INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

MOpt Shield: An Intrusion Detection System based on Meld Optimization Algorithm to mitigate Amalgam Attacks

Jaspreet Kaur[1]*, Rajneesh Talwar[2], Ashok Kumar Goel[3]

1 Research Scholar, I.K. Gujral Punjab Technical University, Jalandhar, Punjab, India
2 Director Engineering, CGC Jhanjeri, India
3 Professor, Department of ECE, GZS Campus College of Engineering and Technology, MRSPTU, Bathinda, India

OPEN ACCESS
Received: 08.04.2021
Accepted: 07.05.2021
Published: 04.06.2021

Citation: Kaur J, Talwar R, Goel AK (2021) MOpt Shield: An Intrusion Detection System based on Meld Optimization Algorithm to mitigate Amalgam Attacks. Indian Journal of Science and Technology 14(20): 1622-1634. https://doi.org/10.17485/IJST/v14i20.601

* **Corresponding author**.

jaspreetwphd@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Background/Objectives: To mitigate network from amalgam attacks, this study is focussed on designing an efficient approach that can prevent the networks from intruders and secure the communication. **Methods:** A crossbreed approach, named 'MOpt Shield,' is proposed in this study. This proposed protocol utilizes the efficacy of the existing Cuckoo Search and Firefly Optimization Algorithm on basic AODV protocol along with the promising factors of the Intrusion Detection System. The proposed protocol is simulated using an NS-2 simulator with two different simulation scenarios, and PDR, Throughput, PLR, and Delay parameters are considered performance measures for the same. **Findings:** The proposed protocol finds the best selected nodes for communication and prepare separate list for the doubted nodes which further analyzed for attacker or non-attacker nodes. This will help to identify the best path with high energy and other capabilities for the efficient transmission of data. The performance of this proposed protocol is analyzed under 5 attacker nodes in which 2 are blackhole and 3 are DoS attacker nodes. For simulation, the scenario includes minimum 5 connections and maximum 25 connections between the 50 nodes with CBR traffic and 20m/s speed. The evaluated results show the astounding performance of the proposed protocol over the other existed protocols in terms of PDR, Throughput and Delay, and hence it reveals its capabilities. **Novelty/Applications:** The proposed protocol effectively handles the amalgam attacks and its novelty lie in its features of hybrid optimization and intrusion detection approach to find the route of transmission and the trusty nodes.

Keywords: MOpt Shield; Crossbreed; Cuckoo Search; Firefly Algorithm; Amalgam Attacks; Blackhole; DDoS; NS2 simulator

1 Introduction

With the advent of technology, most of the services become online provided by various service providers. These services' main components are network architecture that plays a vital role in transmitting data and services. Adhoc is one of them where it offers services in agriculture, military, education, and many more. Nowadays, all the facilities to provide these services are available in the market, and these devices are well suited for such areas to provide services to the users. Mobility, Adaptability, Computation, and Battery power are features of these devices to build an Adhoc network. All these features are for a limited period, so there are some restrictions in using the devices[(1)]. The main problem arose when it lost its battery power because the maximum features are dependent on this. All becomes unavailable in the absence of battery power and results in poor performance. The researchers developed a significant number of techniques to increase the performance parameters based on numerous factors. But nowadays, forged attacks have become a prominent reason for the poor performance of the network. In MANET, it was found that several attacks compromised the security of data and other vital parameters. Forged nodes were performing their attempts to be successful so that vulnerabilities can find out in the system, and accordingly, the attack can also be imposed on the network. The primary reason behind this security comprise is as given below:

- In MANET, every node is a forwarder and is considered a capable node. It is not necessary that every node can handle the risk of security, which may compromise information security.
- Because of its temporary and dynamic behavior, this network is considered an Adhoc network, which means it is usually created for a short time. So, this network can also be regarded as a temporary network. The network is created temporarily among nodes that want to communicate with each other. In this network, nodes are movable, and they may change their location dynamically.
- As the network is infrastructure-less in MANET, so, nodes participating in this network depend upon resources that are carried by these nodes themselves. When good and sufficient resources are required, a node may look for such type of intermediate node. If any malicious node will come and be selected with such provisions, security may be easily compromised.
- The selection of an intermediate node for routing is an essential step in MANET. In most cases, every node needs to send its packet to the destination by the following route. Suppose a malicious node presents itself as the most-nearest node of the goal during the route discovery phase and is selected based on it. In that case, this forged node can start getting access to information, and the probability of security compromise increases accordingly.

So, any of the above reasons may be the cause of compromised security in the Adhoc network. MANET Attacks are categorized into two types: (a) Active Attacks and (b) Passive Attacks. In the active attack, attackers can access the data or node and modify or drop it, whereas passive attacks contain silent attackers that listen to the traffic or nodes. Blackhole and DDoS[(2)] attacks are under the active attacks category, and their combination is considered in this paper. The paper's following sections delineate some of the existing approaches to deal with the blackhole, DDos, and hybrid Attacks. The proposed protocol is also described in the coming section and the implementation and analysis of it.

2 Related Work

This section deals with the work done by various researchers on forged networks. It also discusses the optimization techniques used in Mobile Adhoc Network to provide security and route optimization.

Hybrid approaches are nowadays popular among the other methods in almost every field. It also provides some benefits in the area of MANETs to cater to security against various attacks. Like, Justin et al.[(3)] proposed an SVM-based Hybrid Intrusion Detection System to detect DoS attacks in MANETs. This proposed approach reduces the training time and includes signature and anomaly-based methods to detect malicious nodes. They calculated the results only for the detection of forged nodes and achieved 100% for the same. The other hybrid approach was proposed by Funde and Chourasia[(4)] to detect hybrid attacks in MANETs. Here, hybrid attacks mean the combination of more than one attack. They also used SVM and the dendritic cell algorithm to detect normal and abnormal traffic. They also achieved 100% accuracy for the detection of attackers or anomalous traffic data.

Furthermore, anomaly-based IDS was proposed by Kaur and Singh[(5)] to detect and prevent the network from DDoS attacks. They simulate the proposed approach using a network scenario with 30 nodes in an 800 x 800 area. The performance was analyzed based on different performance metrics and hence conclude that the proposed approach works as a defensive approach in the presence of DDoS attackers. The other method to deal with DDoS attacks was proposed by Gautam et al.[(6)]. They implemented AODV, SAODV, and HWMP protocol using an NS-2 simulator and evaluated the performance by conducting the ANOVA test. They considered the MANETs scenario for the healthcare system and perceived the need for the security approach. From the performance analysis, they elect the best protocol, which is less vulnerable to DDoS attacks.

Moreover, Optimization-based approaches also play a vital role in mitigating the attacks and provides security. Keerthika and Malarvizhi[(7)] proposed a trust-based Bee optimization algorithm with 2-Opt AODV. This hybrid approach used the artificial bee colony algorithm and improved it using the 2-Opt process to evaluate the local search by combining global optimization effectively. The results of the proposed approach justify its effectiveness against the Blackhole attack. For mobile Adhoc networks in IoT, Gowrishankar et al.[8] proposed a trust-based protocol. In this, the sensor nodes have direct, indirect, and mutual trust between them, and they calculate the combined trust values based on a probability distribution on the individual trust values. The results demonstrate the efficiency of the proposed protocol. Pathan et al.[9] proposed another trust-based approach in which the best and reliable path was selected to ensure secure communication.

Cryptography is another approach to secure the data and information from malicious users, and it can be more beneficial for passive attacks. Naveena and Reddy[10] proposed a hybrid security model, where they used anonymity, one-way trapdoor protocol, hash functions, and elliptic curve cryptographic approach to mollify the attacks. They presented this hybrid model to provide security for different layers. They simulate the proposed model using an NS-2 simulator and prove the performance efficacy in various parameters. The other cryptography-based security approach was proposed by Hossain et al.[11]. In this, they used an SHA-3 and Diffie Hellman algorithm to select appropriate routes. They implemented the proposed approach on both AODV and AOMDV protocols using an NS-2 simulator. The proposed approach's performance is evaluated based on different parameters, concluding the proposed solution's potency.

The Timer-based Baited technique was proposed by Yasin and Zant[12] for the detection and evacuation of the Blackhole attack. This proposed approach worked in two phases: Baiting and Non-neighbour response, and based on that, they detect the blackhole nodes and add them to the blacklist. The proposed approach results were calculated both with a single blackhole node and cooperative blackhole nodes and figured out that the proposed approach's performance was improved. Optimization plays an inevitable role in various fields, and communication optimization is one of them. It selects the optimized and best route while data is traveling from source to destination. Nowadays, optimization is also opted in the field of the network to provide security. Mukhedkar and Kolekar[13] proposed an optimization-based approach and combined it with the Encrypted trust-based system to protect the Mobile Adhoc Network. The glowworm swarm optimization (GSO) algorithm was used to detect the attackers and achieve the 99% detection rate. The other Cuckoo search and M-tree-based approach were proposed by Babu and Ussenaiah[14] to enhance the Adhoc network's performance. The other heuristic and metaheuristic approaches based on an optimization algorithm were developed by several researchers[15–28] that optimize the network's performance and provide a secure communication environment.

Hybrid attacks deteriorate the mobile Adhoc network's performance; its detection and prevention must maintain the network's performance. Joshi and Mishra[29] dealt with the rushing and data modification attack simultaneously and proposed a detection algorithm for this. They proposed a trust-based approach and tested performance based on different measures. The other hybrid attack scenario was proposed by Tahboush and Agoyi[30] and analyses its effect with and without detection algorithm.

3 Mopt Shield: An Intrusion Detection System Based on Meld Optimization

MOpt Shield also called Meld Optimization Shield, which helps to protect the network from different attacks. This shield saves every node of a network from the attacker and works as a safeguard, as shown in the figure. The attacker may or may not be a part of the network, but it always tries to harm the network either by data loss or link breaks. So, it is the necessity of the network that intruders can be avoided somehow. For this, a proposed shield uses an intrusion detection system. It added an optimization algorithm for efficient route selection that directly or indirectly protects the attacker nodes based on different parameters. This is named meld optimization because it contains two different algorithms, Firefly Algorithm (FA) and Cuckoo Optimization Algorithm (COA), that works together to form a perfect route while transferring data from one node to another node in Mobile Adhoc Networks (MANETs).

The base protocol used to implement this is the AODV protocol that sends the request packet to find the data transmission route and select the best path. In this proposed protocol, the aim is not to provide the best approach; the main focus is to find the ideal route that protects the data from intruders and delivers it effectively. This protocol works end to end for more robust results and record the elements to handle different attacker types at one go. These elements are based on some parameters and are calculated before the transmission.

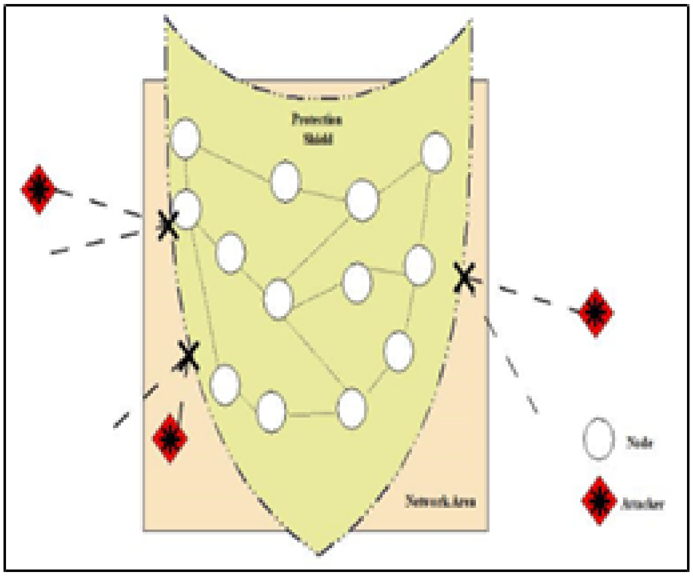


Fig 1. Protection Shield on Network

Some of the general parameters that are considered in this work are Packet Drop Count (λ), Packet Forward Count (μ), Energy (Ę), Packet Receiving Time (Ť) & Packet Sending Time (Ŧ) for different packets, and Accumulate Delay (⊠). These parameters are calculated for each node that will participate in the communication process and stored in different tables.

3.1 Mathematical Formulations

A network with 'n' number of nodes communicates with each other and transfers their data from one end to another end. Data is traveled through the network by following different routes, say 'k' routes, in bits. The Adhoc network's example, so nodes of the network work as a forwarder and transfer the data. So, whenever a node sends or receives the packets, it computes the following parameters:

Firstly, the Packet Travelling Time (⊠) is calculated, it is defined as a time for which a packet traveled from source to destination, and it is calculated based on Packet Receiving Time (Ť) & Packet Sending Time (Ŧ) using the following formula:

$$\mathrm{P} = \check{\mathrm{T}} - \mathrm{T} \tag{1}$$

Then Packet Roaming Time ($\varnothing$) is calculated for both request and reply packet using the following equation:

$$\varnothing = \varnothing_{RREQ} = \varnothing_{RREP} = n * \frac{\gamma}{\delta} \tag{2}$$

Here, n is the number of nodes through which the packet traveled, the transmission range, and the network's propagation speed.

Delay (φ) is an essential factor that defines the performance of a network protocol, so here delay is calculated as:

$$\varphi = -(\varnothing_{RREQ} + \varnothing_{RREP}) \tag{3}$$

Here, Accumulated Delay (⊠) is calculated and used to provide QoS for the path selection process. This factor is dependent on the Delay factor and is calculated as:

$$(i) = \ (i-1) + \varphi(i) \tag{4}$$

Where i=1,2,3,……n and, $(1) = 0$

The other factor like Energy (Ę), has a significant impact on the performance, and it is calculated both at transmitting and receiving node, is calculated as:

The Energy at Transmitter side:

$${}_{T}(b,d) = {}_{F}(b) + {}_{R}(b,d) \tag{5}$$

where b is the number of bits d is the distance between the nodes. $_F$ is the energy dissipated per bit to forward a packet and $_R$ is the energy dissipated per bit to receive a packet and the following formula calculates it:

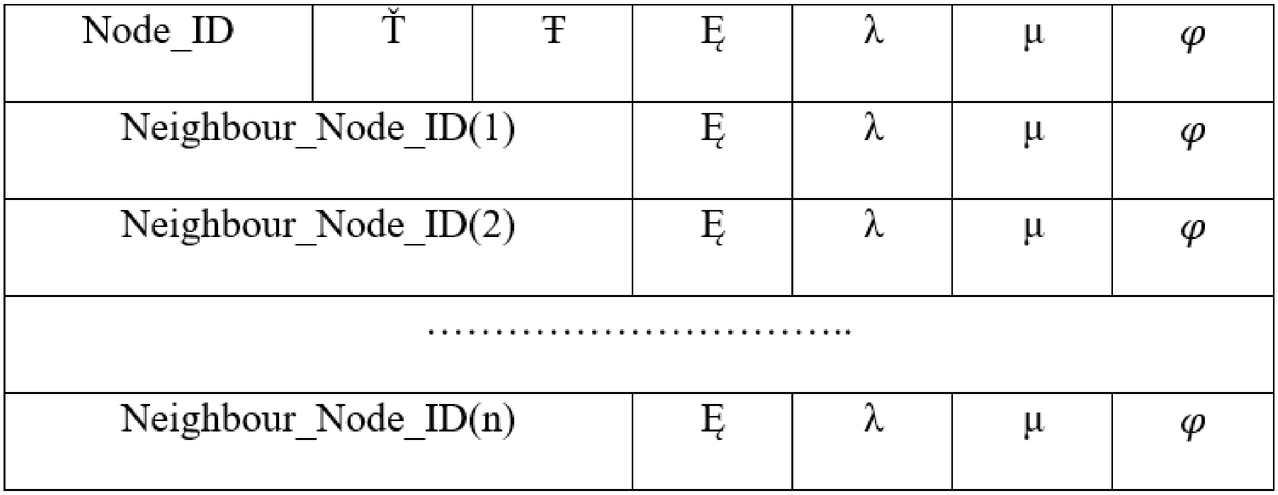
$$_R\,(b,d) = {}_F\,(b) \tag{6}$$

All the above factors are calculated and used to perform a different operation.

3.2 Data Structure

Some of the additional data structures are required to store the computed information during the packets' transmission. So, some new data structures, like Node Table and Bin, are added to this protocol. Also, few additions are there in the existing routing table. The description of each data structure is given in this section.

(a) Node Table (NT): this new data structure stores the additional parameters calculated at the source node that includes Packet Receiving Time (Ť) & Packet Sending Time (Ŧ). It also stores its neighbor node information.

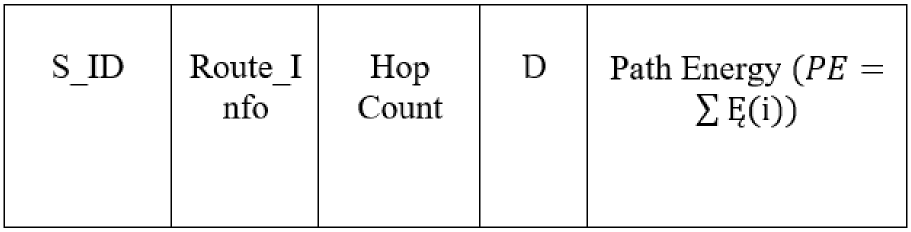


Node_ID	Ť	Ŧ	Ȩ	λ	µ	φ
Neighbour_Node_ID(1)			Ȩ	λ	µ	φ
Neighbour_Node_ID(2)			Ȩ	λ	µ	φ
……………………………						
Neighbour_Node_ID(n)			Ȩ	λ	µ	φ

Fig 2. Node Table

(b) Bin: It is also a new data structure that is added to maintain the dumped node list. Whenever an attacker node identifies as an attacker, it will be added to this list and avoided in any future transmissions.

(c) Routing Table: This table maintains the route information like in the AODV protocol, but the new additional parameters are added to it, as shown in the figure below.

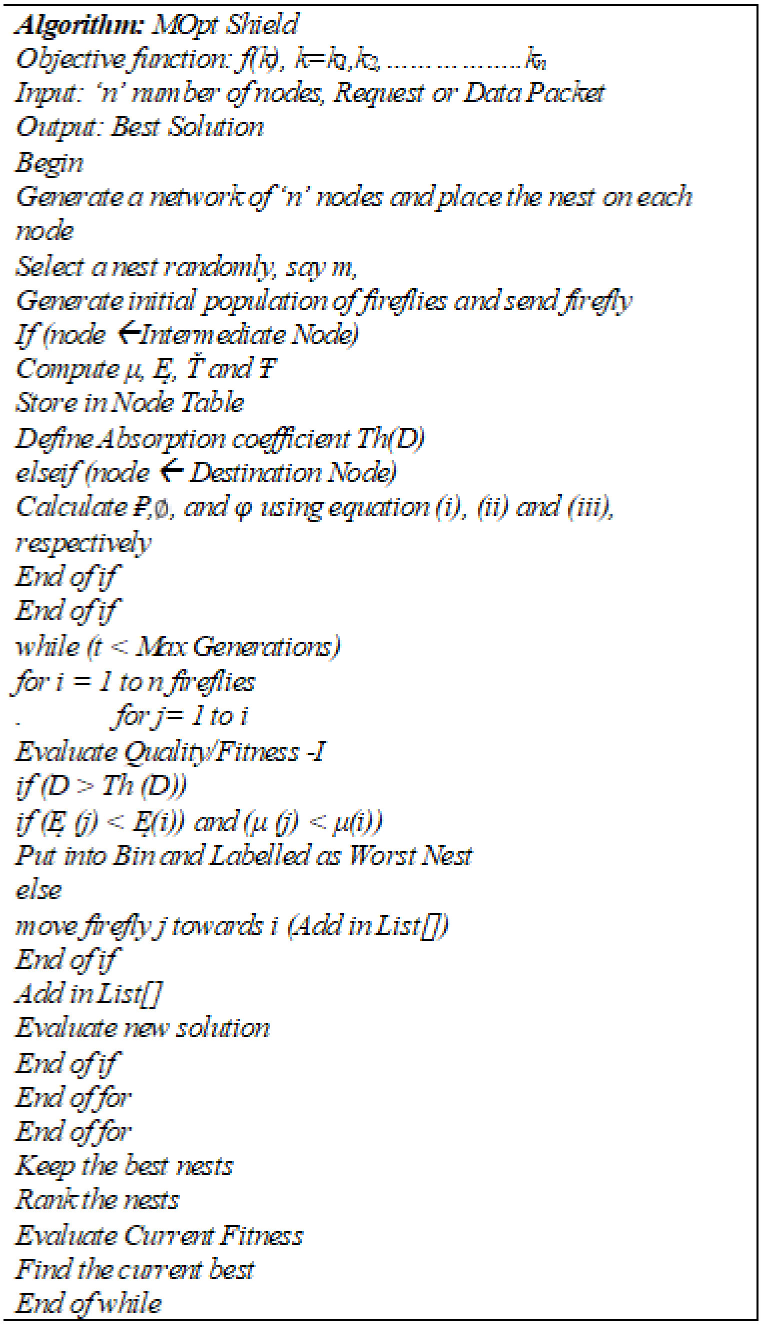


S_ID	Route_Info	Hop Count	D	Path Energy ($PE = \sum$ Ȩ(i))

Fig 3. Routing Table (Additional Details)

3.3 Pseudo Code

MOpt Shield combines a hybrid optimization algorithm and an Intrusion Detection system to select the best data transmission path. Here best means the path which doesn't affect by the attackers of any type. It means it provides a protective environment for the communication between the nodes. The pseudo-code of this new proposed protocol is given in the following figure:



```
Algorithm: MOpt Shield
Objective function: f(k), k=k1,k2,………………kn
Input: 'n' number of nodes, Request or Data Packet
Output: Best Solution
Begin
Generate a network of 'n' nodes and place the nest on each
node
Select a nest randomly, say m,
Generate initial population of fireflies and send firefly
If (node ←Intermediate Node)
Compute μ, Ę, Ť and Ŧ
Store in Node Table
Define Absorption coefficient Th(D)
elseif (node ← Destination Node)
Calculate ₽,∅, and φ using equation (i), (ii) and (iii),
respectively
End of if
End of if
while (t < Max Generations)
for i = 1 to n fireflies
.           for j= 1 to i
Evaluate Quality/Fitness -I
if (D > Th (D))
if (Ę (j) < Ę(i)) and (μ (j) < μ(i))
Put into Bin and Labelled as Worst Nest
else
move firefly j towards i (Add in List[])
End of if
Add in List[]
Evaluate new solution
End of if
End of for
End of for
Keep the best nests
Rank the nests
Evaluate Current Fitness
Find the current best
End of while
```

Fig 4. Proposed Protocol Algorithm

The next section of this paper defines this proposed MOpt shield under the hybrid attack environment.

4 Proposed Work

This proposed work's primary focus is to provide a secure environment for communication in MANETs under different attack scenarios. For this work, the performance is measured in the presence of two separate attacks simultaneously. The attacks are Blackhole and DDoS attacks.

4.1 Amalgam Attack Scenario- Example

Amalgam attacks mean a combination of different attacks simultaneously on the same network for the same transmission. Here Blackhole and DDoS attacks are implemented, as shown in the figure below. The figure shows that in the given network scenario, 5 attackers are there, from which 2 are blackhole, and 3 are DoS attacker nodes. Blackhole attack drops the packets which it received from the source or any intermediate nodes. In contrast, DoS attackers continuously attacked the destination node to stop the destination node from receiving any data.

In this example, Source 'S' wants to communicate with Destination Node 'D' and send its packets to the selected routes. If it sends its packet through route-1, where the black hole node is just the neighbor node, all the packets will be dropped, as shown in the figure below. Similarly, if the packet follows route-2, the other blackhole node will drop all the packets. On the other hand, the DoS attacker node attacks the destination node with multiple packets to make it busy. So, even if route-3 is followed for transmission, it will be an unsuccessful transmission. Because the destination node will not accept packets, and it will again drop. So, in all three cases, packets will not receive by the destination node, and all the data sent by the source node will be lost.

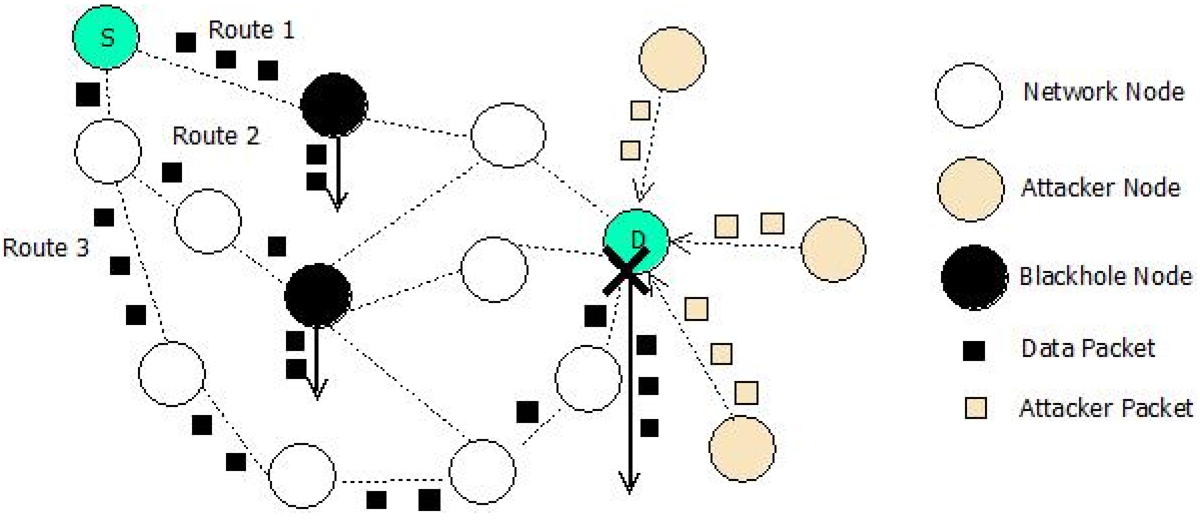


Fig 5. Example of Amalgam Attack

This work proposed a scheme to mitigate amalgam attacks and prevent the network from the above situations. Different types of attackers attack together on the network with multiple attacker nodes.

4.2 Proposed Methodology

The primary purpose of this work is to provide a secure environment for data transmission, even in the presence of more than one attack. For this, an Optimization-based protocol is proposed with IDS features. This proposed work, divided into four phases: (a) Initialization Phase, (b) MOpt Departure Phase, (c) MOpt Returning Phase, and (d) MOpt Acceptance Phase. The details of these phases are as given below:

(a) Initialization Phase: The first phase of this proposed work is the initialization phase in which 'k' nodes are distributed over the 'm x n' area. Nodes are initialized with some parameters like Packet Forward Count (μ)=0, Energy (Ȩ), Delay (φ)=0, Node_ID, and other general parameters. All 'k' nodes are placed randomly on the area and start to communicate with each other.

(b) MOpt Departure Phase: This phase originates whenever a node wants to communicate with the other node. In this, the source node initiates nest discovery in which the cuckoo selects one of the neighbor nests randomly. The following process begins from that nest chosen in which the firefly starts its discovery process and forwards the firefly to the neighbor nodes. Whenever a node receives a firefly, it computes parameters as defined in the pseudo code. Here, two cases arise where; the first case is if an intermediate node receives firefly, then it computes the parameters and store them in the node table. Still, if firefly received by a destination node, then MOpt Return Phase called.

(c)MOpt Return Phase: In this phase, the destination sent the firefly back to the source with the flag firefly_return. Whenever an intermediate node receives this firefly_return, it updates its parameters, adds a delay of the current packet to the firefly packet, and then forwards it to its next hop. Finally, when this firefly reached its source node, then it calls MOpt Acceptance Phase.

(d) MOpt Acceptance Phase: In this phase, the source node first evaluates fitness for all the received firefly_return packets based on Accumulated Delay, Energy, and forward count. The two different lists are generated based on this fitness value: (a) Accepted List and (b) Worst Nest List. The worst nest list will be evaluated for the final worst decision based on quality parameters, and this list is maintained in the bin. On the other hand, the Accepted list is again evaluated the fitness after ranking. The ranking is done to reduce the computations for future transmission, which reduces the algorithm's complexity. This fitness is assessed based on the average value, and the current best will be selected for transmission of the data.

The above phases are called whenever a node wants to communicate with the other node until the data transmission will be completed.

5 Simulation Results and Analysis

The proposed protocol is implemented using the NS-2 simulator to verify its performance based on different factors. In this MOpt Shield, a threshold value is used for fitness evaluation, as mentioned in the previous sections. So, firstly, the proposed work's performance is evaluated based on different threshold values, and then the value with the best results is used for other analyses. In the other scenario, the performance is analyzed based on several connections. It means the performance analysis is done by increasing the network rate in the network, which is a crucial factor that affects the network. In both scenarios, two blackhole attackers and three DDoS attacker nodes are implemented to disturb the network. In total, 5 attackers are present in the network to scrutinize the effectiveness of the proposed protocol.

Scenario-1: Absorption Coefficient (Th(D))

In this scenario, simulation is run with different delay thresholds to identify the best-fitted threshold value used to determine the best results. Delay is an essential factor that affects network performance. Here, delay threshold values, which are also represented as an Absorption coefficient Th(⊠) in MOpt Shield protocol, are varied. Results are evaluated along with the simulation parameters as defined in Table 1.

Table 1. Simulation Setup (Scenario-1)

Simulation Parameter	Value
No. of Nodes	50
Area	1500x1500
traffic	CBR
Simulation Time	200 sec
No. of Connections	10
Traffic Rate	4packets/s
Speed	20m/s
Packet Size	1024
Total Attackers	5
Th(⊠)	0.001, 0.003, 0.005, 0.007

To analyze the results, different performance parameters are used: Packet Delivery Ratio (PDR), Throughput, Packet Loss Ratio (PLR), and Delay. Here Delay is the transmission delay, which is calculated for the whole scenario like other parameters. Table 1 shows the performance analyzed after the simulation using the above simulation parameters.

Table 2. MOpt Shield Performance (based on different Th(⊠))

	Th$_1$(⊠)=0.001	Th$_2$(⊠)=0.003	Th$_3$(⊠)=0.005	Th$_4$(⊠)=0.007
PDR (in %)	79.63	87.12	82.71	77.06
Throughput (in kbps)	94.27	121.98	101.84	91.36
PLR (in %)	20.37	12.88	17.29	22.94
Delay (in sec)	0.085	0.081	0.083	0.089

The above results show that the proposed protocol's performance with Th$_2$(⊠) is the best from other values in all the defined measures. This may be because of the following reasons:

1. Th$_1$(⊠) is a relatively lower value that is impossible to achieve for every path (group of nodes) because of attackers' presence and the nodes' dynamic behavior.
2. Attackers are always trying to cause different performance issues. With the higher threshold value like Th3(⊠) and Th4(⊠), it might be possible that intruders become part of communication cause some delay. So, as a result, performance gets reduced. Secondly, the higher accepted delay may select the unfitted path, which does not provide the desired results.

The above defines factors that might affect the performance and becomes the reason for poor performance with the lower and higher threshold values. In contrast, the best performance is achieved with the threshold value of Th$_2$(⊠),i.e., 0.003 sec, so, for other analyses, this value will be considered. The results for each factor are also shown in the figure below.

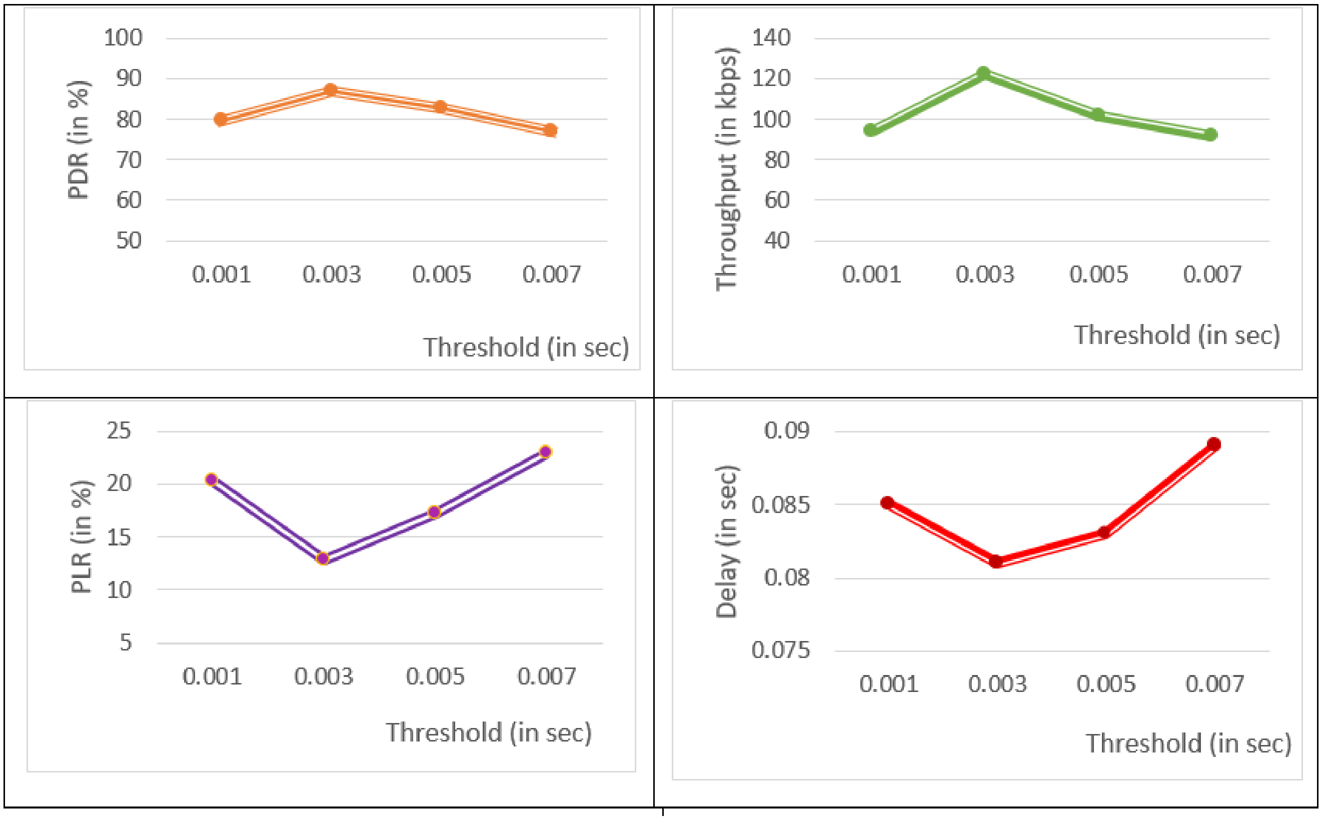


Fig 6. Performance Measures (MOpt Shield)

The above results show that the performance of the proposed protocol is varied with the threshold change. In PDR, the results of Th(⊠) value of 0.003 sec is 8.5%, 5%, and 11% better than the Th$_1$(⊠), Th$_3$(⊠), Th$_4$(⊠) values, respectively. Similarly, for throughput, the improvement percentage is 22.7% from Th$_1$(⊠), 16.5% from Th$_3$(⊠), and 25% from Th$_4$(⊠), which is quite impressive for Th$_2$(⊠). PLR is also significantly less in the case of Th$_2$(⊠), and if compared with the other threshold values, it is 36.7%, 25.5%, and 43.8% better than the Th$_1$(⊠), Th$_3$(⊠), Th$_4$(⊠) respectively. Finally, the minor transmission delay is again achieved by the Th$_2$(⊠). The improvement is not much in percent and is 4.7%, 2.4%, and 8.9% respectively, but still, it is the best performance. So, the proposed protocol's performance with Th$_2$(⊠) value becomes the reason for selecting this value in further analysis.

Scenario-2: Traffic Transition

Traffic is also an influential factor with which the performance transforms from high to low or vice versa. Here, in this scenario, the number of connections is varied to increase network traffic. For this analysis, the MOpt Shield performance is also compared with the other existing protocols, namely, Cu-IDS, which is a cuckoo-based Intrusion detection system, and FF-IDS, a firefly-based intrusion detection system proposed earlier for the blackhole and DDoS attacks separately. But here, these protocols are tested on the Amalgam Attacks. The simulation parameters used for this scenario are as defined in Table 3.

Table 3. Simulation Setup (Scenario-2)

Simulation Parameter	Value
No. of Nodes	50
Area	1500x1500
traffic	CBR
Simulation Time	200 sec
No. of Connections	5,10,15,20,25
Traffic Rate	4packets/s
Speed	20m/s
Packet Size	1024
Total Attackers	5
Threshold	0.003

The performance is analyzed using the same parameters as done in the previous scenario, and the evaluated results are given below.

(a) Packet Delivery Ratio: The PDR defines the number of packets delivered to the destination. The results presented in the figure below forecast the performance of the proposed protocol and conclude that when traffic rate increases, the PDR reduces, but the MOpt shield's performance is better than the other protocols even in the higher traffic rate.

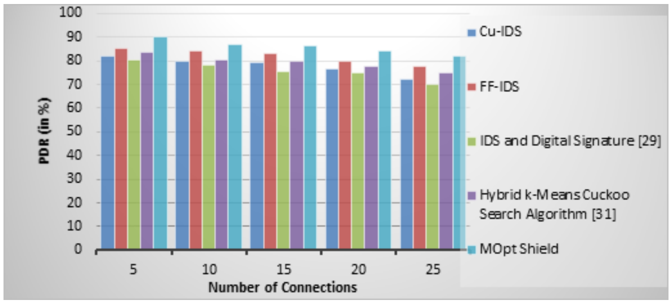


Fig 7. Packet Delivery Ratio (Scenario-2)

The above results show that the performance achieved by the proposed protocol is better in all cases. With statistical analysis, it is clear that, on average, the MOpt shield's performance is improved by 4.6% and 9.2% from FF-IDS and Cu-IDS, respectively. The proposed protocol's maximum achieved delivery ratio is 90.2%, which is pretty impressive in the presence of Amalgam attacks with 5 attackers.

(b) Throughput: This is another factor that helps measure network performance, which defines the rate of data transmission in kbps (kilobits per second). The figure below exhibits the performance of the proposed protocol and the other existing protocols in terms of Throughput and provides another evidence for the effectiveness of the MOpt Shield.

Like PDR, Throughput is also reduced in the immense traffic; however, the attained performance is better than the other protocols. The MOpt Shield performance in terms of throughput is 19% better than the Cu-IDS, whereas it is 11% better than FF-IDS. So, it is clear from the results that the proposed protocol beats other existing protocols and showcases its capabilities.

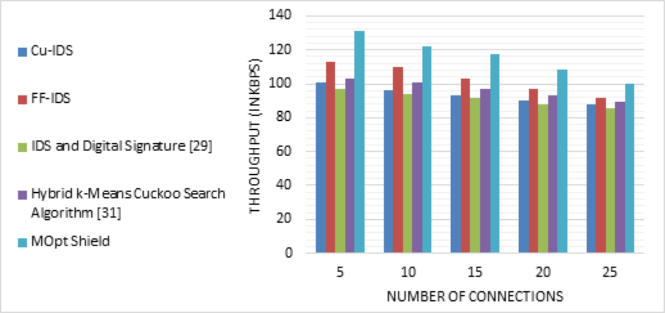


Fig 8. Throughput (Scenario-2)

(c) Delay : This measurement delineates the latency for a data travels from the source to destination, and here it is calculated for the transmission done in the defined simulation time. The results illustrated in figure 9 portray the strength of the proposed protocol regarding the delay factor.

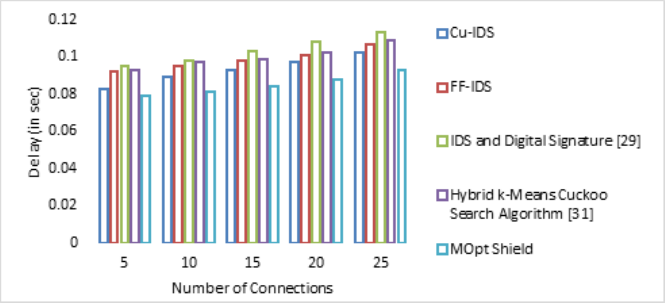


Fig 9. Delay (Scenario-2)

This performance parameter increases with the number of connections but is better than the existing protocols by 13.7% and 8.4 % from FF-IDS and Cu-IDS, respectively. So, the potency of the proposed protocol can also be noticed from the delay factor.

(d) Packet Loss Ratio: PLR is also the crucial factor in transmission that defines the loss ratio of the data while transferring from one location to another. The results of this parameter are exhibits in the figure below:

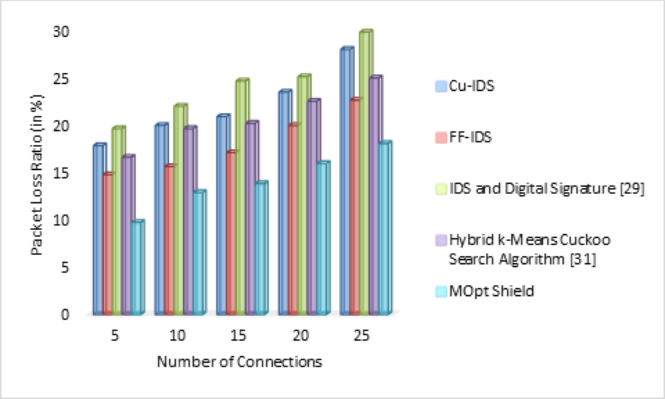


Fig 10. Packet Loss Ratio (Scenario-2)

The packet loss increases with the increase in connections but with proposed protocol it is always lesser than the other protocols.

6 Conclusion and Future Scope

This proposed Protocol 'MOpt Shield' is designed to handle the amalgam attacks in different scenarios. The proposed protocol used the effectiveness of the most standard optimization techniques, namely, Cuckoo Search and Firefly, along with the generosity of the Intrusion Detection System. To simulate this protocol, an NS-2 simulator is used. In this approach, the absorption coefficient is selected from the different values based on parameter analysis. The simulation is done in the presence of five attacker nodes. We consider the amalgam attacks so that two blackholes and three DDoS attackers are part of this simulation. The proposed protocol's performance is compared with the existing Cu-IDS and FF-IDS by increasing the traffic in the same scenario. The analysis shows that the average PDR of MOpt Shield is 85.9%, 82% for FF-IDS, and 77.9% for Cu-IDS. The other performance measure is throughput, and results depict the average throughput is 115.63, 102.84, and 93.61 kbps for MOpt Shield, FF-IDS, and Cu-IDS, respectively. The last and essential factor, Average Delay, is lesser in the proposed approach and is 0.085 sec. The other approaches, like FF-IDS, have a delay of 0.098 sec, whereas Cu-IDS has 0.093 sec. Overall, the performance of the proposed 'MOpt Shield' is on the top in all aspects, and it is concluded that this approach is the conqueror even in the existence of amalgam attacks. The performance of the proposed protocol is quite effective, the only limitation of this protocol is its threshold parameter which is fixed. As we know, the network is of dynamic nature so fixed threshold might fails in some cases (not necessarily). In the future, the main attention can be paid on the network parameters in order to test the performance of the proposed protocol and work can also be done to find the dynamic threshold value for absorption coefficient.

References

1) Villanueva JA, Lacatan LL, Vinluan AA. Information Technology Security Infrastructure Malware Detector System. *International Journal of Advanced Trends in Computer Science and Engineering*. 2020;9(2):1583–1587. Available from: http://www.warse.org/IJATCSE/static/pdf/file/ijatcse103922020.pdf.
2) Quy VK. Review on Security-aware Routing Protocols for Mobile Ad hoc Network. *International Journal of Advanced Trends in Computer Science and Engineering*. 2020;9(3):3655–3661. Available from: 10.30534/ijatcse/2020/175932020.
3) Justin V, Marathe N, Dongre N. Hybrid IDS using SVM classifier for detecting DoS attack in MANET application. In: and others, editor. In2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) 2017. 2017;p. 775–778. Available from: 10.1109/i-smac.2017.8058284.
4) Funde BS, Chourasia. A Hybrid Intrusion Detection System to Detect Hybrid attacks in MANET. *International Journal of Advanced Research in Computer and Communication Engineering*. 2019;8(10):12–20. Available from: 10.17148/IJARCCE.2019.81002.
5) Jasdeep K, Harmeet S. DDoS Attack Detection and Prevention in MANETs. *International Journal of Advanced Science and Technology*. 2020;29(3):2402–2407. Available from: http://sersc.org/journals/index.php/IJAST/article/view/4341.
6) Gautam A, Mahajanb R, Zafarc S. Repercussions of DDoS Attack on MANET based Healthcare Sector Routing Protocols Performance and ANOVA Assessment. *International Journal of Advanced Science and Technology*. 2020;29(05):12157–12177. Available from: http://sersc.org/journals/index.php/IJAST/article/view/25655.
7) Keerthika V, Malarvizhi N. Mitigate Black Hole Attack Using Hybrid Bee Optimized Weighted Trust with 2-Opt AODV in MANET. *Wireless Personal Communications*. 2019;106(2):621–632. Available from: https://dx.doi.org/10.1007/s11277-019-06182-8.
8) Gowrishankar J, Kumar PS, Narmadha T, Natarajan Y. Yuvaraj Natarajan A Trust-Based Protocol for Manets In Iot. *Environment International Journal of Advanced Science and Technology*. 2020;29(7):2770–2775.
9) Pathan MS, He J, Zardari ZA, Memon MQ. Muhammad Qasim Memon . An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. *Future Internet*. 2018;10(2):1–16. Available from: 10.3390/fi10020016.
10) Naveena A, Reddy KRL. Malicious node prevention and mitigation in MANETs using a hybrid security model. *Information Security Journal: A Global Perspective*. 2018;27(2):92–101. Available from: https://dx.doi.org/10.1080/19393555.2017.1415399.
11) Hossain S, Hussain MS, Ema RR, Dutta S, Sarkar S, Islam T. Detecting Blackhole attack by selecting appropriate routes for authentic message passing using SHA-3 and Diffie-Hellman algorithm in AODV and AOMDV routing protocols in MANET. *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. 2019;p. 1–7. Available from: 10.1109/icccnt45670.2019.8944395.
12) Yasin A, Zant MA. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. *Wireless Communications and Mobile Computing*. 2018;2018:1–10. Available from: https://dx.doi.org/10.1155/2018/9812135.
13) Mukhedkar MM, Kolekar U. E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network. *International Journal of Communication Systems*. 2020;33(7). Available from: https://dx.doi.org/10.1002/dac.4252.
14) Babu DM, Ussenaiah M. CS-MAODV: Cuckoo search and M-tree-based multiconstraint optimal Multicast Ad hoc On-demand Distance Vector Routing Protocol for MANETs. *International Journal of Communication Systems*. 2020;p. 1–17. Available from: https://dx.doi.org/10.1002/dac.4411.
15) Priya JS, Femina MA, Samuel RA. APSO-MVS: an adaptive particle swarm optimization incorporating multiple velocity strategies for optimal leader selection in hybrid MANETs. *Soft Computing*. 2020;24(24):18349–18365. Available from: https://dx.doi.org/10.1007/s00500-020-05034-z.
16) Tripathy BK, Jena SK, Bera P, Das S. An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks. *Wireless Personal Communications*. 2020;114:1339–1370. Available from: https://dx.doi.org/10.1007/s11277-020-07423-x.
17) Sinwar D, Sharma N, Maakar SK, Kumar S. Analysis and comparison of ant colony optimization algorithm with DSDV, AODV, and AOMDV based on shortest path in MANET. *Journal of Information and Optimization Sciences*. 2020;41(2):621–632. Available from: https://dx.doi.org/10.1080/02522667.2020.1733193.
18) Jayaraj R, Suresh T, Jayaraman KB. Hybridization of Metaheuristics Optimization Algorithm Based Packet Adjustment Rate Model for Congestion Control in MANET. *International Journal of Advanced Science and Technology*. 2020;29(05):12663–12672.
19) Kondaiah R, Sathyanarayana B. Trust Factor and Fuzzy Firefly Integrated Particle Swarm Optimization Based Intrusion Detection and Prevention System for Secure Routing of MANET. *International Journal of Computer Networks & Communications*. 2020;10(1):13–33. Available from: 10.5121/ijcnc.2018.10102.

20) Devi GGY, Rao V. Security Improved Chicken Swarm Optimization Based A* Routing Algorithm on MANETs. *International Journal of Recent Technology and Engineering Regular Issue*. 2020;8(5):3539–3545. Available from: 10.35940/ijrte.e6379.018520.

21) Joshua CJ, Varadarajan V. An optimization framework for routing protocols in VANETs: A multi-objective firefly algorithm approach. . *Wireless Networks*. 2019;p. 1–10. Available from: 10.1007/s11276-019-02072-w.

22) Manoranjini J, Chandrasekar A, Jothi S. Improved QoS and avoidance of black hole attacks in MANET using trust detection framework. *Automatika*. 2019;60(3):274–284. Available from: https://dx.doi.org/10.1080/00051144.2019.1576965.

23) Mohan CR, Ananthula VR. Reputation-based secure routing protocol in mobile ad-hoc network using Jaya Cuckoo optimization. *International Journal of Modeling, Simulation, and Scientific Computing*. 2019;10(03):1–24. Available from: https://dx.doi.org/10.1142/s1793962319500144.

24) Veeraiah N, Krishna BT. An approach for optimal-secure multi-path routing and intrusion detection in MANET. *Evolutionary Intelligence*. 2020. Available from: https://doi.org/10.1007/s12065-020-00388-7.

25) Vishal P, Babu AR. Firefly Algorithm for Intelligent Context-Aware Sensor Deployment Problem in Wireless Sensor Network. *Journal of Circuits, Systems and Computers*. 2019;28(06):1–38. Available from: https://dx.doi.org/10.1142/s0218126619500944.

26) Talukdar MI, Hassan R, Hossen MS, Ahmad K, Qamar F, Ahmed AS. Performance improvements of Aodv by black hole attack detection Using ids and digital signature. *Wireless Communications and Mobile Computing*. 2021;p. 1–13. Available from: 10.1155/2021/6693316.

27) Srivastava A, Gupta SK, Najim M, Sahu N, Aggarwal G, Mazumdar BD. DSSAM: Digitally signed secure Acknowledgement method for mobile ad hoc network. *EURASIP Journal on Wireless Communications and Networking*. 2021;20(1):1–29. Available from: 10.1186/s13638-021-01894-7.

28) García J, Yepes V, Martí JV. A hybrid k-means cuckoo search algorithm applied to the counterfort retaining walls problem. *Mathematics*. 2020;8(4):555–577. Available from: 10.3390/math8040555.

29) Joshi S, Mishra DK. Detection of Rushing Attack and Data Modification Attack in Mobile Ad Hoc Networks. *Journal of Critical Reviews*. 2020;7(19):9486–9498.

30) Tahboush M, Agoyi M. A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET). *IEEE Access*. 2021;9:11872–11883.