Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs

Sathyaraj P (Sathyaraj24122019@gmail.com)
R.M.K College of Engineering and Technology https://orcid.org/0000-0003-4063-772X
Rukmani Devi D
R.M.D Engineering College
K Kannan
R.M.K College of Engineering and Technology

Research Article

Keywords: MANET, Elastic property, Black hole, Improved Crossover Chicken Swarm Optimization (ICCSO), Enhanced Partially-Mapped Crossover operation.

Posted Date: July 20th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-188928/v1

Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs

[*1] Sathyaraj P, [2] Rukmani Devi D, [3]Dr. K. Kannan

[1] Assistant Professor, Department of ECE,
R.M.K College of Engineering and Technology, Chennai, India.

[2]Professor, Department of ECE, R.M.D Engineering College, Chennai, India.

[3]Assistant Professor, Department of ECE,
R.M.K College Of Engineering And Technology, Chennai, India.

[*]Corresponding Author Mail ID: Sathyaraj24122019@gmail.com

Abstract—

Background: Mobile Ad-hoc Networks (i.e.) MANETs are gaining rapid fame in recent days and are considered as very significant because of their easier implementation and growing property. Various types of attacks are prone to damage the networks due to the elastic property possessed by the network. And among different categories of attacks that can affect MANETs, black hole attack is considered as the commonly occurring one within a MANET. Chicken Swarm Optimization (CSO) algorithm is one among the technique used for the detection of black hole attacks occurring in the MANETs. But the CSO algorithm possesses some disadvantages and necessity rises for overcoming the weakness in the CSO algorithm.

Objective: Therefore, in this research paper, to address the black hole attack in MANET, an Improved Crossover Chicken Swarm Optimization (ICCSO) algorithm and the concept of Enhanced Partially-Mapped Crossover operation proposed and the best fitness values obtained.

Methods: In ICCSO algorithm, parameter initialization is carried out in step 1 of the algorithm, where the attacked nodes and non-attack nodes are created separately with the aid of parameters like PDR (i.e.) Packet Delivery Ratio and RSSI (i.e.) Received Signal Strength Indicator. Further, If the node is affected by any attack, then the nodes are discarded and the data is transmitted through the non-attacked node. Routing is carried by a protocol of AODV.

Results: The effectiveness of the algorithm proposed in the work is evaluated using various performance measures like packet delivery ratio (PDR), end-to-end delay (EED) and throughput. The performance measures are compared with a different state of the art routing protocols and it can be inferred that the proposed methodology comes up with improved results.

***Index Terms*—MANET, Elastic property, Black hole, Improved Crossover Chicken Swarm Optimization (ICCSO), Enhanced Partially-Mapped Crossover operation.**

I. INTRODUCTION

MANET is a portable and adaptable wireless infrastructure which serves many benefits to the network[1]. The wireless sensor network comprises of automatic wireless connection sensors which can detect the performance of the surrounding and have the ability to connect the internet via the base station. In many cases, sensors have spatial distribution. Sensors have low cost, they are developed with a constrained power source, computational ability, size of the memory. But they failed to implement the security issues which is prone to node attacks. Node attacks lead to delay transmission rate, packet corruption, data loss, energy loss, duplication of data, holding of data, routing problems and so on. This attack mostly targets on routing layer of the network. But in this research is based on the black hole attack. It is also called a packet drop attack. In networking, it is the shutdown attack where the node rejects the packet instead of transmitting them. Hence it increases the count of packet drop which in turn decreases the packet delivery ratio and affects the performance of the MANET. If there are multiple black holes developed on the network, the packet drop will be increased more and leads to a huge decrease in packet delivery ratio. In black hole attack, malevolent node applications follow this protocol to broadcast itself to give the shortest path available between a source nodes to the destination node. This destructive node broadcast its availability of new path without checking in the routing table. In this node attack, attacker node constantly replies to route request to adapt the data packet then drop it. If the attack happens based on flooding, the reply from the corrupted node is obtained by the requesting node before the reply from the real node. Hence, the malicious node will create a fake path. When this path is defined, it depends on the node to decide whether to drop or forward the packets to an unknown address. [2]The intrusion detection system is a popular technique to safeguard the network. The main role is to detect the strange activities which possibly indicates the ongoing attacks. Genetic algorithm is applied for searching. It examines an output equal to or close to the solution of a given problem. The strategy followed by GA is to give the best solution to crossover the parental genes[3]. It is built to get optimum answers as soon as possible in the least generations. The selection of crossover techniques impacts on the performance of the genetic algorithm[4]. The genetic operators improved is then maximize the fitness function and overall residue is minimized.

The method to handle this problem is chicken swarm optimization which has decreased local optimum value when solving high-dimensional optimization issues, but it's expensive and has nonlinear constraints. By implementing

crossover and improved chicken swarm optimization, the shortcoming of CSO [5]can be reduced in MANET. Mostly MANET is applied in military applications, emergency rescue, mesh networks, wireless community networks. The major issues of MANET when it's is prone to node attack to be discussed in this research are PDR and RSSI.

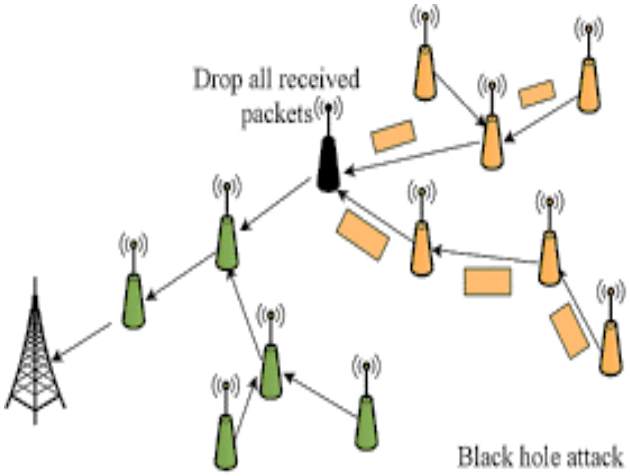

Figure 1. Representation of Black Hole Attack

Stability is maintained among quality of the solution and the convergence rate by various swarm intelligence algorithms and this has gained significant interest in the research area. CSO algorithm (i.e.) Chicken Swarm Optimization algorithm was first formulated in the year 2014 by Meng et al. This CSO algorithm falls under the stochastic optimization category and imitates the behaviour possessed by the group of chickens. The chicken group consist of different subcategories like a single rooster, few hens and numerous chicks. All the above categories of chicken searches for food based on their individual and distinct movements. Moreover, a particular hierarchy is present in every individual subcategory and similarly, competition exists among various subcategories. The global optimum solution is attained by proper search through the utilization of chicken swarm optimization.

Later improved security and lower consumption of energy are attained with the aid of certain watchdog nodes by providing the optimal location. The efficient delivery of packets to the destination is recognised by the packet delivery ratio. In the identification of wormholes, both the reliability of nodes and the anomaly of the packet distribution ratio play a significant role.A wormhole is a speculative design relating disparate score in space-time and depends on a particular outcome. An alternative path is employed for communication by the secured technique when the malicious nodes are identified within the network. And hence a complete message is delivered by the secured technique on the utilization of this alternative path.

Received Signal Strength Indicator (RSSI) is a computation of power in a received radio signal. It is invisible to the user. RSSI are employed for detecting the wormholes. These indicators work in terms of the malicious node is located far away to the remaining neighbours. Hence, on comparing with the normal neighbours, the affected malicious neighbours possess lower signal strength. The sender identifies a node as a malicious one depending upon the previous information.

Various types of attacks are prone to damage the networks due to the elastic property possessed by the network. And among different categories of attacks that can affect MANETs, black hole attack is considered as the commonly occurring one within a MANET. Chicken Swarm Optimization (CSO) algorithm is one among the technique used for the detection of black hole attacks occurring in the MANETs. But the CSO algorithm possesses some disadvantages and necessity rises for overcoming the weakness in the CSO algorithm.

By focusing on the above issues, the major contribution of the study involves,

- By generating the MANET system model, attacked node and non-attack node generated separately with the help of Packet Delivery Ratio (PDR) and Received Signal Strength Indicator (RSSI).
- To address the black hole attack in MANET, an Improved Crossover Chicken Swarm Optimization (ICCSO) algorithm and the concept of Enhanced Partially-Mapped Crossover operation proposed and the best fitness values obtained.
- By AODV routing, if the node is affected by any attack, then the nodes are discarded and the data is transmitted through the non-attacked node.

A. Organization of Paper

This section provides a general introduction about MANET, attacks occurring in MANET and Chicken Swarm Optimization (CSO) algorithm. The remaining portion of the research work is devised as follows: Section II provides the review of the existing optimization algorithms and protocols utilized in MANET for optimizing the attacks in MANET. Section III provides with the implementation of the proposed ICCSO (i.e.) Improved Crossover Chicken Swarm Optimization algorithm for the detection of attacks present in MANET. Section IV illustrates the performance analysis of the proposed methodology by comparing the proposed algorithm with the prevailing algorithms. Section V concludes the research paper by providing the overall summary of the research work.

II. RELATED WORKS

The previously existing works related to MANET, AODV protocols and black hole types of attacks in MANET are listed separately.

A. MANET

[6] This study presented SRDPV technique that aided the source finds a compassionate destination and conducted a secrecy-protecting verification of the path across the multiple nodes. At the beginning stage, transferring the information data through malevolent nodes are avoided and then evaluated the authentication without adding a third party. Here, it was demonstrated that the efficiency by deploying SRPV in two aspects: resisted the cumulative black hole attack of the

protocol AODV and detected an inserted malware routers which assign passive and active attack in MANETS. As compared to the other existing secure routing algorithms this approach detected the malicious nodes and above of SRDPV was sensible. [7] Proposed an innovative lightweight mechanism with the name of INDIA (i.e.) Intruder Node Detection and Isolation Action. Because of the lack of a central beurocrat, providing proper security to the network becomes a significant problem. Each node was derived from the direct and indirect trust features and by combining, the total trust feature was evaluated. By the utilization of PSO algorithm (i.e.) Particle Swarm Optimization algorithm, the extracted features or attributes are enhanced and then these enhanced features are subjected to classification with the aid of classifier like Neural network classifier (NN). The performance of the proposed approach was surveyed in concern with various parameters namely communication delay, success rate and volume of the consumption of energy to identify and isolate the intruder into the networks. [8] Discussed the security issues and various attacks to MANET layers. MANET framework enabled various nodes to merge the network along with the intrinsic mutual trust that was existing between the networks[9, 10]. It allows nodes to merge on the fly due to severe damage and occurs harmful damage. So the dynamic MANET was vulnerable during the worst condition. The importance of MANET is to show a better choice than others. Finally, Securing MANET and identifying a solution to these attacks was described. [11] Introduced a proactive neighbour knowledge-based hybrid broadcasting scheme to decrease the routing overhead and attain energy consumption. Many routing protocols utilized flooding as a basic mechanism for routing in MANET which occurs performance degradation and another is based on link failure issues by power exhaustion of mobile nodes. The simulation result revealed that the proposed approach reduces the routing overhead and power consumption by attaining better packet delivery.

By analyzing all the studies, effective MANET system is required with lesser attacking nodes for the accurate data transmission. Hence in this study effective MANET system model is generated.

B. AODV Protocol

[12] Utilized sequence number of designation and hop count fields of RREP message of AODV to find the malevolent node in a mobile ad-hoc network. A malicious node that contain a propensity of attracting traffic towards itself so that it can evaluate the different types of attacks namely misrouting, altering the information and dropping the packet. To achieve the destination malicious nodes transmit reply for RREQ messages that received from the source. The proposed system is capable of predicting every RREP messages that are obtained from different kind of nodes inside the network. If some information present within a network to be routed, the routing node must be decided much before the start of the routing process. The result revealed that the proposed work had an accuracy factor in terms of PDR increased and it provides more robust and stable delivery. However, the delay was improved slightly but it is bearable when delivery got more smooth and better in many cases. [13] Suggested a new algorithm that improves the safety of the AODV routing protocol to come across the black hole attack[14, 15]. A progressive type of network which gets handled by the independent node that does not belong to any particular constant network is known as Ad-hoc network. In the black hole attack, data packets were got attracted by the malevolent nodes and were eliminated by the malevolent nodes. Hence, the recommended process was subjected to simulation through NS2 software. This outcome revealed that some of the results possess higher end-to-end delay packet values. [16] Proposed a novel accurate detection and prevention of jellyfish attack detection (APD-JFAD). The DOS occurrence affected the normal process of MANETs. This one is a combination of based outline which depends upon the authentic routing to detect outbreaks and packet forward behaviour was studied by the utilization of support vector machine (SVM). The recommended approach selected the confidential nodes to perform the routing of packets. Here NS-2 is a testing simulator for this technique. This result proved that APD-JFAD is highly operative in jellyfish attack detection and performed well than existing algorithms.

[17]Proposed a modified AODV routing protocol with the enhancement of RREQ- Route Request and RREP-Route Replies packet protocols. Here, VANET security is one of the important problems as it affects communication among both vehicles to vehicle V-2-V and vehicle to infrastructure (V-2-I). A malicious attack causes the problem in network security and it is required to detect and secure in VANET. Any node has been used as a router and the router-related infectious node will attach a spoofed routing table to many other nodes that influence the network activity. To rectify these issues, modified AODV routing protocol was proposed and cryptographic function-based encryption and decryption were added to check the source as well as destination nodes. Using the NS-2-33 simulator, the proposed solution was illustrated via various system parameters such as drop packets, end-to-end latency, Packet Delivery Ratio (PDR) and overhead routing request. Finally, the outcome showed that in terms of black hole attack and improved network efficiency, the proposed method gave improved results.

[18] Implemented the attack like flooding and black hole attack through enhanced AODV routing protocol. Recently, vehicular connectivity in the area of science and academic industry has increasingly gained visibility. VANET is the structural less network that connects and disconnect automatically. Because of this disconnectivity, the attack can interrupt easily. So to overcome this problem, an enhanced AODV routing protocol was implemented. The simulation was done using Network Simulator Version 2.35. Here, the modifications are done in the source file such as aodv. cc and aodv. h. When testing was done with 3, 5 and 10 nodes, the simulated work demonstrated the working of the AODV protocol. The flooding also was carried out under the Protocol. Based on routing overhead, packet drop ratio, and packet delivery rate, the performance measurements were analyzed. Results showed that the overhead protocol for flooding attack routing is 21.8 percent, but the overhead protocol for black hole attack routing is 18.04 percent. When the packet delivery

ratio of flooding attack is 15.6 % but in black hole attack, it is 10.5% which outperforms AODV.

Due to disruption in network because of the various attacks, AODV routing protocol utilized in the existing approaches. This study also utilized this AODV routing protocol finally for the effective transmission among the unattacked nodes.

C. Black Hole

[19] Proposed a new technique based on common classification algorithms namely ReiefF to choose the most suitable features to generate black hole nodes. This node was marked as a bad node. Denial of service is one of the black hole attacks that damage the process of the network to reduce efficiency.

Experiments are deployed using the simulation environment. The result gave the essential improvement in the network performance varied from 20 % to 40%. [20] Introduced a novel mechanism to find the malicious node. The identification of this node was created with the help of increased data routing information (DRI). Malicious nodes are wrongly advertised as a sensitive path to a destination node throughout the route discovery approach in these types of attacks. This causes complicated nodes when a group of malicious nodes are acted together. To overcome these issues a novel system was introduced which effectively manage the effect of a joint grey-black hole attack[21]. Furthermore, it will be extended using conventional neural network (CNN) to predict the intruder with better accuracy. [22] Proposed a secured MANET routing protocol BPAODV to resolve the security gap related to SAODV. Additionally, the BPAODV is to safeguard against the black hole attack which was established during the routing process. During the forwarding process, the BPAODV guards against the black hole attack. It was further established by enhancing the AODV protocol's functionality. Results revealed that the BPAODV was more secure than SAODV. [23]The probability of the black hole attacks is reduced by proposing an artificial bee colony 2-opt algorithm depending upon the hybrid weighted trust. This research aimed at protecting a MANET with the increasing number of black hole attacks. Here, the hybridization of the algorithm was completed using 2-pt as local search. This had been improved based on the fitness for detecting new results. The resulting method revealed that it enriches the efficiency of factors namely packet delivery ratio, end-end-delay and hop to sink delay. [24] Proposed an upgraded Trust detection procedure to improve the possibility of detecting and preventing the black hole nodes. Here, the nature of the malicious nodes extended the risk of threats and seduces the operations. The proposed outline extracted the nature of the node with the help of several trust metrics. Using Zone routing protocol (ZRP), this technique eliminates the black hole nodes. The result revealed that the proposed method was active with the different parameters such as trust level, energy consumption, false acceptance, packet loss and missing rate of detection.

[25]Studied about the specificity of black hole attack in AODV and DSR. MANET did not need any fixed structure and can be arranged in an aggressive environment where the implementation of the classic network is tough. Here, routing and security are the most preferable consequences for dealing with the MANET's deployment. Both protocols are analyzed with different aspects during the black hole attack. It was analyzed with the measures of end to end delay, packet delivery ratio and throughput. DSR is the better protocol than AODV below black hole attack in the end to end delay but in the packet delivery ratio, AODV is better than DSR. Finally, in the throughput, DSR outperforms than AODV. Result revealed that the analysis was done using the simulation of AODV and DSR below black hole attack and here the AODV is more vulnerable as compared to DSR.

[22] Proposed a secured MANET called BP-AODV (Blackhole Protected AODV) to rectify the security breaches concerning SAODV and AODV. The BP-AODV is capable of protecting over cooperative black hole attack established during the routing process as well as security against black hole attack which can be taken place during the forwarding process. Particularly, during the routing process, the SAODV protocol can secure against black hole attack done through the malicious attack. However, it can support the cooperative black hole attack in which two nodes are malicious node. The BP-AODV was developed using extended functionality of the AODV protocol and also the chaotic map features. Results revealed that the functionality of the BP-AODV protocol is more secure than the SAODV protocol and effectively fought the black hole attack attained by malicious nodes. And the BPAODV can secure over the black hole attack that occurred during the forwarding process.

[26]Utilized Mitigating Black Hole effects through Detection and Prevention (MBDP) protocol based on the dynamic sequence number threshold. To reduce the issues of black hole attack below various network density, MBDP was introduced and based on a threshold value of dynamic sequence number, MBDP AODV protocol was used. Though it enhances the network efficacy concerning throughput and packet delivery and also mitigates the normalized routing load it had overhead of high routing. [27, 28]This research study of Fuzzy differential equation-FDEs subject to fuzzy BCs forms a suitable setting for the mathematical modeling of real-world problems in which uncertainty or vagueness pervades. This paper has introduced a new efficient iterative algorithm for solving fuzzy BVPs by using the RKHS method under the assumption of strongly generalized differentiability.
Malicious nodes are wrongly advertised as a sensitive path to a destination node throughout the route discovery approach in these types of attack namely black hole attack. This attack is addressed in this study effectively using the ICCSO algorithm.

III. PROPOSED WORK

A modern category of wireless networks utilized for communication purposes is the MANETs which functions in extremely energetic and varying surroundings. MANETs are gaining rapid fame in recent days and are considered as very

significant because of their easier implementation and growing property. By the utilization of fixed arrangement or the centralized administration, the set of wireless mobile nodes present within the MANETs can be able to interconnect and transfer information between them. Due to this reason, MANETs attracts applications in various fields. Yet, the elasticity present within the networks gives rise numerous issues related to security. Among various attacks occurring in the MANET, black hole attack is most commonly occurring attacks.

The conventional techniques of securing wireless networks do not employ completely in the case of MANETs. And hence this paves the need for the usage of an Intrusion Detection System (IDS) which contributes significantly to the security of MANET. Therefore an innovative ICCSO (i.e.) Improved Crossover Chicken Swarm Optimization algorithm is proposed for determining the black hole attacks causing within the MANETs. Thus, introduced the concept of Enhanced Partially-Mapped Crossover operation of the chicken based on the best fitness values obtained which provides overall throughput and lower overall delay per packet.The flow of the proposed methodology is illustrated in figure 2.

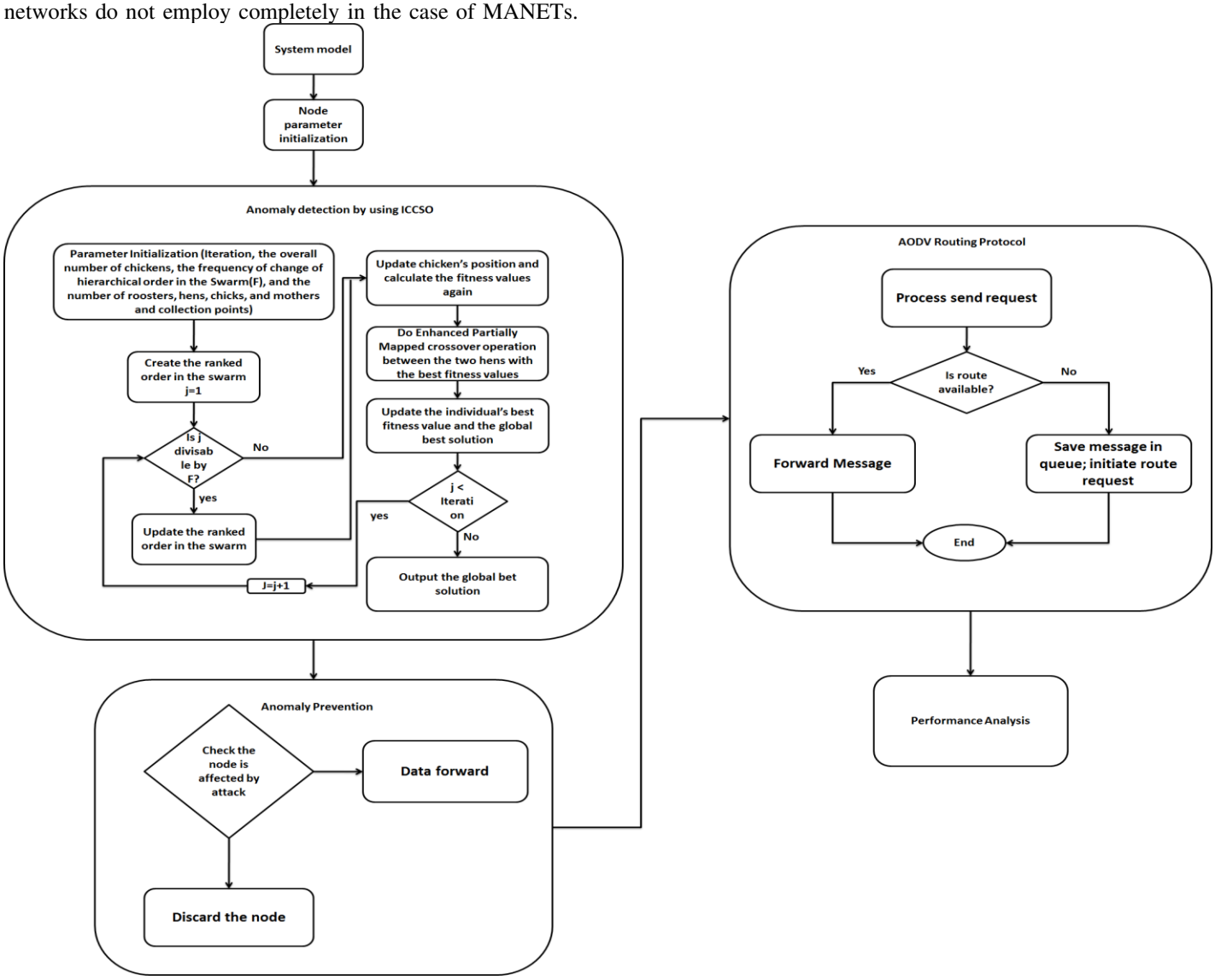

Figure 2. The overall flow of the proposed work

First, the basic model of Mobile Ad-hoc network system is generated. Then node parameter initialization is carried out in step 1 of the algorithm, where the attacked nodes and non-attack nodes are created separately with the aid of parameters like PDR (i.e.) Packet Delivery Ratio and RSSI (i.e.) Received Signal Strength Indicator. Then the anomaly or the abnormalities present within the network are detected by the usage of proposed Improved Crossover Chicken Swarm Optimization (ICCSO) algorithm. This algorithm is formulated for rectifying the shortcomings of the conventional CSO algorithm which is in the usage. An enhanced partially mapped crossover operation is introduced newly in the proposed algorithm. The required parameters like the number of iterations, number of chickens and frequency of hierarchical order changing in the chicken swarm etc. are initialized in step 3 to step 7. The nodes are taken as chickens in step 1 of the

algorithm. The suitable ranked order in the chicken swarm is created. Based on the fitness value of the chicken, the initial ranked order is defined. The frequency of transition in hierarchical order in the swarm is denoted as G_{freq} in step 3 of the algorithm. In step 17, the ranked order gets updated, if it gets divisible by hierarchical order G_{freq}. If it does not gets divisible by F (i.e.) G_{freq}, the ranked order does not gets updated and proceeds directly for updating the position of chickens like roosters, hens and chicks. Then in the same step fitness values are evaluated once again. Then, enhanced partially mapped crossover operation is carried out by selecting two hens that possess higher fitness value. An individual's best fitness value and global best solutions are attained and get updated. The quality of the best solution is enhanced by some rate through this operation. Hence all the roosters are attracted by the global optimum. It is suitable for dealing with the final restriction of the problem.

Then just before the last step of the algorithm, the anomaly detected can be prevented by determining both the anomaly and non-anomaly separately by the usage of the proposed ICCSO algorithm. If the node is affected by any attack, then the nodes are discarded and the data is transmitted through the non-attacked node.

Afterwards, a routing protocol is performed in the final step of the algorithm. Routing is carried by a protocol of AODV. In AODV protocol, a source node initiates a unique and separate routing discovery process, whenever it needs to distribute the desired data to the destination node. Route Request packet (RREQ) is formed by the source node. Various information like IP address of the source node, sequence number of the source node, IP address of the destination node, sequence number of the destination node and broadcast ID are all contained within the formed RREQ packet. The value of the hop count field is also set to zero. These RREQ packets are distributed to all the neighbours by the source node. But before distributing it to the neighbouring nodes, it must be properly checked that whether the neighbour nodes already consist of the RREQ. If it already possesses the RREQ, it must be discarded before the distribution of RREQ by the source node. Process request is sent by the AODV routing protocol. If the route is possible, the message is forwarded and similarly if the route is not possible, the message is saved in the queue then the route request is initiated.

Algorithm for ICCSO

---

1. Parameter initialization
   1. $N_{chicken} \rightarrow Total\ no\ of\ chickens$ or population(nodes)
   2. $M_{iter} \rightarrow Iteration$
   3. $G_{freq} \rightarrow Frequency\ of\ transition\ in\ hierarchical\ order\ in\ the\ swarm$
   4. $N_{rooster} \rightarrow number\ of\ rooster$
   5. $N_{hens} \rightarrow number\ of\ hens$
   6. $N_{chicks} \rightarrow number\ of\ chicks$
   7. $N_{mothers} \rightarrow number\ of\ mothers$
   8. $D_{solu} \rightarrow Solution\ dimension$
   9. $Upper_{bound} \rightarrow set\ upper\ limit(Max\ node)$
   10. $lower_{bound} \rightarrow set\ lower\ limit(Min\ node)$

Create the ranked order in the swarm

11. $For\ \ each\ population$
    $fit_{val}(i)$
    $\rightarrow calculate\ the\ fitness\ function\ for\ each\ node$
    end
12. $best_{fitness} \rightarrow fit_{val}$
13. $best_{position} \rightarrow N_{chicken}$
14. $best_{index} \rightarrow Calculate\ the\ minimum\ index\ of\ the\ fit_{val}$
15. $best_{min} \rightarrow Calculate\ minumum\ \ fit_{val}$
16. $X_{best} \rightarrow N_{chicken}(best_{index})$
17. $For\ l = 1\ \ to\ \ M_{iter}$
    $FL_{val} \rightarrow Randomly\ initialization$
    $If\ l\ is\ divisible\ by\ G_{freq}$

// Update the hierarchical order in the swarm

Sort the $best_{fitness}$ in ascending order, compute the index $index_{sort\_as}$ and sorted value

Randomly select $N_{mothers}$ hens which would be the mother hens $m_{lib} \rightarrow randperm(N_{mothers} + N_{hens}) + N_{rooster}$

Randomly select the hens mate

$m_{mate} \rightarrow randperm(N_{rooster} + N_{hens})$

$mother_{sel} \rightarrow m_{lib}(rand)$

$End\ if$

Update the positions of roosters, hens, and chicks and calculate the fitness values again

// update the rooster value

$For\ i\ to\ N_{rooster}$

Randomly select another rooster

$Ano_{roo} \rightarrow randitabu(1, N_{rooster}, i, 1)t_{sig}$

$$= \begin{cases} 1 & if \begin{pmatrix} best_{fitness}\left(index_{sort_{as}}(i)\right) \leq \\ best_{fitness}\left(index_{sort_{as}}(Ano_{roo})\right) \end{pmatrix} \\ exp \dfrac{best_{fitness}\left(index_{sort_{as}}(Ano_{roo})\right) - best_{fitness}\left(index_{sort_{as}}(i)\right)}{\left|best_{fitness}\left(index_{sort_{as}}(i)\right)\right|} \end{cases}$$

$$N_{chicken}\left(index_{sort_{as}}(i)\right) = best_{position}\left(index_{sort_{as}}(i)\right) * \left(1 + t_{sig} * rand\right)$$

$N_{chicken}\left(index_{sort_{as}}(i)\right) = update\ the\ new\ move$

$fit_{val}\left(index_{sort_{as}}(i)\right) \rightarrow$U

$pdate\ the\ fitness\ value\ for\ corresponding\ \ fit_{val}\left(index_{sort_{as}}(i)\right)$

End for

// update the hens value

$For\ i\ =\ N_{rooster} + 1\ to\ N_{rooster} + N_{hens}$

Randomly select another chicken

$temp_{other} \rightarrow randitabu(1, i, m_{mate}(i - N_{rooster}), 1)$

$$c_{mate1} \rightarrow exp \frac{best_{fitness}\left(index_{sort_{as}}(i)\right) - best_{fitness}\left(index_{sort_{as}}(i - N_{rooster})\right)}{\left|best_{fitness}\left(index_{sort_{as}}(i)\right)\right|}$$

C_{mate2}

$\rightarrow exp^{-best_{fitness}\left(index_{sort_{as}}(i)\right)+ best_{fitness}\left(index_{sort_{as}}(temp_{other})\right)}$

$N_{chicken}\left(index_{sort_{as}}(i)\right)$

$= best_{position}\left(index_{sort_{as}}(i)\right)$

$+ best_{position}\left(index_{sort_{as}}(m_{mate}(i\right.$

$\left.- N_{rooster}))\right)$

$- best_{position}\left(index_{sort_{as}}(i)\right) * c_{mate1}$

$* rand$

$* best_{position}\left(index_{sort_{as}}(temp_{other})\right)$

$- best_{position}\left(index_{sort_{as}}(i)\right) * c_{mate2}$

$* rand$

$N_{chicken}\left(index_{sort_{as}}(i)\right) = update\ the\ new\ move$

$fit_{val}\left(index_{sort_{as}}(i)\right) \rightarrow$U

$pdate\ the\ fitness\ value\ for\ corresponding\ fit_{val}\left(index_{sort_{as}}(i)\right)$

End for

// update chicks value

$For\ i = N_{rooster} + N_{hens} + 1\ to\ N_{chicken}$

$N_{chicken}\left(index_{sort_{as}}(i)\right)$

$= best_{position}\left(index_{sort_{as}}(i)\right)$

$+ best_{position}\left(index_{sort_{as}}(mother_{sel}(i\right.$

$\left.- N_{rooster} - N_{hens}))\right)$

$- best_{position}\left(index_{sort_{as}}(i)\right) * FL_{val}(i)$

End for

Select the two hens do the cross over operation and replace that value into worst hens place

Update the individual's best fitness value and the global best one

$For\ i\ to\ N_{chicken}$

$If\ (\ fit_{val}(i) < best_{fitness}(i))$

$best_{fitness}(i) = fit_{val}(i)$

$best_{position}(i) = N_{chicken}(i)$

$End\ if$

$If\ (best_{fitness}(i) < best_{min})$

$best_{min} = best_{fitness}(i)$

$X_{best} = best_{position}(i)$

$End\ if$

end

end

2. To find the anomaly/non-anomaly node by suing ICCSO algorithm.
3. Attacked node are discarded, finally data transmitted through only non-attacked node via ADOV protocol

IV. RESULTS AND DISCUSSION

The proposed algorithm has been implemented and evaluated on NS-3 and all the simulation information are provided. The ratio of packet transmission-PDR and throughput was found to be significantly higher and the end-to-end delay was lower than the normal black hole attack AODV. Three parameters can be used for calculating the algorithm's efficiency:

(A) Packet Delivery Ratio (PDR): It is a ratio of pocket number received to the pocket number sent.

(B) Throughput: The speed of transmission of information through a network.

(C) End to End Delay: It takes time for packets to reach the source destination.

4.1 Environmental configuration:

In the proposed study, the comparison and verification of the test implemented on Windows 8 operating system. Executing the proposed study using the python 3.7, anaconda spyder IDE environment. The hardware and software configuration is in table form below.

Table 3- Environmental configuration

Hardware Configuration	Software Configuration
CPU - Intel Core i7 – 7700 @ 2.80 GHz	Windows 8
GTX 1050	Python 3.7
16GB RAM	Anaconda Spyder

4.2 Comparative Analysis:

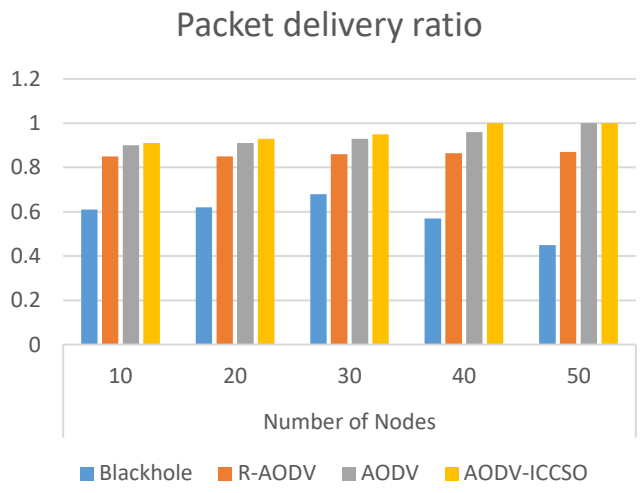

Figure 3. (a) Packet Delivery Ratio (PDR)[29]

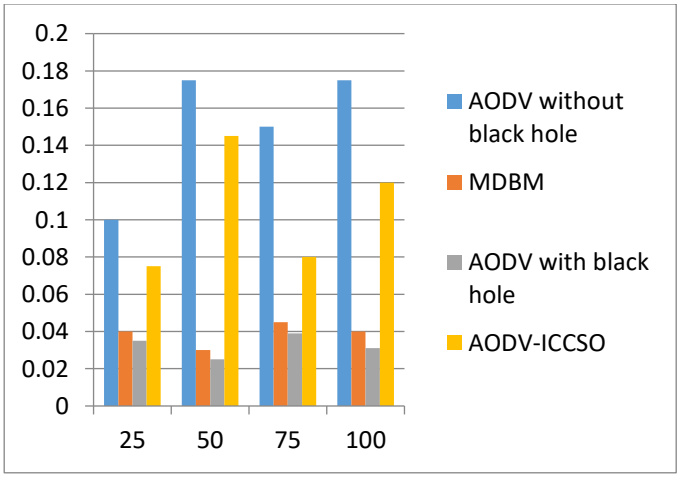

Figure 3. (b) Packet Delivery Ratio (PDR)[30]

Figure 3 (a) and (b) exhibits the packet delivery ratio of the proposed system compared with existing studies[29, 30]. This is a ratio of the number of forwarded packets to the number of total packets. PDR value of the proposed algorithm is noticed higher than the existing routing protocols. In figure 3 (b) AODV with black hole and without black is mentioned and stated as 0.21 and 0.031 which the AODV without black holes shows lesser value.

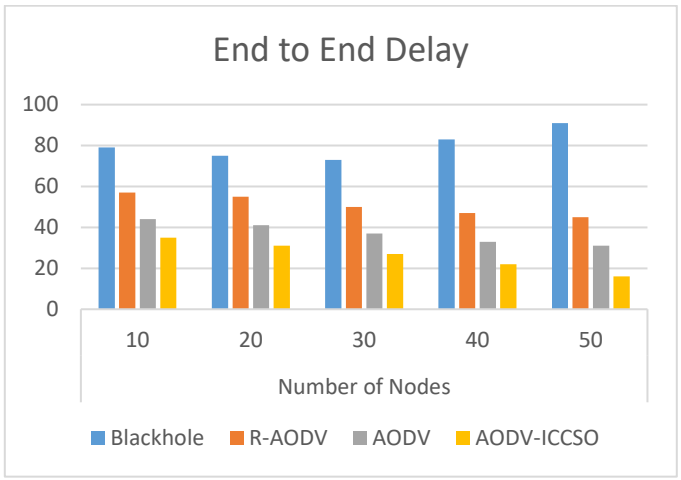

Figure 4. (a) End to End Delay (EED)[29]

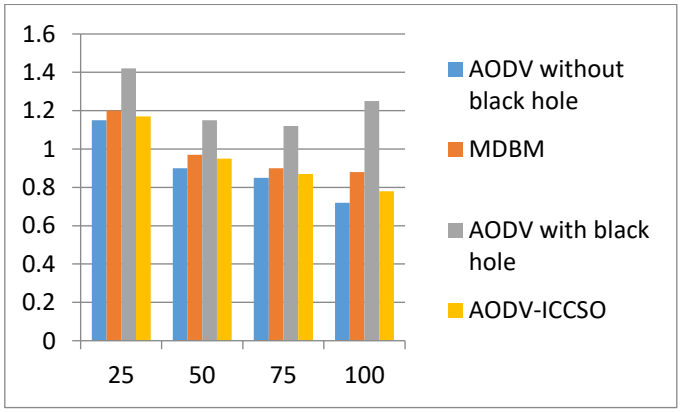

Figure 4. (b) End to End Delay (EED)[30]

Figure 4 (a) and (b) exhibits the End to End delay compared with existing studies[29] [30], In figure 3 (b) AODV with black hole and without black is mentioned and stated as 1.25 and 0.72 which the AODV without black hole had lesser value.

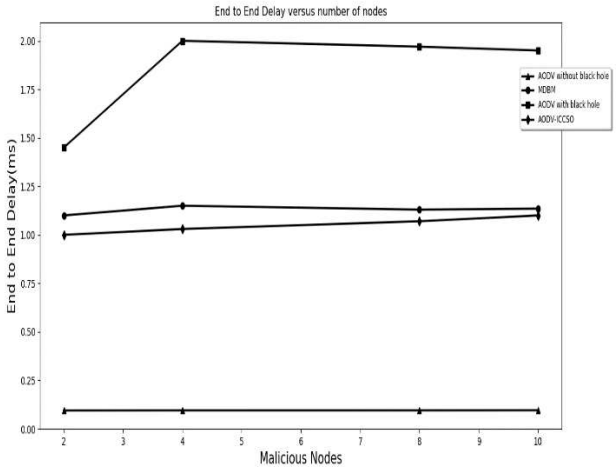

Figure 4. (c) End to End Delay (EED) in malicious nodes [30]

Figure 4 (a), (b) represents the comparison of end to end delay (EED) and (c) gives the comparison of EED in malicious nodes. The time taken by the packet from the source to the destination is lower for the proposed algorithm when comparing with other existing routing protocols.

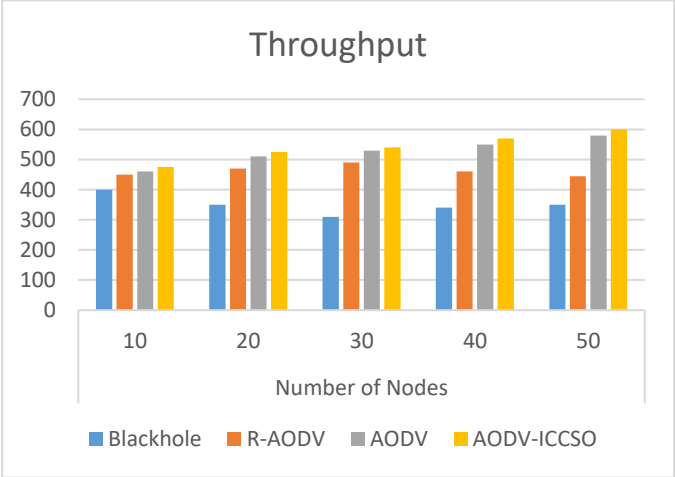

Figure 5. (a) Throughput[29]

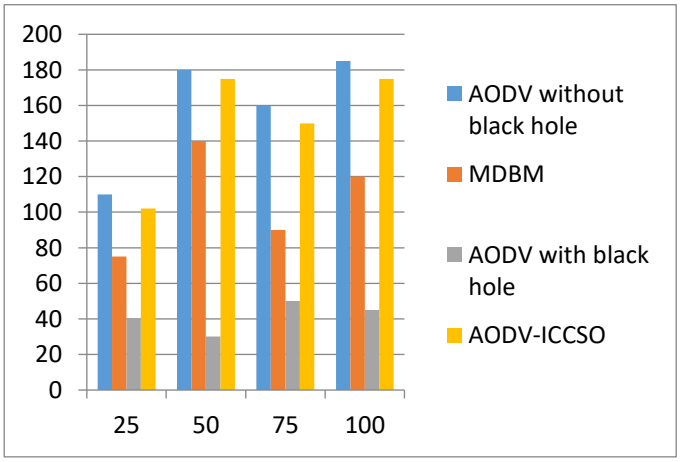

Figure 5. (b) Throughput [30]

Figure 5(a) and 5(b) Figure 3 (a) and (b) exhibits the throughput. Throughput value of the proposed algorithm is noticed higher than the existing routing protocols. In figure 5 (b) AODV with black hole and without black is mentioned and stated as 45 and 185 which the AIDV without black hole had higher throughput.

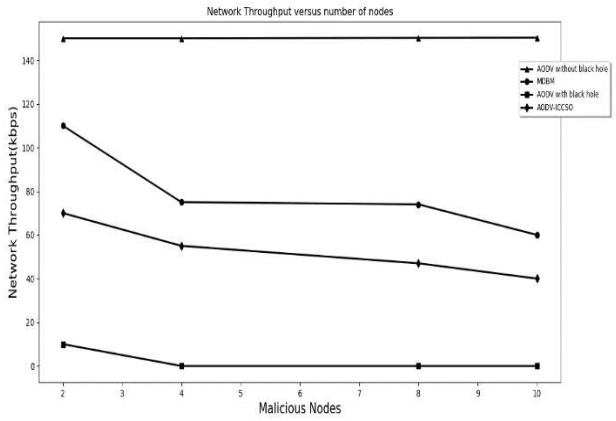

Figure 5. (b) Throughput in malicious nodes [30]

Figure 5 (a), (b) provides the throughput comparison of the proposed algorithm with different routing protocols and similarly (c) gives throughput comparison in malicious nodes. It can be seen that the proposed algorithm comes up with higher throughput value.

From the above results, it clearly observed that packet delivery ratio is high by using AODV protocol and the proposed ICCSO algorithm performed effectively while addressing black hole attack. Further, the End-to-End delay is reduced compared with the state of arts approaches. Higher throughput resulted by reducing the malicious nodes with black hole attack. Thus the proposed algorithm performed better in terms of throughput, end-end delay and packet delivery ratio.

V. CONCLUSION

This study focused on the black hole attack which is generally occurs on MANET. Thus to address this issue, Improved Crossover Chicken Swarm Optimization and the Enhanced Partially-Mapped Crossover operation concept introduced which addressed this issue and provides overall throughput and lower overall delay per packet. Based on the proposed system the best fitness values have been obtained. The efficiency of the proposed system was examined through several performance analysis concerning packet to delivery ratio, throughput and end to end delay and proved that the study outperforms the state of art methods by providing optimized results.

VI. COMPLIANCE WITH ETHICAL STANDARDS STATEMENTS

Ethical approval

No animals or human participants are involved in this research work.

Funding

This research work was not funded by any organization/institute/agency.

Conflict of interest

I confirm that this work is original and has either not been published elsewhere, or is currently under consideration for publication elsewhere. None of the authors have any competing interests in the manuscript.

Informed Consent

I confirm that any participants (or their guardians if unable to give informed consent, or next of kin, if deceased) who may be identifiable through the manuscript (such as a case report), have been given an opportunity to review the final manuscript and have provided written consent to publish.

Data Availability Statement

N/A

Author's contribution

I Am Sathyaraj P Hereby State That The Manuscript Title Entitled “Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs” Submitted To Soft Computing , I Confirm That This Work Is Original And Has Not Been Published Elsewhere, Nor Is It Currently Under Consideration For Publication Elsewhere. And I Am Assistant Professor in the Department of ECE, R.M.K College of engineering and Technology, Chennai.

I’m the corresponding author of our paper, my contribution work on this paper is to Writing, developing, and reviewing the content of the manuscript. And my co-authors Rukmani Devi D, Dr.K. Kannan works were to cite the figure, table and references. I have done 50% and my Co-Authors have equally done 50%. We are the entire contributors of our paper. And no other third party people are not involved in this paper.

REFERENCES

[1] R. A. Sowah, K. B. Ofori-Amanfo, G. A. Mills, and K. M. Koumadi, "Detection and Prevention of Man-in-the-Middle Spoofing Attacks in MANETs Using Predictive Techniques in

Artificial Neural Networks (ANN)," *Journal of Computer Networks and Communications,* vol. 2019, 2019.

[2] Z. A. Khan and P. Herrmann, "Recent Advancements in Intrusion Detection Systems for the Internet of Things," *Security and Communication Networks,* vol. 2019, 2019.

[3] A. Umbarkar and P. Sheth, "CROSSOVER OPERATORS IN GENETIC ALGORITHMS: A REVIEW," *ICTACT journal on soft computing,* vol. 6, no. 1, 2015.

[4] M. Adam, D. Werner, C. Wendt, and A. Benlian, "Containing COVID-19 through physical distancing: the impact of real-time crowding information," *European Journal of Information Systems,* pp. 1-13, 2020.

[5] Y. Wu, B. Yan, and X. Qu, "Improved chicken swarm optimization method for reentry trajectory optimization," *Mathematical Problems in Engineering,* vol. 2018, 2018.

[6] T. Li, J. Ma, and C. Sun, "SRDPV: secure route discovery and privacy-preserving verification in MANETs," *Wireless Networks,* vol. 25, no. 4, pp. 1731-1747, 2019.

[7] T. Kavitha, K. Geetha, and R. Muthaiah, "India: Intruder Node Detection and Isolation Action in Mobile Ad Hoc Networks Using Feature Optimization and Classification Approach," *Journal of medical systems,* vol. 43, no. 6, p. 179, 2019.

[8] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security Challenges and Attacks in Dynamic Mobile Ad Hoc Networks MANETs," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019: IEEE, pp. 28-33.

[9] M. Ponnusamy, "Detection of Selfish Nodes Through Reputation Model In Mobile Adhoc Network-MANET," *Turkish Journal of Computer and Mathematics Education (TURCOMAT),* vol. 12, no. 9, pp. 2404–2410-2404–2410, 2021.

[10] A. S. Babu, "Study for Enhanced Intrusion Detection and Response System for MANET," *International Journal of Research in Engineering, Science and Management,* vol. 3, no. 5, pp. 252-253, 2020.

[11] M. Deshmukh and S. Kakarwal, "Proactive Neighbor Knowledge-based Hybrid Broadcasting in MANET," 2019.

[12] D. K. Verma, R. Jain, and A. Kush, "Intrusion Detection using RREP Messages Of AODV Routing Protocol," *International Journal of Applied Engineering Research,* vol. 12, no. 9, pp. 1956-1961, 2017.

[13] S. Shahabi, M. Ghazvini, and M. Bakhtiarian, "A modified algorithm to improve security and performance of AODV protocol against black hole attack," *Wireless Networks,* vol. 22, no. 5, pp. 1505-1511, 2016.

[14] A. Kumar *et al.*, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems,* vol. 80, p. 103352, 2021.

[15] A. M. Bamhdi, "Efficient dynamic-power AODV routing protocol based on node density," *Computer Standards & Interfaces,* vol. 70, p. 103406, 2020.

[16] S. Doss, A. Nayyar, G. Suseendran, S. Tanwar, A. Khanna, and P. H. Thong, "APD-JFAD: accurate prevention and detection of jelly fish attack in MANET," *Ieee Access,* vol. 6, pp. 56954-56965, 2018.

[17] A. Kumar *et al.*, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors and Microsystems,* p. 103352, 2020.

[18] A. Kumar and M. Sinha, "Design and analysis of an improved AODV protocol for black hole and flooding attack in vehicular ad-hoc network (VANET)," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 4, pp. 453-463, 2019.

[19] F. Albalas, M. B. Yaseen, and A. Nassar, "Detecting black hole attacks in MANET using relieff classification algorithm," in *Proceedings of the 5th International Conference on Engineering and MIS*, 2019: ACM, p. 22.

[20] M. C. Trivedi and S. Malhotra, "Identification and Prevention of Joint Gray Hole and Black Hole Attacks," *International Journal of Ambient Computing and Intelligence (IJACI),* vol. 10, no. 2, pp. 80-90, 2019.

[21] S. Naveena, C. Senthilkumar, and T. Manikandan, "Analysis and countermeasures of black-hole attack in manet by employing trust-based routing," in *2020 6th international conference on advanced computing and communication systems (ICACCS)*, 2020: IEEE, pp. 1222-1227.

[22] A. M. El-Semary and H. Diab, "BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map," *IEEE Access,* vol. 7, pp. 95185-95199, 2019.

[23] V. Keerthika and N. Malarvizhi, "Mitigate Black Hole Attack Using Hybrid Bee Optimized Weighted Trust with 2-Opt AODV in MANET," *Wireless Personal Communications,* vol. 106, no. 2, pp. 621-632, 2019.

[24] J. Manoranjini, A. Chandrasekar, and S. Jothi, "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework," *Automatika,* pp. 1-11, 2019.

[25] N. Panda and B. K. Pattanayak, "Analysis of Blackhole Attack in AODV and DSR," *International Journal of Electrical and Computer Engineering,* vol. 8, no. 5, p. 3093, 2018.

[26] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET," *Wireless Networks,* vol. 25, no. 4, pp. 1685-1695, 2019.

[27] O. A. Arqub, M. Al-Smadi, S. Momani, and T. Hayat, "Application of reproducing kernel algorithm for solving second-order, two-point fuzzy boundary value problems," *Soft Computing,* vol. 21, no. 23, pp. 7191-7206, 2017.

[28] O. A. Arqub and M. Al-Smadi, "Fuzzy conformable fractional differential equations: novel extended approach and new numerical solutions," *Soft Computing,* pp. 1-22, 2020.

[29] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET," in *Smart Innovations in Communication and Computational Sciences*: Springer, 2019, pp. 271-279.

[30] M. S. Pathan, J. He, N. Zhu, Z. A. Zardari, M. Q. Memon, and A. Azmat, "An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs," *International Journal of Advanced computer Science and Applications,* vol. 10, no. 1, pp. 243-251, 2019.