2019, pp.1-17.

[6] Sridhar, Baskaran, Anitha and Sankar, “Proficient and Secured Routing in MANET based on Trust and Energy supported AODV”, *Applied Mathematics and Information Science*, vol.11, no.3, 2017, pp.807-817.

[7] Vikram Neerugatti and A. Rama Mohan Reddy, “Acknowledgement Based Technique for Detection of the Wormhole Attack in RPL Based Internet of Things Networks”, *Asian Journal of Computer Science and Technology*, vol. 8, no.3, 2019, pp.100-104.

[8] Ramireddy Kondaiah and Bachala Sathyanarayana, "Trust Factor and Fuzzy-Firefly Integrated Particle Swarm Optimization based Intrusion Detection and Prevention System for Secure Routing of MANET", *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018, pp.41-48.

[9] Devakumari, Shanthini, "An Energy Efficient Technique in MANETs modified Trust based Route selection Algorithm", *International Journal of Pure and Applied Mathematics*, vol.119, no.18, 2018, pp.3215-3222.

[10] Rohi Tariq, Sheeraz Ahmed Corresp., Raees Shah Sani , Zeeshan Najam , Shahryar Shafique, "Securing ad hoc on-demand distance vector routing protocol against the black hole DoS attack in MANETs", 2019, *Peer J prints*, 1-40.

[11] Zaid Abdulkader, "Malicious Node Identification Routing and Protection Mechanism for VANET against Various Attacks", *Journal of Information Security Research*, vol. 8, no. 4, 2017, pp.161-177.

[12] Binuja Philomina Marydasan and Ranjith Nadarajan, "Topology Change Aware on Demand Routing Protocol for Improving Reliability and Stability of MANET", *International Journal of Intelligent Engineering and Systems*, vol.5, no.4, 2022, pp.468-478.

[13] Udhaya Sankar, Dhinakaran, Cathrin Deboral and Ramakrishnan, "Safe Routing Approach by Identifying and Subsequently Eliminating the Attacks in MANET", *International Journal of Engineering Trends and Technology*, vol. 70, no.11, 2022, pp. 219-231.

[14] R. Suresh Kumar, P. Manimegalai, P. T. Vasanth Raj, R. Dhanagopal and A. Johnson Santhosh, "Cluster Head Selection and Energy Efficient Multicast Routing Protocol based Optimal Route Selection for Mobile Ad Hoc Networks" , *Wireless Communications and Mobile Computing*, Vol. 2022, pp.1-12.

[15] S. Rahamat Basha, Chhavi Sharma, Farrukh Sayeed, A. N. Arularasan, P. V. Pramila, Santaji Krishna Shinde , Bhasker Pant, A. Rajaram , and Alazar Yeshitla, "Implementation of Reliability Antecedent Forwarding Technique Using Straddling Path Recovery in Manet", *Wireless Communications and Mobile Computing*, 2022, pp.1-9.

[16] Meena Bharti, Shaveta Rani and Paramjeet Singh, "Efficient Cluster Head Selection and Trust Based Routing in MANET", *Journal of Physics: Conference Series*, 2327, 2022, pp.1-8.

[17] Anugraha and Krishnaveni, "An Efficient and Secure Routing in MANET using Trust Model ", *International Journal of Engineering Trends and Technology*, vol. 70, no. 9, 2022, pp.330-336.

[18] Nassir Harrag, Abdelghani Harrag, "Fuzzy-ZRP: An Adaptive MANET Radius Zone Routing Protocol", *Engineering, Technology & Applied Science Research*, vol.13, no.2, 2023, pp.10601-10607.

[19] S. J. Sangeetha and T. Rajendran, "Improving QoS Using Mobility-Based Optimized Multipath Routing Protocol in MANET", *Computer Systems Science & Engineering*, vol.46, no.1, 2023, pp.1169-1181.

[20] K. Nirmaladevi and K. Prabha, "A selfish node trust aware with Optimized Clustering for reliable routing protocol in MANET", *Measurement: Sensors*, 2023, pp.1-10.