International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6533
***Article Received**: 19 January 2023 **Revised**: 25 February 2023 **Accepted**: 04 March 2023*

Cooperative Self-Scheduling Secure Routing Protocol for Efficient Communication in MANET

[1]Y.M. Mahaboob John, [2]Dr. G. Ravi
[1]Mahendra College of Engineering, Salem, Tamilnadu, India,
mehaboobece07@gmail.com
[2]Sona College of Technology , Salem, Tamilnadu, India
raviraj.govind@gmail.com
*Corresponding Author: Y. M. Mahaboob John. Email: mehaboobece07@gmail.com

Abstract —In wireless transmission, a Mobile Ad-hoc Network (MANET) contains many mobile nodes that can communicate without needing base stations. Due to the highly dynamic nature of wireless, MANETs face several issues, like malicious nodes making packet loss, high energy consumption, and security. Key challenges include efficient clustering and routing with optimal energy efficiency for Quality of Service (QoS) performance. To combat these issues, this novel presents Cooperative Self-Scheduling Secure Routing Protocol (CoS3RP) for efficient scheduling for proficient packet transmission in MANET. Initially, we used Elite Sparrow Search Algorithm (ESSA) for identifies the Cluster Head (CH) and form clusters. The Multipath Optimal Distance Selection (MODS) technique is used to find the multiple routes for data transmission. Afterward, the proposed CoS3RP transmits the packets based on each node authentication. The proposed method for evaluating and selecting efficient routing and data transfer paths is implemented using the Network simulator (NS2) tool, and the results are compared with other methods. Furthermore, the proposed well performs in routing performance, security, latency and throughput.

Keywords—MANET; wireless communication; QoS; Cluster Head (CH); multipath; security; authentication; scheduling; routing protocol.

I. INTRODUCTION

A MANET is considered a contactless, fixed node for dynamically delivering and accessing data, acting as a mobile node capable of remote control and scalable routing services using efficient routing security techniques. MANET relies on unique security solutions for each mobile node, and the network is distributed over minimal infrastructure. So it is not easy to achieve centralized security control this time. Due to the instability of the network, multiple attacks may occur. Depending on the infrastructure, the self-configuration network is used in the MANET. The powerful technology that provides virtual hardware and software sources works as needed in the MANET

However, MANET requires further discussions and improvements in terms of security. The main reason is that the network topology is dynamic and unreliable. The nature of ad hoc networks lends itself to different types of attacks. Furthermore, the inconsistency of these networks poses a challenging problem when implementing security. The frequent effects of security in the MANET, the change in its placement, the cooperatives, the lack of central monitoring, the lack of management, and the precise defensive technique. Acting on the central infrastructure, such as Ad-hoc network routers or access points, is complex.

Primary defects such as limited bandwidth, memory, processing capabilities, and open media are highly susceptible to malicious node. Dynamic topologies and lack of infrastructure in ad-hoc wireless networks make them vulnerable to malicious attacks.

To solve this problem, we introduce Cooperative Self-Scheduling Secure Routing Protocol (CoS3RP) for secure communication in MANET. Our main contribution is secure packet communication based on multiple routes with less packet drop ratio and latency in the network.

II. LITERATURE SURVEY

H. Xia t al, (2020): The author proposed that lightweight subjective confidence inference frameworks can be divided into two categories, evaluative and predictive. The node reliability evaluation process is based on the historical performance of nodes in the system. However, it is vulnerable to malicious attacks and denial of service.

J. Tu et al, (2021): The author proposed to characterize an active routing protocol using an active-routing authentication scheme (AAS). AAS is effective against route spoofing attacks in MANET using selective forwarding, false routing, Byzantine-like attacks and BAN logic. They also considered the possibility of malicious nodes.

M. Tahboush et al; (2021): The author proposed a HWAD algorithm for attack identification. These can detect out of band wormholes by doing things like RTT based on hop count and PDR. Compared to existing solutions, out-of-band wormholes can more reliably control propagation between adjacent nodes.

B. U. I. Khan et al, (2021): The author proposes that mobile nodes can use real-time streaming to exchange multimedia signals in a practical scenario as a test case. There are two fundamental security requirements, namely protecting packets and understanding the unpredictable behaviour of attackers.

A.M. El-Semary et al, (2019): The author proposed that the security violations related to the original AODV and specifically, (SAODV) protocols can be overcome using secure MANET routing protocols called BP-AODV. However, joint black hole attacks cannot be resisted, and two nodes join together and attack.

R. J. Cai et al, (2019): The author proposed an evolutionary self-cooperative trust (ESCT) scheme that mimics human cognitive processes and provides trust-level information to avoid various routing interference effects. These processes allow mobile nodes to exchange trust and analyze the information received based on cognitive judgment.

Jain Andy B et al, (2016): The author proposes that all mobile users can create a new class of network, a MANET, if they want to communicate without a support system. Discuss the concept of Manet and various solutions for secure routing in MANET briefly. The lack of support for mobile computing is due to the high cost, low predictable usage and poor performance of wireless communications, and ubiquitous access points.

M. Abdan et al, (2022): The author proposed that classification can be done by several ML methods, such as Linear Discriminant Analysis (LDA), NB, and CNN. Also, MANET can exploit the nodes' properties and the nodes' speed for feature extraction. However, wormhole attacks occur at the network layer that simulators routing protocols.

G. Farahani et al, (2021): The author proposes that a new algorithm can be used in Manets to detect black hole attacks of clustering and fuzzy assumption of cluster head selection. The cluster head will be selected in stages according to the fuzzy inference's reputation and remaining energy. Finally, the target node's trusted server can be verified.

S. Gurung et al, (2019): The author proposed a classification of DoS attacks and highlights the critical variances between black-hole, sequence-based gray-hole, and innovative gray-hole attacks. The AODV protocol can be modified and simulated using two types of attacks. Various protocols have been proposed to mitigate the black-hole attack, but these protocols cannot be analyzed under the gray-hole attack.

N. Veeraiah et al, (2021): The author proposed that the reason for increasing the Manet routing protocol is ideal for navigating the stable optimal selection of multi-paths. Given the network's changing topology and constrained resources, providing efficient power and secure routing is considered a challenging task.

U. Srilakshmi et al, (2021): The author proposes that the routing protocol Genetic Algorithm with Hill Climbing (GAHC) can be used to demonstrate a hybrid GAHC algorithm. Previously, an developed fuzzy C-means method was built on density peaks, and more recently, CHs were selected based on implicit and direct correlation confidence. An additional confidence threshold value can be found in the computation of nodes.

K. S. Sankaran et al, (2021): The author proposes that the paradigm can use conventional routing and intelligent ML techniques. The behavior of the nodes can be fully learned at all hop levels, thus enabling the establishment of secure and consistent routing and transmission paths at all hop levels of destination communications.

I. Zografopoulos et al, (2022): The author proposed that malicious cyber-physical attacks can be detected based on subset methods and validate a unified approach for heterogeneous Microgrids (MG) systems. A small-signal model of an autonomous or island MG and a secondary standard of MG should address the different models that target frequency control.

U. Srilakshmi et al, (2022): The author recommends using basic and functional navigation mechanisms to use the highest BFOA in the improvement of the path. Loss of power to a mobile node affects the node's packet forwarding capabilities and overall system lifetime.

A. M. El-Semary et al, (2019): The author proposed that a secure token routing protocol called BP-AODV can overcome the security violations related to the SAODV protocol and the original AODV protocol. Also, it can protect against a black hole attack that may occur during the forwarding process and against an initiated combined black hole attack. These are performed during the BP-AODV routing process.

X. Wang et al, (2020): The author suggested using a routing algorithm based on belief entropy. Routing algorithms reflect the detailed influence of route hops and node trust values on routing choices to improve MANET service quality. Routes with low confidence entropy can be added to the routing table. However, some performance measures are ambiguous and more accessible to define qualitatively than quantitatively.

N. Veeraiah et al, (2020): The author proposed that an effective multipath routing protocol optimization algorithm can be used in MANET. MANET's energy and security crisis is effectively solved by using CH selection and intrusion detection techniques such as fuzzy clustering and NB. Energy optimization is reflected to be a hot challenge in most of the current techniques which have been efficiently addressed using routing protocols.

M. Naseem et al, (2021): The author proposed to develop a load-balanced multi-path routing protocol with energy constraints (EE-LB-AOMDV). It can first use hop count, round-trip time, and residual energy to classify multiple paths. Only the basis of path quality can be used to initiate data transfer.

G. M. Borkar et al, (2017): The authors propose extending the ad hoc on-demand multipath distance vector protocol as a basic routing protocol for approximating the model. The proposed mesh-based multi-path routing scheme uses the secure neighbor location trust verification protocol to find all probable secure paths and the best link optimal path through the Dolphin Echolocation algorithm for efficient communication in MANETs.

R. Prasad et al, (2020): The author proposed that a novel and energy-efficient short path can use a routing mechanism called energy-aware on-demand routing protocol. An economically effective routing mechanism can be providing for packets depending on the routing condition, and the protocol can increase the period of the MANET.

S. V. Kumar et al, (2020): The author proposed that Energy Efficiency-Optimal Hierarchical Routing Algorithm (EE-OHRA) can be used to provide high routes of node characteristics that can be implemented in different fixed strength-based routing and network environments. Routing is carried out with the ability to select a node and the features with similar or related nodes to perform precise routing. These are more difficult when mobile ad-hoc network devices must be used for long periods and have limited battery charging capabilities.

M. Sirajuddin et al, (2021): The author proposed a trust-based multipath routing protocol called TBSMR to improve the overall performance of MANET. Congestion control, packet loss reduction, and malicious node detection are considered significant strengths of the MANET protocol. Achieving these challenging goals requires designing secure routing protocols to improve QoS.

T. V. S. Kumar et al, (2020): The author proposed neighbor node discovery developed in MANET to identify black hole nodes. A routing path can be created through a network using a multi-discovery routing protocol. The main objective is to create a routing path without interfering with black hole nodes.

C. Ran et al, (2021): The novel presents a node of the chain that is established in the network, and the states of all nodes can be stored, creating intermediate nodes in the chain. Also, a smart contract on the blockchain is set up to filter nodes that meet the quality of service constraints. Two communication paths, the primary and standby paths, are observed through a smart contract in the blockchain network.

O. Singh et al, (2018): The author proposes multilevel trust-based cryptography schemes to design an intelligence intrusion detection system and contract to detect attackers. Attackers can be identified with Elliptic Curve Cryptography (ECC) algorithm, which proposes new trust management. Hence, designing an intelligent intrusion detection system is very necessary.

Z. Ali Zardari et al, (2019): The author proposed a well-known technique in MANET for Dual Attack Detection for Black and Gray Hole attacks (DDBG). Additional features can be grouped into two categories, which are the Intrusion Detection System (IDS) node Connected Dominating Set (CDS) technique and the DDBG technique proposed. Before placing the nodes in the IDS package, the power and blacklist are checked.

S. Sankara et al, (2020): The authors proposed MANET against wormhole attacks. Attacks are detected using quality of service for the entire network. Each node detects active and passive aggression, packet delivery rate, and round trip time. Thus the proposed method can make complete identification of wormhole attacks possible.

A. Mallikarjuna et al, (2021): The authors proposed a hash function consuming the location update algorithm of the AODV routing protocol to increase security against selfish nodes. The AODV routing protocol routes packets from source to purpose. Therefore, the use of hash functions along with location update algorithms to prevent self-centred nodes Prevention of Selfish Node using Hash Function (PSNHF) is proposed to decrease packet loss in the network.

Deepika Kukreja et al, (2018): The author proposed the Power-Aware Malicious Detection for Security (PAMDS) protocol. In some cases, substituting or recharging node batteries is impractical, so an energy-aware feature is requisite to extend the life of MANETs. The protocol uses an Intrusion Detection System (IDS) to attack nodes in the network to perform packet forwarding failure attacks. Similarly, P. Satyanarayana et al. (2022) aims to enhance network lifetime in wireless network employed by the EEACBR technique. Energy consumption is considered the most critical challenge in WSN.

MU-HHO, MS-ASFO, and ABRR-CHIO algorithms designed by P. Satyanarayana et al. (2023) for privacy preservation in MANET for IoT applications. However, this method didn't analyse the malicious node in the MANET. Gopalakrishnan et al. (2021) developed an ANFIS method for malicious node detection in MANET.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6533
***Article Received**: 19 January 2023 **Revised**: 25 February 2023 **Accepted**: 04 March 2023*

Trust parameters are extracted from the ANFIS method-certified trusted and malicious nodes. Nonetheless, downgrading occurs through the detection of malicious nodes. Malicious node identification is a complicated issue because of the similar characteristics of trusted nodes within the sensitive region.

III. PROPOSED METHODOLOGY FOR COOPERATIVE SELF-SCHEDULING SECURE ROUTING PROTOCOL

As mentioned, in this novel presented Cooperative Self-Scheduling Secure Routing Protocol (CoS3RP) for secure routing protocol in MANET. Figure 1 illustrates the detailed process of secure packet transmission. Here, the first forms a clusters and elects the CH using Elite Sparrow Search Algorithm (ESSA) technique.

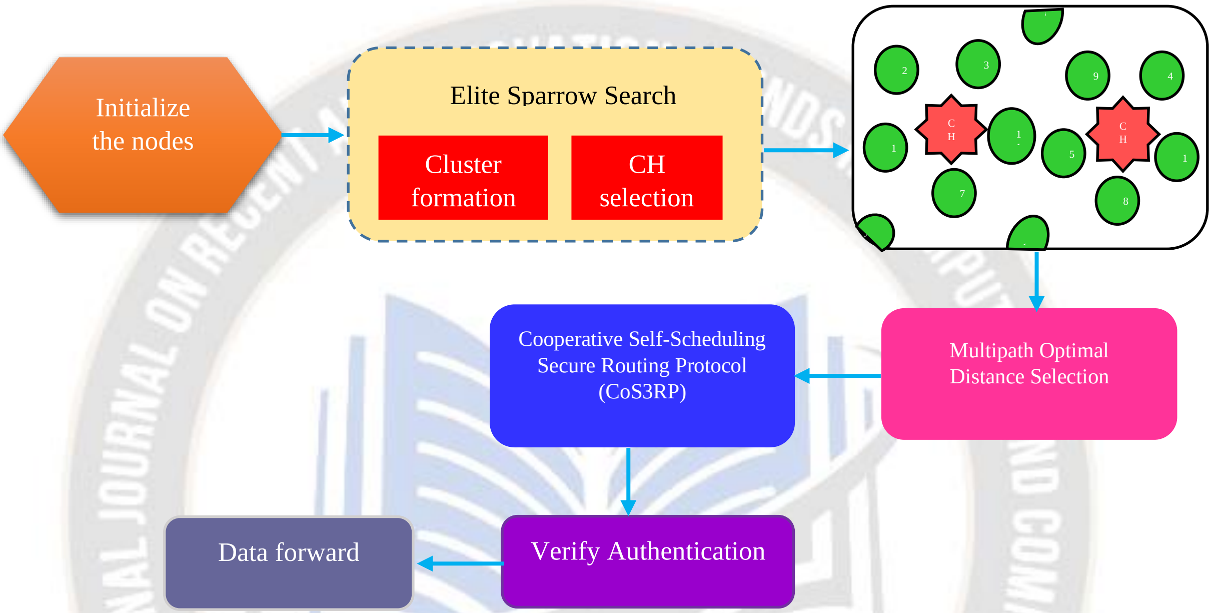

Figure 1. Structure of secure data communication in MANET

Then we apply Multipath Optimal Distance Selection (MODS) technique for analysis the multiple routes for packet transmission among CH to base station. After that, we use the proposed CoS3RP transmits the packets based on each node authentication. Each method is described in detail below.

A. Elite Sparrow Search Algorithm (ESSA)

This section uses the Elite Sparrow search algorithm to select the CH among the infinite number of nodes. This method consists of a sparrow's food foraging process to select CH. This means that sparrows have two strategies during foraging, which are finder-follower. In sparrows, those good at finding food act as finders, while others act as followers. To get high-quality food, some follower observes their finder and contest with those with high predation rates for food to enhance their nutrition. The nodes are assumed sparrow Sw and are set randomly in the network. The set of sparrow Sw resented and estimated by equation 1.

$$Sw = \begin{bmatrix} Sw_{1,1} & \cdots & Sw_{1,n} \\ \vdots & \vdots & \vdots \\ Sw_{k,1} & \dots & Sw_{k,n} \end{bmatrix} \qquad (1)$$

Where n denotes dimension, and k presents number of sparrows in the network.

$$F_{funtc} = \frac{A_{Ener}}{T_{Ener}} \qquad (2)$$

The above equation is used to estimate the fitness function $F_{funtc}$for sparrow food search space best solution. Assuming that, A_{Ener} denotes available energy and T_{Ener} denotes total energy.

$$Sw_{F_{funtc}} = \begin{bmatrix} F\left(Sw_{1,1}, Sw_{1,2} \dots Sw_{1,n}\right) \\ F\left(Sw_{2,1}, Sw_{2,2} \dots Sw_{2,n}\right) \\ F\left(Sw_{k,1}, Sw_{k,2} \dots Sw_{k,n}\right) \end{bmatrix} \qquad (3)$$

The above equation is find the each sparrows fitness values in the network.

$$M_R = R_{sw} + f * (R_{sw1} - R_{sw2}) \qquad (4)$$

From equation 4 is used to estimate the mutation rate for CH node selection. Assuming that R_{sw} denotes randomly

***Article Received**: 19 January 2023 **Revised**: 25 February 2023 **Accepted**: 04 March 2023*

selected sparrows R_{sw1}, R_{sw2}, and F denotes mutation rate variation factor.

```
Algorithm 1
Require: Number of node list  $N_{list}$
Ensure: Elect the Cluster Head (CH)
Begin
        Import nodes randomly $N_{list}$
        Generate preliminary population k sparrows
        For each node in $N_{list}$ do
                Calculate constraint of upper and lower bound in the nest
                        $B_{p,q} = L_{bouq} + (U_{bouq} - L_{bouq}) * R(1,n)$  // R denotes random number
                Estimate the each node sparrow fitness values using equation 2
                Identify the crossover of the sparrow population $Co_{n+1}$
                        $Co_{n+1} = \begin{cases} M_R & if(R \leq Co) \\ T_v & if(R \geq Co) \end{cases}$
                Evaluate the sparrow distance $Sw_{dis}$
                        $Sw_{dis} = \sqrt{\sum_{Sw=1}^{k} (Sw_{p,q} - Sw_{bestp,q})^2}$
                If $(R < Co)$
                        Perform CH selection process
                                Sparrow movement based best solution for CH $(Sw_{CH})$
                                        $Sw_{CH} = Sw_{dis}[Sw_{best} + \alpha|Co_{n+1} - Sw_{best}|^{(Sw+1)}]$
                Else
                        Ignore the sparrow (node)
                End if
                Update best Sparrow positions
        End for
        Return best result for CH selection
End
```

The above equation is used to find the Sparrow best position is selected the Cluster Head (CH). When the finder discovers the food, the whole sparrow searches the area and consumes all the food.

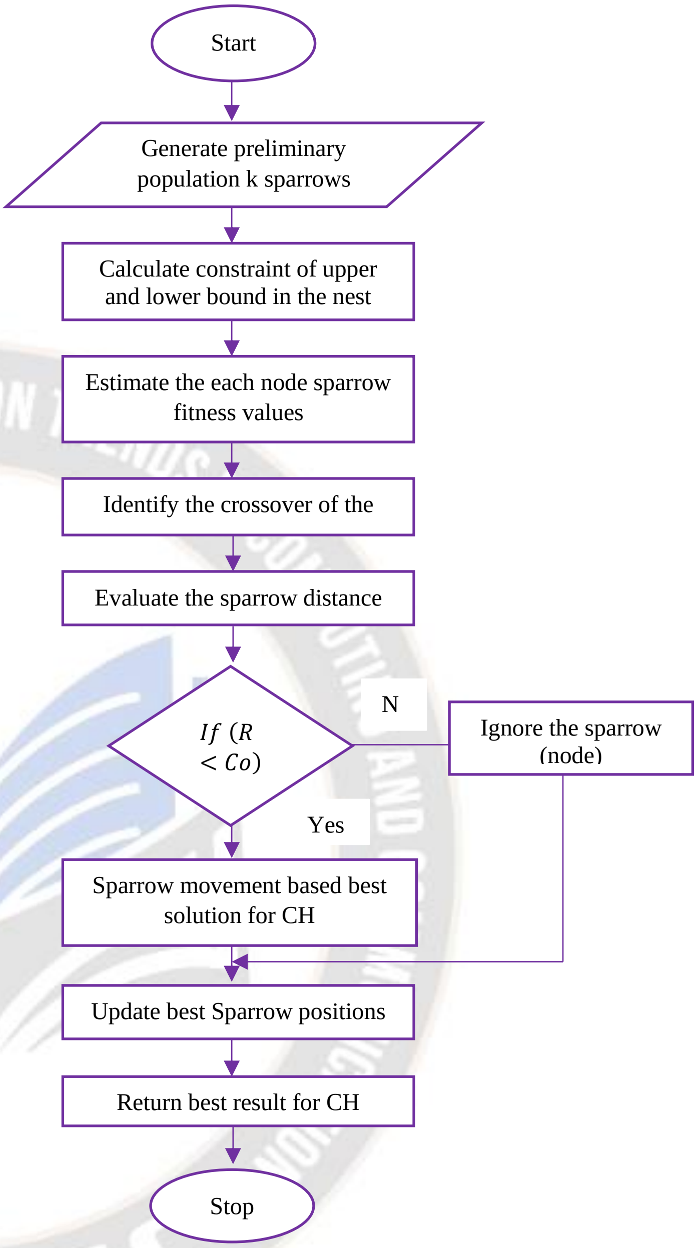
Start
Generate preliminary population k sparrows
Calculate constraint of upper and lower bound in the nest
Estimate the each node sparrow fitness values
Identify the crossover of the
Evaluate the sparrow distance
If (R < Co)
N
Ignore the sparrow (node)
Yes
Sparrow movement based best solution for CH
Update best Sparrow positions
Return best result for CH
Stop

Figure 2. Flowchart of Elite Sparrow Search Algorithm (ESSA)

Figure 2 defines the flowchart of Elite Sparrow Search Algorithm (ESSA) for CH selection. Finally, CH is the position of the best food node. A CH node gathers data and sends it to a sink in an aggregated form.

B. Multipath Optimal Distance Selection (MODS)

This section explains to find the multiple route for packet transmission using Multipath Optimal Distance Selection (MODS) algorithm, which is a method that works based on reactive routing. When routing is required, the source reveals the Route Request (RREQ) of the destination across the network. The node receiving the RREQ verifies the

***Article Received**: 19 January 2023 **Revised**: 25 February 2023 **Accepted**: 04 March 2023*

destination field of the RREQ packet. Routing information for the target node sends an RREP packet to the sender. Sends a Route Error (RRER) message to the sender if there is no routing information. If a source node accepts multiple Route Reply (RREP), the numerous routes to the destination with the fewest hops are selected. To identify the number of cluster (G_p) in the network described by equation.

$$G_p = \sqrt{\frac{N_{nodes}}{2}} \tag{5}$$

Where, N_{nodes} denotes amount of nodes in the network.

$$R_{Ey} = I_{Ey} - Ey(T) \tag{6}$$

The above equation is used to estimate Remaining energy for node selection. Then we estimate the distance of data sent from the common node to CH and the distance of data sent from CH to BS is calculated by Equation (7).

$$D_E = \frac{D_E{}^{a}_{disrance}}{D_E{}^{b}_{distance}} \tag{7}$$

Subject to,

$$D_E{}^{a}_{disrance} = \sum_{g=1}^{n} \sum_{h=1}^{C_m} \left|\left|E_g - c_m\right|\right| + \left|\left|c_m - \mathrm{CH}\right|\right| \tag{8}$$

$$D_E{}^{b}_{disrance} = \sum_{g=1} \sum_{h=1} \left|\left|E_g - E_h\right|\right| \tag{9}$$

The above equation is used to find the distance between CH to cluster members. Assuming thatE_g, E_h is the energy of two neighbour nodes, and c_m denotes nodes in the clusters.

$$TN^{T}_{(g,h)} = \left(\omega 1 * D^{T}_{cp}\right) + \left(\omega 2 * D^{T}_{df}\right) \tag{10}$$

Equation is used to calculating trust node TN. Assuming that$\omega 1$, $\omega 2$ are the weight values of node. D^{T}_{cp} is a control packet forwarding ratio and D^{T}_{df} data forwarding ratio according to their time T.

Algorithm 2
Require: Number of clusters and CH
Ensure: Multiple path selection MP

```
Begin
    Read clusters and CH information
    For each node $i$=1 do then
        Source $(src)$ node broadcast the RREQ via intermediate nodes
        Estimate the Energy utilization
            $E_{utli}(node, D_E) = E_{dis}(node, D_E) + E_{Rec}(node)$
        Calculate path trust $(PT)$
            $TP = \sum_{node=1} TN_{(g,h)} |\ node_g, node_h \in R\ and\ node_g \rightarrow node_h$
        Estimate Direct trust $DT$
        $DT_{(g,h)} = \sum(TN_{(g,h)} + TP)$
        Calculate the indirect trust $IT$
            $IT = DT_g * DT_h$
        Evaluate the fitness values $F_v$
            $F_v = \omega_1 f_1 + \omega_2 f_2 + \omega_3 f_3 + \omega_5 f_5$
        If node Route reply (RREP)
        Select the $S_{node}$
    $S_{node} = \frac{1}{Non_{CH}} \sum_{i=1}^{c_m} D_E(N_H(CH_i))$
        Else
            Select another neighbour node
        End if
        Return $MP$ ← Multiple path selection
    End for
End
```

The above algorithm 2 efficiently obtained multiple routes for packet transmission. In the algorithm steps source node (src) broadcasts RREQ via intermediate nodes, then analysis each node's energy utilization. Afterward, we analysed the path of trust and their fitness values for route selection. If the node gets a Route Reply (RREP), it will select that path; otherwise, it will ignore the route. Assuming that E_{dis} presents energy dispersed, E_{Rec} receiver, N_H is a next hop.

C. Cooperative Self-Scheduling Secure Routing Protocol

In this phase we use Cooperative Self-Scheduling Secure Routing Protocol (CoS3RP) for secure packet transmission. After multiple paths are detected, this algorithm sends data from the destination to the source by verifying the authentication of each node. Whenever a node transmits a packet to its neighbours, it includes its certificates in the packet to encrypt with the private key. When the closest node obtains the packet, it utilizes the Authentication's (A_n) public key to decrypt the received. If the closet node successfully decrypts the certificate and discovers the IP, sender's public key, and timestamp, it confirms that the sender is a legitimate node. A neighbouring node is considered malicious if it does not decrypt the data successfully.

Algorithm 3
Require: Multiple path MP
Ensure: Secure communication from source to destination

```
Begin
    Initialize the available path
        $MP = \{MP1, MP2 \dots MPn\}$
    $For\ (i = 0, i <= n, i + +)$
        If g is new closet node of h then
            Initiate the authentication node
            Estimate the node reliability
```

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6533
***Article Received**: 19 January 2023 **Revised**: 25 February 2023 **Accepted**: 04 March 2023*

```
            $R_i = \alpha \frac{D_i(node_g)}{G_i(node_g)} + \beta \frac{D_i(node_h)}{G_i(node_h)}$
            Calculate the delay $L_y$
                $L_y = \frac{Maximum(CH)}{w_c}$
            Verify the each node authentication $A_n$
                $A_n = (IP_h, pc_h, t, Ex)pk_h$
            If $A_n == true$
                Packet forward
            Else
                Discard the packet
            End if
        End if
    End for
End
```

The above algorithm steps produces efficient secure communication from sender to receiver. Assuming that α, β refers to weight rendering to the time that node g and h in the network. $D_i(node_i)$ Denotes packet delivered node g and j. $G_i(node_i)$ denotes packet generate node g, h. IP_h Denotes IP adders of h node, pc denotes h node public key, t time stamp of authentication generated, Ex denotes expire and pk_h denotes private key.

IV. RESULT AND DISCUSSION

This phase illustrates the simulation result analysis of the secure packet communication in the MANET environment and the evaluation result of the proposed method. This section elaborates on environment setup and comparative result analysis in this simulation model.

A. Environment setup

The evaluation of the simulation result implemented of the proposed method was accomplished using the NS2 using various parameters like routing performance, security, throughput, packet drop ratio, latency, and energy consumption.

Table 1: Parameters for simulation

Parameters	Values/units
Tool	NS2
Network Size	900*900m
Number of nodes	100
Packet size	512bytes
Channel type	Wireless
Initial energy	0.10J
Number of CH	5

The proposed protocol is executed with a windows 10 Operating System (OS), 8GB RAM, and an I7 processor.

B. Comparative result analysis

In this phase, a comparison of the proposed algorithm among other different previous algorithms is Multi Constrained Network Feature Approximation (MCNFA), Real-time Regional Mobility Energy (RRME), Efficient Prevention Restricted Routing Protocol (EPR2P), and Energy Efficiency-Optimal Hierarchical Routing Algorithm (EE-OHRA).

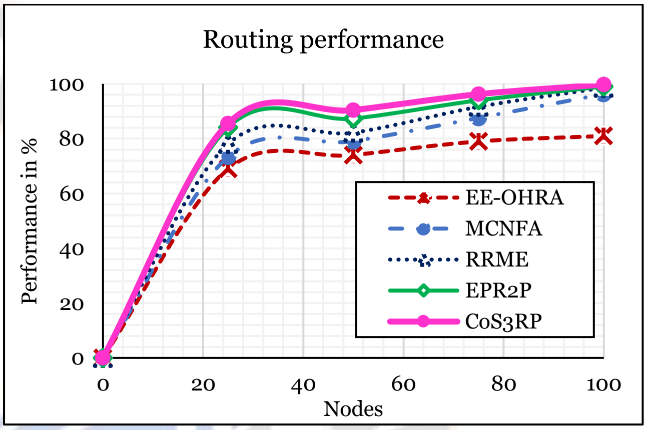

Figure 3. Impact of routing performance

Figure 3 illustrates the routing performance for data transmission in MANET. The routing performance is increased per packet. The proposed protocol outperforms the other methods because the proposed algorithm identifies the multiple paths with node authentication for secure communication to the receiver. Hence the proposed obtain the 99. 76% of security performance.

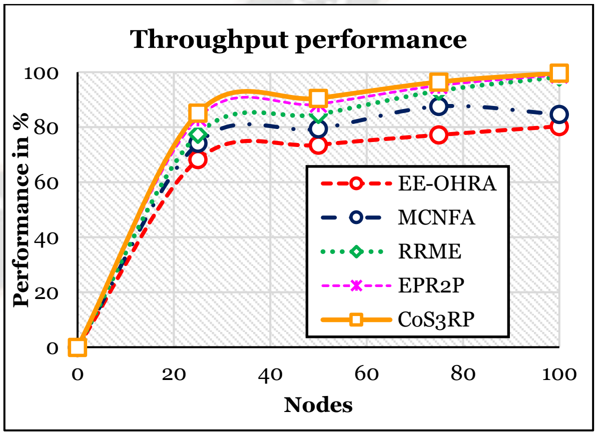

Figure 4. Analysis of Throughput performance

Figure 4 defines the result of throughput performance comparison result present in the graph. The proposed protocol has high throughput performance due to multiple reliable routes selected for communication from src to receiver. Thus the proposed protocol achieved 99.73% of throughput performance.

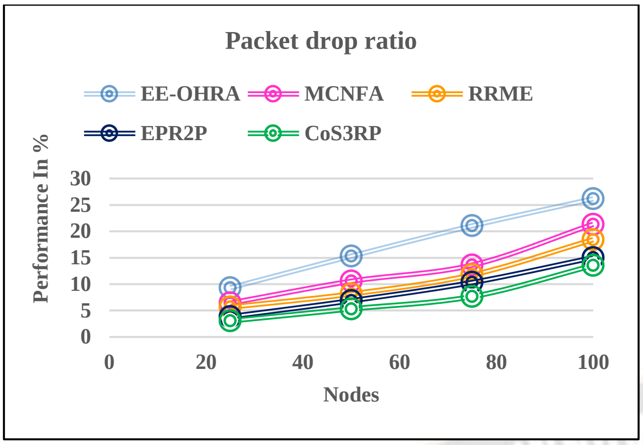

Figure 5. Analysis of Packet drop ratio performance

The simulation packet drop ratio is present in Figure 5. From the graph, it can be perceived that the packet drop ratio increased in previous methods than the proposed protocol. So the proposed obtained 13.54% of the packet drop ratio performance.

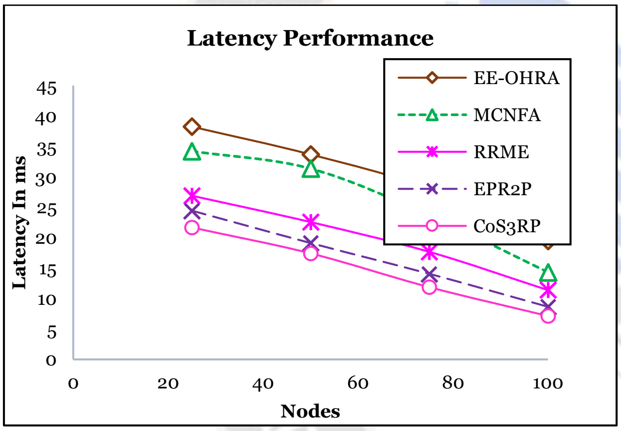

Figure 6. Impact of latency performance

Figure 6 shows the analysis of latency performance with various comparison approaches. As the node increases in the network, the latency is high in previous approaches because their pathfinding is more challenging, and the number of nodes is also high. Thus the latency increased the communication in the network. However, the proposed system has trust-based multiple paths to reduce latency performance. The proposed protocol average latency is 7.13% than EPR2P is 8.65%.

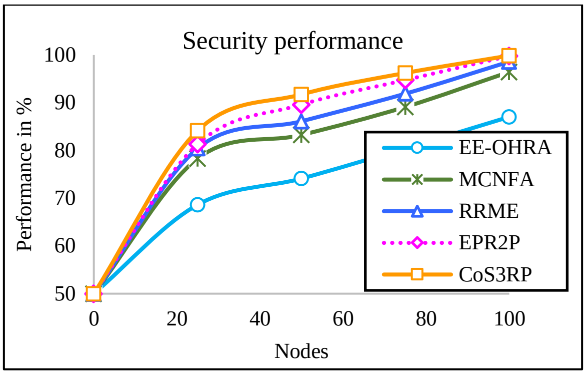

Figure 7. Impact of security performance

Figure 7 shows the proposed has obtained high-security performance than other methods. The proposed protocol determines each node authentication based on the MODS algorithm. Also, the proposed protocol identifies the reliability and delay of packet communication to schedule the transmission in the network. Hence the proposed obtained security performance increased result is 99.87% than EPR2P MCNFA, RRME approaches.

V. CONCLUSION

This research introduced Cooperative Self-Scheduling Secure Routing Protocol (CoS3RP) and Multipath Optimal Distance Selection (MODS) technique for secure communication. The presented algorithm to solve the issues of security and QoS performance in the MANET. To obtain high security and routing performance a number of process are following: Elite Sparrow Search Algorithm (ESSA) for identifies the Cluster Head (CH) and form clusters. The Multipath Optimal Distance Selection (MODS) technique is used to find the multiple routes for data transmission. Afterward, the proposed CoS3RP transmits the packets based on each node authentication. The proposed method for evaluating and selecting efficient routing and data transfer paths is implemented using the Network simulator (NS2) tool, and the results are compared with other methods. Furthermore, the proposed well performs in routing performance, security, latency and throughput.

REFERENCE

[1] H. Xia, Z. Li, Y. Zheng, A. Liu, Y. -J. Choi and H. Sekiya, "A Novel Light-Weight Subjective Trust Inference Framework in MANETs," in IEEE Transactions on Sustainable Computing, vol. 5, no. 2, pp. 236-248, 1 April-June 2020, doi: 10.1109/TSUSC.2018.2817219.

[2] J. Tu, D. Tian and Y. Wang, "An Active-Routing Authentication Scheme in MANET," in IEEE Access, vol. 9, pp. 34276-34286, 2021, doi: 10.1109/ACCESS.2021.3054891.

[3] M. Tahboush and M. Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)," in

IEEE Access, vol. 9, pp. 11872-11883, 2021, doi: 10.1109/ACCESS.2021.3051491.

[4] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, M. L. B. M. Kiah and R. N. Mir, "Game Theory Analysis and Modeling of Sophisticated Multi-Collusion Attack in MANETs," in IEEE Access, vol. 9, pp. 61778-61792, 2021, doi: 10.1109/ACCESS.2021.3073343.

[5] A.M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019, doi: 10.1109/ACCESS.2019.2928804.

[6] R. J. Cai, X. J. Li and P. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," in IEEE Transactions on Mobile Computing, vol. 18, no. 1, pp. 42-55, 1 Jan. 2019, doi: 10.1109/TMC.2018.2828814.

[7] Jain Andy B. Buksh, "Solutions for secure routing in mobile ad hoc network (MANET): A survey", *Imperial Journal of Interdisciplinary Research*, vol. 2, no. 4, pp. 5-8, 2016.

[8] M. Abdan and S. A. H. Seno, "Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad Hoc Network (MANET)", *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. e2375702, janv. 2022.

[9] G. Farahani, "Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks", *Secur. Commun. Netw.*, vol. 2021, pp. e8814141, 2021.

[10] S. Gurung and S. Chauhan, "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET", *Wirel. Netw.*, vol. 25, no. 3, pp. 975-988, 2019.

[11] N. Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," in IEEE Access, vol. 9, pp. 120996-121005, 2021, doi: 10.1109/ACCESS.2021.3108807.

[12] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf and B. V. Subbayamma, "An Improved Hybrid Secure Multipath Routing Protocol for MANET," in IEEE Access, vol. 9, pp. 163043-163053, 2021, doi: 10.1109/ACCESS.2021.3133882.

[13] K. S. Sankaran, N. Vasudevan, K. R. Devabalaji, T. S. Babu, H. H. Alhelou and T. Yuvaraj, "A Recurrent Reward Based Learning Technique for Secure Neighbor Selection in Mobile AD-HOC Networks," in IEEE Access, vol. 9, pp. 21735-21745, 2021, doi: 10.1109/ACCESS.2021.3055422.

[14] I. Zografopoulos and C. Konstantinou, "Detection of Malicious Attacks in Autonomous Cyber-Physical Inverter-Based Microgrids," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 5815-5826, Sept. 2022, doi: 10.1109/TII.2021.3132131.

[15] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah and Y. Alotaibi, "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks," in IEEE Access, vol. 10, pp. 14260-14269, 2022, doi: 10.1109/ACCESS.2022.3144679.

[16] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map," in IEEE Access, vol. 7, pp. 95197-95211, 2019, doi: 10.1109/ACCESS.2019.2928804.

[17] X. Wang, P. Zhang, Y. Du and M. Qi, "Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network," in IEEE Access, vol. 8, pp. 47675-47693, 2020, doi: 10.1109/ACCESS.2020.2978143.

[18] N. Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET" in Evolutionary Intelligence, Berlin, Germany:Springer, pp. 1-15, Mar. 2020.

[19] M. Naseem, G. Ahamad, S. Sharma and E. Abbasi, "EE-LB-AOMDV: An efficient energy constraints-based load-balanced multipath routing protocol for MANETs", *Int. J. Commun. Syst.*, vol. 34, no. 16, 2021.

[20] G. M. Borkar and A. R. Mahajan, "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks", *Wireless Netw.*, vol. 23, no. 8, pp. 2455-2472, Nov. 2017.

[21] R. Prasad and P. S. Shankar, "Efficient performance analysis of energy aware on demand routing protocol in mobile ad-hoc network", *Eng. Rep.*, vol. 2, no. 3, 2020.

[22] S. V. Kumar and V. Anuratha, "Energy efficient routing for MANET using optimized hierarchical routing algorithm (Ee-Ohra)", Int. J. Sci. Technol. Res., vol. 9, no. 2, pp. 2157-2162, Feb. 2020.

[23] M. Sirajuddin, C. H. Rupa, C. Iwendi and C. Biamba, "TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network", Secur. Commun. Netw., vol. 2021, Apr. 2021.

[24] T. V. S. Kumar and D. P. G. Benakop, "A secure routing protocol for MANET using neighbor node discovery and multi detection routing protocol", *Int. J. Eng. Trends Technol.*, vol. 68, no. 7, pp. 50-55, 2020.

[25] C. Ran, S. Yan, L. Huang and L. Zhang, "An improved AODV routing security algorithm based on blockchain technology in ad hoc network", EURASIP J. Wireless Commun. Netw., vol. 2021, no. 1, pp. 1-16, 2021.

[26] O. Singh, J. Singh and R. Singh, "Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET", *Cluster Comput.*, vol. 21, no. 1, pp. 51-63, Mar. 2018.

[27] Z. Ali Zardari, J. He, N. Zhu, K. Mohammadani, M. Pathan, M. Hussain, et al., "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*, vol. 11, no. 3, pp. 61, Mar. 2019.

[28] S. Sankara Narayanan and G. Murugaboopathi, "Modified secure AODV protocol to prevent wormhole attack in MANET", *Concurrency Comput. Pract. Exper.*, vol. 32, no. 4, Feb. 2020.

[29] A. Mallikarjuna and V. C. Patil, "PUSR: Position update secure routing protocol for MANET", *Int. J. Intell. Eng. Syst.*, vol. 14, no. 1, pp. 93-102, Feb. 2021.

[30] Deepika Kukreja, S.K Dhurandher and B.V.R Reddy, "Power aware malicious nodes detection (PAMDS) for securing MANETs against packet forwarding misbehaviour attack", *Journal of Ambient Intelligence and Humanized Computing*, August 2018.

[31] P. Satyanarayana, U. D. Yalavarthi, Y. S. S. Sriramam, M. Arun, V. G. Krishnan and S. Gopalakrishnan, "Implementation of Enhanced Energy Aware Clustering Based Routing (EEACBR)Algorithm to Improve Network Lifetime in WSN's," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-6, 2022.

[32] P. Satyanarayana, G. Diwakar, B.V. Subbayamma, N.V. Phani Sai Kumar, M. Arun, S. Gopalakrishnan, Comparative analysis of new meta-heuristic-variants for privacy preservation in wireless mobile adhoc networks for IoT applications, Computer Communications, vol.198, 2023.

[33] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2021) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, 2021.