DOI: 10.56452/2021SP-8-020

ISSN: 0974-5823 Vol. 6 (Special Issue 3, November 2021)

International Journal of Mechanical Engineering

Optimized Intrusion Detection System to Mitigate Hybrid Attacks

Jaspreet Kaur[1,*], Rajneesh Talwar[2] and Baljeet Kaur[3]

[1]Research Scholar, I.K. Gujral Punjab Technical University, Jalandhar, Punjab, India

[2]Director, Engineering Section, Chandigarh Engineering College, Jhanjeri, Mohali-140307, Punjab, India

[3]Department of Computer Application, Chandigarh School of Business, Jhanjeri, Mohali-140307, Punjab, India

E-mail: jaspreetwphd@gmail.com

Abstract: As the need for technology grows, so do the risks associated with it, such as confidentiality, data loss, and other issues in the realm of communication. Due to its dynamic nature, the majority of the community now uses digital communication to transport data from one end to the other via wireless media rather than wired media. Ad hoc network is a type of wireless network that does not require any transmission infrastructure. A crossbreed protocol is presented in this work called optimized Intrusion Detection System, as hybrid optimization algorithms are favoured over other approaches currently. The efficacy of the current Cuckoo Search and Firefly Optimization Algorithm on the fundamental AODV protocol is combined with the advantages of the Intrusion Detection System is suggested in this protocol. The proposed protocol is simulated using an NS-2 simulator with two different simulation scenarios. PDR, Throughput, PLR, Overhead and End to End Delay characteristics are used as performance measurements for the proposed protocol. 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 by varying number of attacker nodes and threshold values. For simulation, the scenario includes minimum 2 and maximum 10 attackers between the 50 nodes with CBR traffic and 20m/s speed. The assessed findings demonstrate the suggested protocol's superior performance over other existing protocols, revealing its potential.

Keywords: Hybrid Attacks, Blackhole, Crossbreed, Cuckoo Search, DDoS, Firefly Algorithm, NS-2 simulator

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 [26]. 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.

MANET Attacks are categorized into two types: (a) Active Attacks and (b) Passive Attacks. In the inactive 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 [27] 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.

Literature Survey

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. [1] 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 [2] 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 [8] 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. [9]. 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 [3] proposed a trust-based Bee optimization algorithm with 2-Opt AODV. This hybrid approach usedthe 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. [11] 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. [12] 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 [4] 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 invarious parameters. The other cryptography-based security approach was proposed by Hossain et al. [7]. 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 [10] 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

DOI: 10.56452/2021SP-8-020

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 [15-25],[29-31] 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 [28] 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 [32] and analyses its effect with and without detection algorithm.

Optimized Intrusion Detection System

Optimized Intrusion Detection System, is a network defence system that helps to defend the network from different attacks. As illustrated in the diagram 1, this shield protects every node in the network from the attacker and acts as a guard. The attacker may or may not be a network member, but it will always try to harm the network by causing data loss or connection failure. As a result, it is a network need that intruders be avoided in some way. For this, a suggested shield employs an intrusion detection system, as well as an optimization method for effective route selection that, depending on various factors, provides direct or indirect protection from attacker nodes. This technique is called meld optimization since it combines two separate algorithms, Firefly Algorithm (FFA) and Cuckoo Optimization Algorithm (COA), to build a perfect path in Mobile Adhoc Networks (MANETs) while transmitting data from one node to another.

The AODV protocol is the basic protocol used to implement this method, which sends a request packet to locate a route for data transfer and pick the optimal option among alternatives. The goal of this algorithm isn't only to discover the optimal way; it's also to find the best route that protects the data from attackers while still delivering it effectively. This method works from beginning to end for more reliable results, and it records the elements in order to handle many sorts of attackers at once. These elements are computed before transmission depending on a set of criteria.

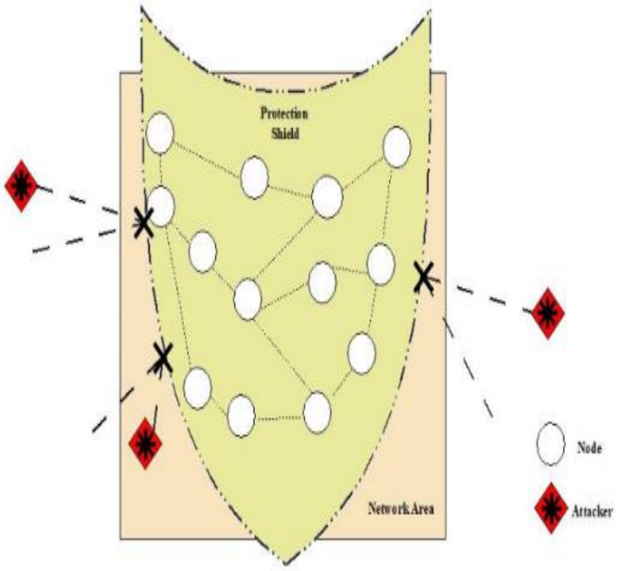


Figure. 1: Optimized Intrusion Detection System on Network

DOI: 10.56452/2021SP-8-020

Some of the general parameters that are considered into account for this study are, Packet Drop Count (λ), Packet Forward Count (μ), Energy (Ȩ), Packet Receiving Time (Ť) & Packet Sending Time (Ŧ) for different packets, and Accumulate Delay (D). These parameters are computed and saved in distinct tables for each node that will participate in the communication process.

Mathematical Formulations

A network of ‘n' nodes communicates with one another and transfers data from one end to the other. In the form of bits, data travels across the network by taking multiple routes, such as ‘k' pathways. Because this is an example of an adhoc network, the network's nodes act as forwarders and transport data. As a result, whenever a node sends or receives packets, the following parameters are computed.

To begin, the Packet Travelling Time (P) is computed, which is defined as the time it took a packet to travel from source to destination and is calculated using the following formula based on Packet Receiving Time (Ť) and Packet Sending Time (Ŧ).

$$\text{Ᵽ} = \text{Ť} - \text{Ŧ}P = \text{Ť} - \text{Ŧ}P = \text{Ť} - \text{Ŧ⍰} = \text{Ť} - \text{Ŧ}\text{......(i)}$$

Then, using the following equation, Packet Roaming Time $(\emptyset)\emptyset)$ is computed for both the request and reply packets:

$$\emptyset = \emptyset_{RREQ} = \emptyset_{RREP} = n * \frac{\gamma}{\delta}\emptyset = \emptyset_{RREQ} = \emptyset_{RREP} = n * \frac{\gamma}{\delta}\text{.....(ii)}$$

Here, n denotes the number of nodes through which the packet traveled, $\gamma\gamma$ is the transmission range, and $\delta\delta$ is the network propagation speed.

Delay $(\varphi\varphi)$ is a key element that determines the performance of a network protocol, and it is computed as follows:

$$\varphi = P - (\emptyset_{RREQ} + \emptyset_{RREP})\varphi = P - (\emptyset_{RREQ} + \emptyset_{RREP})\varphi = \text{⍰} - (\emptyset_{RREQ} + \emptyset_{RREP})\text{.....(iii)}$$

To offer QoS, Accumulated Delay (D) is computed and employed in the path selection process. This factor is derived as a function of the Delay factor.

$$D(\mathrm{i}) = D(\mathrm{i}-1) + \varphi(i)D(\mathrm{i}) = D(\mathrm{i}-1) + \varphi(i)\text{⍰}(\mathrm{i}) = \text{⍰}(\mathrm{i}-1) + \varphi(i)\text{......(iv)}$$

Where i=1,2,3,……n and, $D(1) = 0D(1) = 0\text{⍰}(1) = 0$

Another component, Energy (Ȩ), has a significant influence on performance and is measured at both the transmitting and receiving nodes.

The Energy at Transmitter side:

$$\text{Ȩ}_T(b,\text{ƌ}) = \text{Ȩ}_F(b) + \text{Ȩ}_R(b,\text{ƌ})\text{Ȩ}_T(b,\text{ƌ}) = \text{Ȩ}_F(b) + \text{Ȩ}_R(b,\text{ƌ})\text{........(v)}$$

The number of bits is b, while the distance between the nodes is ƌƌ. The following formula is used to compute $\text{Ȩ}_R\text{Ȩ}_R$, where is the energy wasted per bit to transmit a packet $\text{Ȩ}_F\text{Ȩ}_F$, and $\text{Ȩ}_R\text{Ȩ}_R$, is the energy dissipated per bit to receive a packet.

$$\text{Ȩ}_R(b,\text{ƌ}) = \text{Ȩ}_F(b)\text{Ȩ}_R(b,\text{ƌ}) = \text{Ȩ}_F(b)\text{.....(vi)}$$

All of the above variables are computed and utilised to carry out various operations.

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

Figure 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.

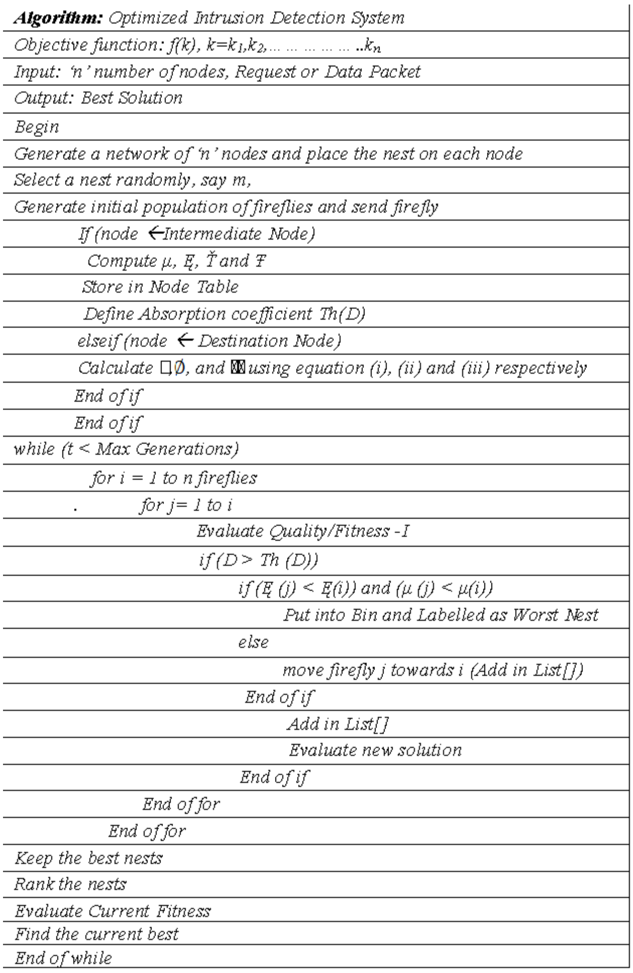
(c) Routing Table: This table maintains the route information like in the AODV protocol, but the new additional parameters are added to it, as shown in the figure below.

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

Figure 3: Routing Table (Additional Details)

Pseudo Code

The proposed system 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: Optimized Intrusion Detection System
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, Ȩ, Ť and Ŧ
         Store in Node Table
         Define Absorption coefficient Th(D)
        elseif (node ← Destination Node)
        Calculate □∅, and ▩ 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 (Ȩ (j) < Ȩ(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
```

Figure. 4: Proposed Protocol Algorithm

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

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.

Hybrid Attack Scenario- Example

Hybrid attacks are when several attacks are launched simultaneously on the same network for the same transmission. As indicated in the diagram 5, blackhole and DDoS attacks are used. Figure 5 illustrates that there are a total of 5 attackers in the provided network environment, two of which are blackholes and three of which are DoS attacker nodes. DoS attackers continuously target the destination node to prevent the destination node from receiving any sort of data, whereas blackhole attacks causes dreadful situation in the network and hence discard packets received from the source or any intermediary nodes.

In this case, Source 'S' wishes to interact with Destination Node 'D' and transmit packets to the routes that have been chosen. If it sends its packet through route-1, where the blackhole node is simply a neighbour node, all packets are lost, as illustrated in the diagram below. In the same way, if packets follow route-2, the second blackhole node will discard all of them. DoS attacker nodes, on the other hand, bombard the target node with numerous packets in order to keep it occupied. As a result, even if route-3 is used for transmission, it will be ineffective. Because packets will not be received by the destination node, the connection will be dropped once more. As a result, packets will not be received by the destination node in all three circumstances, and all data supplied by the source node will be lost.

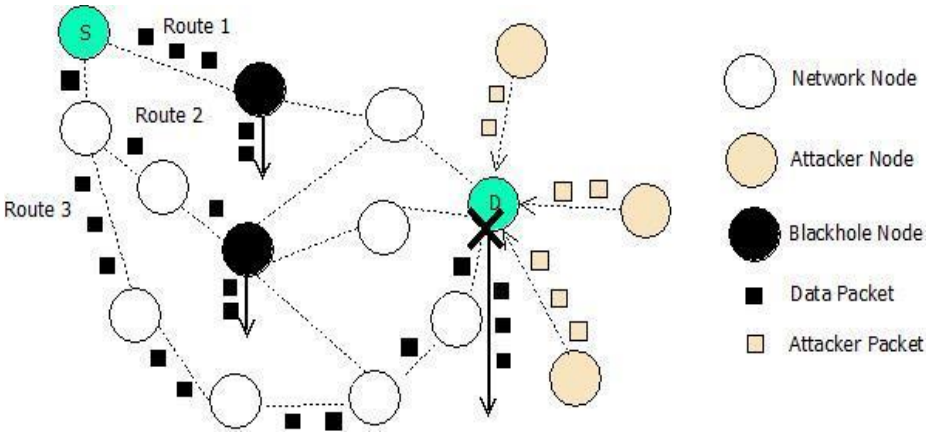


Figure 5: Example of hybrid Attack [3])

As a result, this work suggested a strategy to minimise hybrid attacks and protect networks against the circumstances described above, in which various types of attackers assault the network simultaneously with multiple attacker nodes.

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) Departure Phase, (c) Returning Phase, and (d) Acceptance Phase.

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

Simulation Results and Analysis

The proposed protocol is implemented using the NS-2 simulator to verify its performance based on different factors. In this proposed approach, 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(D) in proposed protocol, are varied. Results are evaluated along with the simulation parameters as defined in table 1.

DOI: 10.56452/2021SP-8-020

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(D)	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: Proposed Approach Performance (based on different Th(D))

	Th_1(D)=0.001	**Th_2(D)=0.003**	**Th_3(D)=0.005**	**Th_4(D)=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(D)is the best from other values in all the defined measures. This may be because of the following reasons:

(a) Th_1(D)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.

(b) Attackers are always trying to cause different performance issues. With the higher threshold value like Th3(D) and Th4(D), it might be possible that intruders become part of communication cause some delay. So, asa 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(D),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.

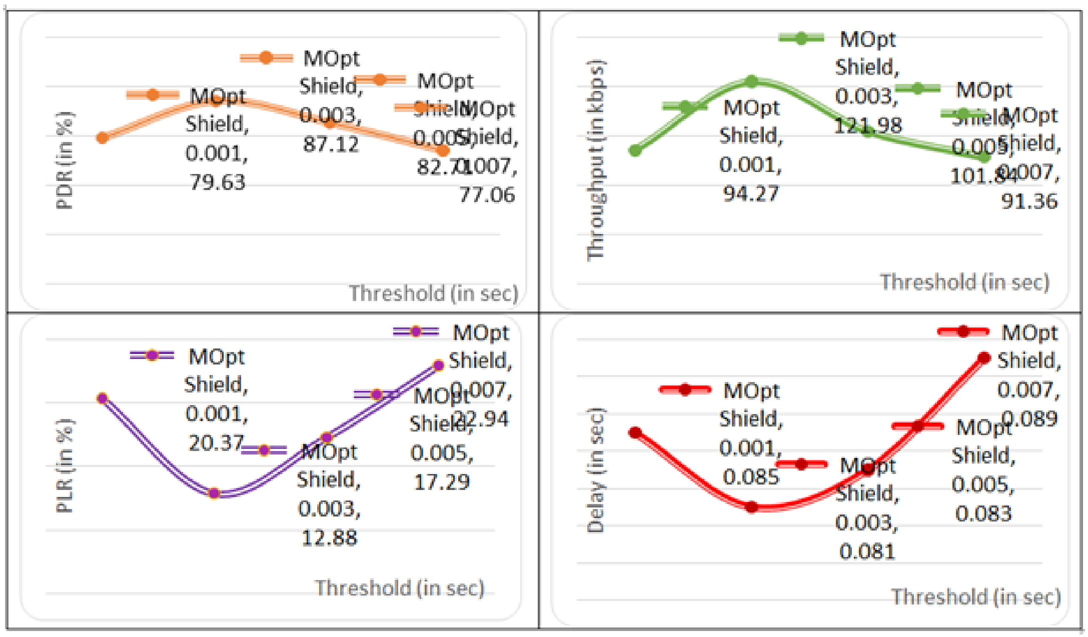


Figure. 6: Performance Measures (Proposed Approach)

The above results show that the performance of the proposed protocol is varied with the threshold change. In PDR, the results of Th(D) value of 0.003 sec is 8.5%, 5%, and 11% better than the Th$_1$(D), Th$_3$(D), Th$_4$(D)values, respectively. Similarly, for throughput, the improvement percentage is 22.7% from Th$_1$(D), 16.5% from Th$_3$(D), and 25% from Th$_4$(D), which is quite impressive for Th$_2$(D). PLR is also significantly less in the case of Th$_2$(D), and if compared with the other threshold values, it is 36.7%, 25.5%, and 43.8% better than the Th$_1$(d), Th$_3$(D), Th$_4$(D) respectively. Finally, the minor transmission delay is again achieved by the Th$_2$(D). 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$_2$(D) value becomes the reason for selecting this value in further analysis.

***Scenario-2:* Varying Number of Attacker Nodes:** In this, a network of 50 nodes is created over a 1500 x 1500 square metre space. The performance of the protocols Cu-IDS and FF-IDS is compared to that of the proposed Approach, and the impact of Single (blackhole and DDoS attacks) and Hybrid attacks is investigated. Table 3 lists the remaining simulation settings.

Table 3: Simulation Parameters (Scenario 2)

Simulation Parameter	Value
No. of Nodes	50
Area	1500 x 1500
traffic	CBR
Simulation Time	500 s
No. of Connections	20
Traffic Rate	4 packets/s
Speed	20m/s
Packet Size	1024
No. of Attacker Nodes	2,4,6,8,10

DOI: 10.56452/2021SP-8-020

The parameters given in Table 3 are used in simulation to test the proposed protocol's performance. Both blackhole and DDoS attacker nodes are merged in different ratios of nodes in the hybrid attack scenario, as shown in table 4.

Table 4: Attacker Node Ratio

Total Number of Attacker Nodes	Blackhole Attacker Nodes	DDoS Attacker Nodes
2	1	1
4	2	2
6	3	3
8	4	4
10	5	5

Below is an analysis of the performance in detail.

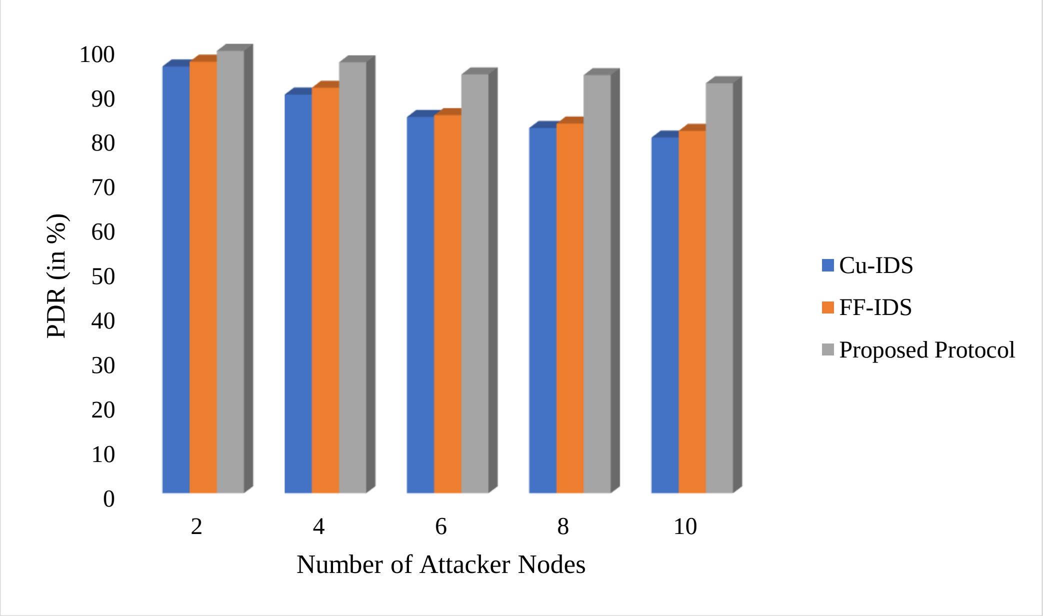


Figure 7: Packet Delivery Ratio (in presence of Hybrid Attack)-Scenario 2

According to the findings, the PDR for each protocol decreases with the increase in the number of attacker nodes. Despite this, the suggested method beats both Cu-IDS and FF-IDS on a constant basis. The proposed protocol has an average performance of 85.57 %, which is 8.7% better than FF-IDS and 11.9 % better than Cu-IDS.

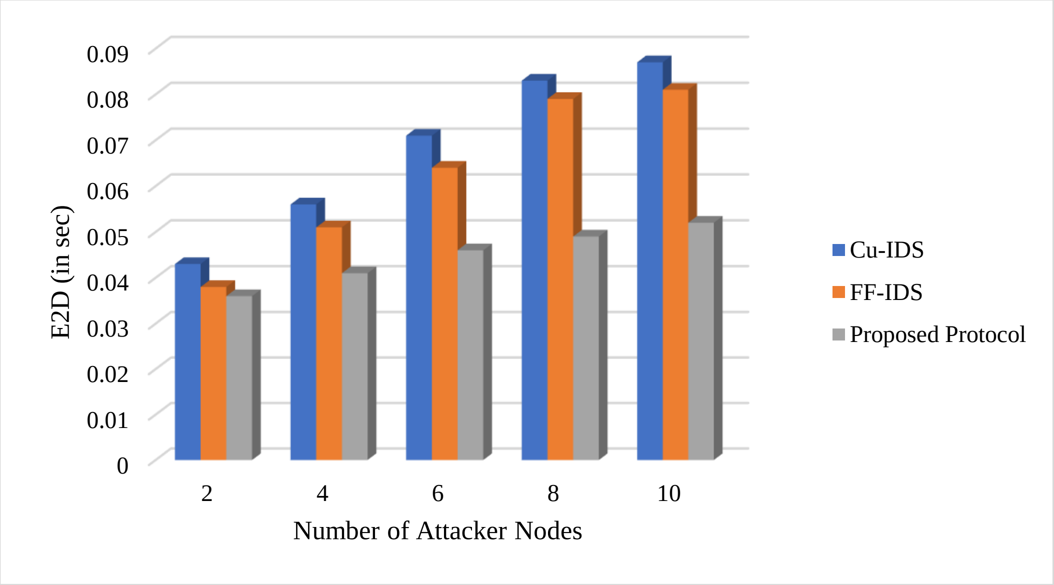


Figure 8: End to End Delay (in presence of Hybrid Attack)-Scenario 2

The proposed technique improves End to End Delay performance by 15.5% for FF-IDS and 11.2% for Cu-IDS as compared to proposed protocol. As the number of attacker nodes grows, the E2D climbs, as seen by the results.

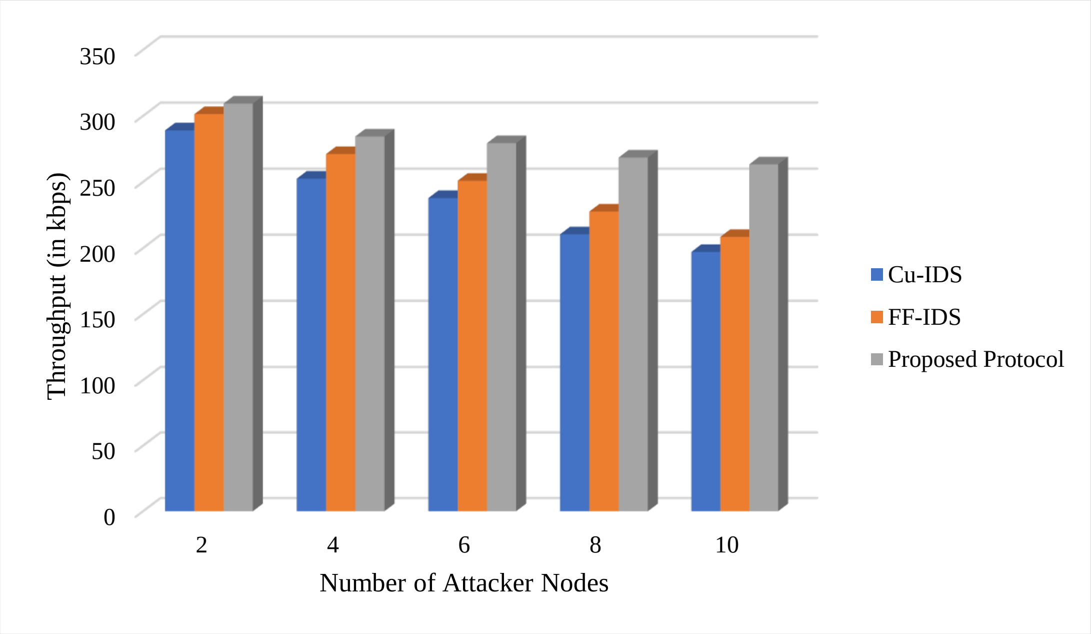


Figure 9: Throughput (in presence of Hybrid Attack)-Scenario 2

According to the findings, when the number of attacker nodes increases, the network's throughput decreases, suggesting that attackers have an effect on performance. The findings also show that the suggested protocols are less vulnerable to assaults and outperform Cu-IDS and FF-IDS when it comes to hybrid attacks. FF-IDS and Cu-IDS had average improvement rates of 12.8 percent and 21.3 percent, respectively.

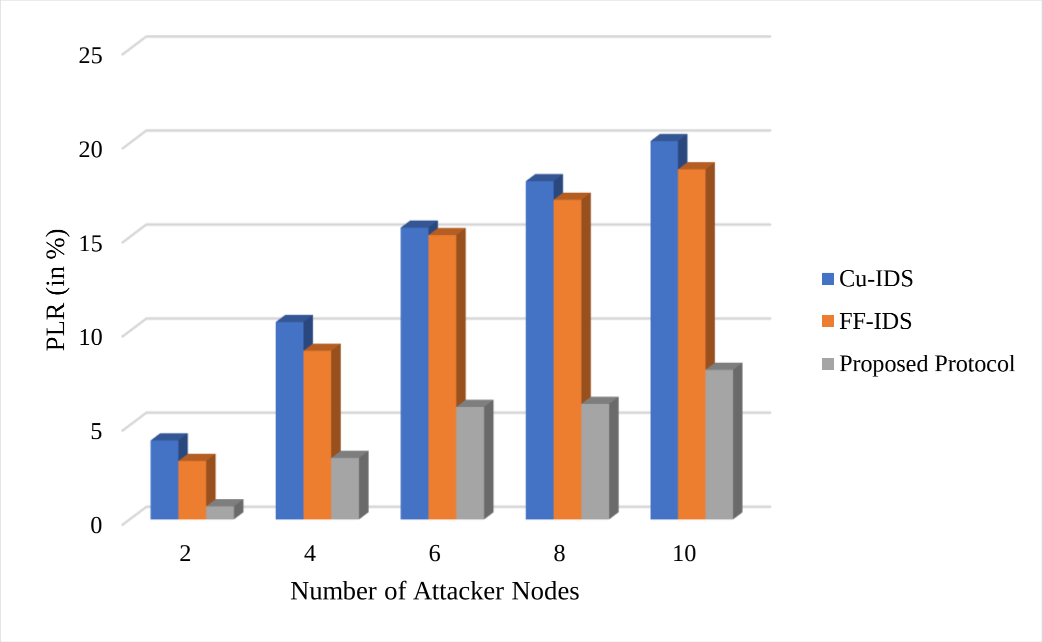


Figure 10: Packet Loss Ratio (in presence of Hybrid Attack)-Scenario 2

When there are various numbers of attacker nodes, the proposed protocol has a lower packet loss ratio than both Cu-IDS and FF-IDS. According to the results, the PLR from FF-IDS and Cu-IDS is decreased by 34% and 41%, respectively, which is a significant reduction that improves Network performance.

Conclusion and Future Scope

This proposed Protocol is designed to handle the Hybrid 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 50 nodes. The proposed protocol's performance is compared with the existing Cu-IDS and FF-IDS by varying number of attacker nodes in the same scenario.

The proposed protocol outperforms Cu-IDS and FF-IDS in the Hybrid attack scenario, with the greatest PDR, throughput, and least E2D, and PLR, as indicated in the table below.

Table 5: Performance comparison of Cu-IDS and FF-IDS and Proposed Protocol

Performance Parameter	*Protocols*	*Number of Attacker Nodes*				
		2	**4**	**6**	**8**	**10**
PDR	Cu-IDS	88.76	82.83	73.45	67.84	63.82
	FF-IDS	90.82	84.18	78.06	72.04	65.47
	Proposed Protocol	94.74	91.41	83.98	79.92	77.81
E2D	Cu-IDS	0.086	0.091	0.099	0.108	0.114
	FF-IDS	0.091	0.099	0.103	0.111	0.119
	Proposed Protocol	0.079	0.083	0.089	0.093	0.098
Throughput	Cu-IDS	119.93	102.81	89.23	74.83	71.81
	FF-IDS	130.28	112.74	94.38	87.92	83.04
	Proposed Protocol	154.27	128.47	107.97	98.37	94.36
PLR	Cu-IDS	11.24	17.17	26.55	32.16	36.18
	FF-IDS	9.18	15.82	21.94	27.96	34.53
	Proposed Protocol	5.26	8.59	16.02	20.08	22.19

Overall, the performance of the proposed protocol is on the top in all aspects, and it is concluded that this approach is the conqueror even in the existence of Hybrid attacks. The performance of the proposed protocol is quite effective.

References

[1] Justin V, Marathe N, Dongre N. Hybrid IDS using SVM classifier for detecting DoS attack in MANET application. *In2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* 2017; 775-778. DOI:10.1109/i-smac.2017.8058284

[2] Shailesh Funde, Bharti 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. DOI: 10.17148/IJARCCE.2019.81002

[3] 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. DOI:10.1007/s11277-019-06182-8

[4] Naveena A, Reddy KR. Malicious node prevention and mitigation in MANETs using a hybrid security model. *Information Security Journal: A Global Perspective*. 2018;27(2), 92-101. doi:10.1080/19393555.2017.1415399

[5] Yaseen QM, Aldwairi M. An enhanced AODV protocol for avoiding black holes in MANET. *Procedia Computer Science*. 2018; 134-376 doi:10.1016/j.procs.2018.07.196

[6] Mahuwa Goswami, Prashant Sharma, Ankita Bhargava. Black Hole Attack Detection in MANETs using Trust-Based Technique. *International Journal of Innovative Technology and Exploring Engineering Regular Issue*, 2020; 9(4), 1446-1451. doi:10.35940/ijitee.d1497.029420.

[7] Sazzat Hossain, Md. Sazzad Hussain, Romana Rahman Ema, Songita Dutta, Suborna Sarkar, Tajul Islam. 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; 1-7. doi:10.1109/icccnt45670.2019.8944395

[8] Jasdeep K., Dr.Harmeet S. DDoS Attack Detection and Prevention in MANETs. *International Journal of Advanced Science and Technology,* 2020; 29(3), 2402-2407. http://sersc.org/journals/index.php/IJAST/article/view/4341

[9] Ashu Gautam, Rashima Mahajanb, Sherin Zafarc. 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.

http://sersc.org/journals/index.php/IJAST/article/view/25655

[10] Adwan Yasin, Mahmoud Ameen Abu-Zant. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. *Wireless Communications and Mobile Computing*, 2018; 1-10. doi:10.1155/2018/9812135

[11] J Gowrishankar , P Senthil Kumar T Narmadha, Yuvaraj Natarajan A Trust-Based Protocol for Manets In Iot. Environment. *International Journal of Advanced Science and Technology*. 2020; 29(7). 2770-2775.
https://www.researchgate.net/publication/341642784_A_Trust_Based_Protocol_For_Manets_In_Iot_Environment

[12] Muhammad Salman Pathan, J. He, Z. A. Zardari, Muhammad Qasim Memon . An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. *Future Internet*, 2018; 10(2), 1-16. DOI:10.3390/fi10020016

[13] Moresh Madhukar Mukhedkar, Uttam Kolekar. 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). doi:10.1002/dac.4252

[14] Doddi Madhu Babu, & Maligala Ussenaiah, 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; 1-17. doi:10.1002/dac.4411

[15] J. Sathya Priya, M. A. Femina, R. A. Samuel, APSO-MVS: An adaptive particle swarm optimization incorporating multiple velocity strategies for optimal leader selection in hybrid MANETs. *Soft Computing*, 2020;1-17. doi:10.1007/s00500-020-05034-z

[16] Bata Krishna Tripathy, Swagat Kumar Jena, Padmalochan Bera, Satyabrata Das , An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks. *Wireless Personal Communications*, 2020; 114(2), 1339-1370. doi:10.1007/s11277-020-07423-x

[17] Deepak Sinwar,Nisha Sharma,Sunil Kumar Maakar, Sudesh Kumar. 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. doi:10.1080/02522667.2020.1733193

[18] Mr. R. Jayaraj, Dr. T. Suresh, Dr. K. B Jayaraman. 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] Ramireddy Kondaiah, Bachala Sathyanarayana. Trust Factor and Fuzzy Firefly Integrated Particle Swarm Optimization Based Intrusion Detection and Prevention System for Secure Routing of MANET. *International Journal of Computer Networks & Communications*, 2020; 10(1), 13-33. doi:10.5121/ijcnc.2018.10102

[20] Gondi Yasoda Devi, Gurrala Venkateswara Rao. 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. doi:10.35940/ijrte.e6379.018520

[21] Christy Jackson Joshua , Vijayakumar Varadarajan An optimization framework for routing protocols in VANETs: A multi-objective firefly algorithm approach. *Wireless Networks*, 2019; 1-10. doi:10.1007/s11276-019-02072-w

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

[23] Ch. Ram Mohan, Venugopal Reddy Ananthula. 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. doi:10.1142/s1793962319500144

[24] Neenavath Veeraiah, B. T. Krishna. An approach for optimal-secure multi-path routing and intrusion detection in MANET. *Evolutionary Intelligence*. 2020. doi:10.1007/s12065-020-00388-7

[25] Puri Vishal, A. Ramesh Babu. Firefly Algorithm for Intelligent Context-Aware Sensor Deployment Problem in Wireless Sensor Network. *Journal of Circuits, Systems and Computers,* 2019; 28(06), 1-38. doi:10.1142/s0218126619500944.

[26] Luisito Lolong Lacatan, Jaevier Angcao Villanueva, Albert Vinluan Information Technology Security Infrastructure Malware Detector System. *International Journal of Advanced Trends in Computer Science and Engineering,* 2020; 9(2), 1583-1587. doi:10.30534/ijatcse/2020/103922020

[27] Quy, V. K. A 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. doi:10.30534/ijatcse/2020/175932020

[28] Shubham Joshi, Dr. Durgesh Kumar Mishra. Detection of Rushing Attack and Data Modification Attack in Mobile Ad Hoc Networks. *Journal of Critical Reviews*, 2020; 7(19), 9486-9498.

[29] Md Ibrahim Talukdar,Rosilah Hassan, Md Sharif Hossen, Khaleel Ahmad, Faizan Qamar, and Amjed Sid Ahmed. Performance improvements of Aodv by black hole attack detection Using ids and digital signature. *Wireless Communications and Mobile Computing*, 2021; 1-13. doi:10.1155/2021/6693316

[30] Ashutosh Srivastava, Sachin Kumar Gupta, Mohd Najim, Nitesh Sahu, Geetika Aggarwal, Bireshwar Dass Mazumdar , DSSAM: Digitally signed secure Acknowledgement method for mobile ad hoc network. *EURASIP Journal on Wireless Communications and Networking*, 2021; 20(1), 1-29. doi:10.1186/s13638-021-01894-7

[31] José García, Victor Yepes, José V. Martí A hybrid k-means cuckoo search algorithm applied to the counterfort retaining walls problem. *Mathematics,* 2020; 8(4), 555-577. doi:10.3390/math8040555

[32] Muhannad Tahboush, Mary Agoyi A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET). *IEEE Access*, 2021; 9, 11872-11883

[33] kaur, J.,Talwar, R. and Goel, A.K., **“**MOpt Shield: An Intrusion Detection System based on Meld Optimization Algorithm to mitigate Amalgam Attacks” International Journal of Science and Technology,2021;14(20),1622-1634.doi:: 10.17485/IJST/v14i20.601