Security Improvement of AODV Routing Protocol through IPSO-IDRS Mechanism for Ad-hoc Networks

Shruti Dixit, Rakesh Singhai

***Abstract:** Ad-hoc network is vulnerable to different types of attacks because of its vigorously changing topology, limited storage capacity, absence of centralized infrastructure etc. Ad-hoc On Demand Distance Vector (AODV) is established protocol for routing for this type of networks. AODV is exposed to black hole attack due to the inadequacy of security consideration. The malicious nodes drop all information packets rather than sending it to the neighboring node. In this research paper, Anomaly based intrusion detection system (IDS) known as Particle swarm optimization (PSO) is purposefully utilized to detect the misbehavior activities in the network. In AODV routing protocol, swarm agents are used for identifying misbehavior activities of nodes based on dropping behavior of data packets. An intrusion response system (IRS) is activated after the detection of an intrusion. It is necessary to take action against black hole attack or reduce the effect of the damage caused by the attack. IDS and a response system are integrated for detection and removal of the source of an attack respectively. The guard nodes are placed in the network with the aim to oppose black hole attackers and in this way IR is initiated. The malevolent nodes detected by PSO are bypassed and new routing paths are established using guard nodes. This research has been carried out for analyzing the influence of malicious nodes and guard nodes on varying network size vice versa. The simulation study of proposed technique integrated particle swarm optimization intrusion detection response system (IPSO-IDRS) explains how it is better in terms of the performance metric like throughput and PDR.*

***Keywords:** Particle Swarm Optimization, Intrusion Detection Systems, Intrusion response system, black hole attack, guard nodes, AODV.*

I. INTRODUCTION

A MANET [1] is made out of wireless correspondence nodes performing self-setup in a dynamic mode. It does not require a perpetual infrastructure or centralized supervision and all mobile nodes are randomly moving within the network. The communication established between the mobile nodes are operational with a wireless transmitter as well as a receiver by means of bidirectional wireless links and plays the role of an end host and as a router. The routing protocol is approved to decide the routes and give correspondence between end points. MANET is well liked and appealing prepared to be utilized as a part of mishap conditions where an infrastructure is inaccessible or unfeasible to install like natural disaster, environmental monitoring, medical urgent situations, military conflicts etc.

The routing protocol schemes such as Dynamic Source Routing (DSR) and AODV are well-known on-demand routing for MANETs. Forwarding data packets between the source and target nodes is the basic routing operation performed by these protocols. Route request is broadcast by a source node to a target node first without the routing. It is received by the neighbouring node with the source and destination nodes addresses; it judges if it is identical with the target nodes address routing protocol should consider the uniqueness of the MANET. The essential requirements of these networks are trustworthiness of data transmission, robust, and adaptable selection of multiple path and giving protection to the system which expands the system execution. [2, 3]

The wide open channel and distant dissemination of ad-hoc network make it susceptible to various types of attacks rather than wired networks. Additionally, MANET's distributed architecture, dynamic topology, exposure of nodes and channels; a regular centralized monitoring system which is not possible in MANETs. It is crucial to build up IDS. Directly or indirectly, it affects the performance of each and every node in the network. It is tough to recognize an attack from a compromised node inside the system [4].

These networks are revealed to passive type of attacks as well as active attacks. Passive attacks target the confidentiality trait of the system and assemble the information about the network. During active attacks, the attacker may be focused to disturb the routine functioning of a definite node and target the functioning of the entire network. During the path finding process, a malicious node propagates the incorrect paths as correct paths to the source node. In black hole attack, the malevolent node make use of routing protocol for announcing itself as the closest route to the target node. It opposes to send packets to this node and it drops the routing packets.

There are two kinds of black hole attacks: 1. Single black hole type: the malicious node attacks independently. 2. Cooperative black Hole attack: multiple malicious nodes attack and take action collectively [5, 6].

[7, 8] An IDS is an integrated method to detect any attack in the network by analysing and continues monitoring network activities. It detects the attack commenced outside a network as well inside the network. In network security, intrusions are characterized as any pernicious activities that could trade off the uprightness, mystery or accessibility of systems or data sources.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Shruti Dixit*, Department of Electronics and Communication, UIT, RGPV, Bhopal, India. Email: shrutikdixit@gmail.com

Rakesh Singhai, Department of Electronics and Communication, UIT, RGPV, Bhopal. Email: sanikaskd@gmail.com

It is the kind of tool to detect and make alarms against such intrusions. Research paper talks about thought of intrusion detection and the overview some of principle methodologies of it, for example, sort of attacks addressed and architecture in MANET's. In distributed and cooperative (DAC) architecture, all nodes of the network participate in the detection of intrusion. This framework responds by means of agent of IDS working over them. It distinguishes and assembles neighbourhood activities and information for classifying the achievable interruption and furthermore responds independently. They additionally take part in the cooperative interruption discovery and additionally response methodology by switching the review information as well as identification results with neighbouring nodes so as to determine uncertain activities.

New branch in evolutionary algorithms is PSO [9]. It is capable for searching finest solutions build on the conception of swarm. It divulges itself very effectively in facing multi variable problems where real values are considered for variables. It has information sharing ability which improves the performance of routing protocol. It is a computational technique and for a given measurement value, it optimizes a candidates problem by repeatedly attempting to get better result and improve a user solution.

Swarm intelligence (SI) is an artificial intelligence discipline and multi-agent systems is designed which takes motivation from the cooperative activities of insects such as ants, wasps etc. and from group of animals of flock of birds, school of fish etc [10].

The research paper has five sections. Section II summarizes previous research works. Section III describes the proposed technique based on integration of PSO technique and IDRS for MANET. Section IV displays simulation results and a relevant performance analysis. Finally, Section V presents conclusion.

II. RELATED WORK

The research paper [11] has focused on security enhancement of ad-hoc networks. A unique trust management method has two types of observations: Direct and indirect. Bayseian interference method is used in case of direct and indirect type of observation in which Dempster- shefer theory is applied. Two observations are combined and performance metric like throughput and PDR are improved but at the cost of upsurge in overhead message and End to end delay. The extra processing and communication overhead is added by the scheme in order to form and sustain the hierarchical structure. An algorithm in [12] is based on PSO which improves QoS metrics such as end to end delay, NRL and PDR of AODV protocol. Energy aware multiple paths routing scheme in [13] is proposed in view of PSO which ascertain the best route to decrease the directing overhead which upgrades the reliability of the system in terms of transmission cost, energy and traffic ratio. The research paper [14] explains how the identified and unidentified traffic entering IDS is recognized by means of an incremental categorization algorithm based on PSO. It consists of two phases: 1. Classification phase (CLA) and 2. Clustering phase (CLU). CLA forms the classifier from the established network traffic data (labeled data). The newly incoming patterns are classified by CLU, labeling is done by PSO clustering. It is the CLU that makes the classifier dynamic. In [15], the routing behavior of the network for identifying the malicious paths for prevention against packet drop attack is analyzed. The research paper [16] has proposed two algorithms for detection of single black hole attack and multiple black hole attack in which routing overhead and communication overhead is reduced.

The proposed mechanism is the hybridization of DAC IDS, IRS architecture and heuristic method based Anomaly detection system. The advantage of DAC is it improves the detection accuracy and Anomaly based IDRS is efficient to identify new, unforeseen attacks and requires less maintenance. It constantly learns from the activities of the network. Anomaly based IDS called PSO in which swarm agents of the network discover misbehavior activities based on dropping nature of packets due to black hole attack. The updation of velocity and position in PSO is based on equations; it is efficiently used on large data sets. The main goal is to develop deterrent technique for misbehaving nodes by isolating and barring them from participating in the network and also from getting services of the network. It successfully detects malicious nodes against the AODV routing protocol and improves performance metrics.

III. PROPOSED TECHNIQUE

A. Overview

The fundamental motivation behind the anomaly based IDRS is to discover black hole attackers for creating unnecessary malicious activities. The prevention technique Known as IRS is used to avoid black hole nodes from taking part in the regular routing process. When black hole attack is activated, malicious nodes are randomly moving in the network. Swarm agents are connected to all nodes which are randomly moving in the network. The important function of the swarm agents is to collect packet information inside its range of transmission. The packet information is evaluated which are exchanged between the nodes of the selected routes. A node with a less packet dropping behaviour is considered as normal node for forwarding data packet from source to destination. Particular node in the path having high packet dropping behaviour is considered as malicious nodes. When an misbehaviour activities has been recognized by the IDS, the response system takes charge of reacting to attack and It keeps the attack from initiating any additional damage to the system. The guard nodes are placed randomly in the network for taking care of disturbed routing. Malicious nodes are bypassed by guard nodes from taking part in the routing. In this way, guard nodes play very important role in the routing by giving substitute routes. The degraded performance of the overall network is enhanced by combining PSO and IDRS in the AODV routing procedure.

B. Proposed technique

Identification of Malicious node Using PSO

In MANET, mobile nodes are randomly dispersed, independently moving and participate in routing procedure and thus data packets are forwarded between these nodes. Misbehaviour occurs in the mobile nodes due to the well known restricted operation of MANET. It is essential to shield network from malicious nodes. The characteristic of malevolent nodes is to drop the data packet or discards it instead of sending to its destination. Thus MANET performance automatically degrades due to the delinquency operation by black hole attackers. PSO is an effective computational technique which is inspired from swarm intelligence.

In PSO, the individual mobile nodes are called particles (Part) and the group of these mobile nodes is called a cluster (CL). The velocity and position of node i at iteration t+1 are calculated as shown below:

$$V_i^{t+1} = wV_i^t + c_1r_1(pbest(t) - S_i^t) + c_2r_2(gbest(t) - S_i^t) \quad (1)$$

$$S_i^{t+1} = S_i^t + V_i^{t+1} \quad (2)$$

Where w= inertia weight, it is utilized to control the effect of the past history of speeds on the present speed. c is constant used to find out the local best and global best position. pbest(t) is the Particle's own best and gbest(t)is the Particle's global best. From (2), position refreshed S_i^{t+1} is estimated dependent on the present position of the particles S_i^t and adjusted velocity V_i^{t+1}. When the speed for each particle is calculated as shown in equation (1), each particle's position is refreshed by applying the new speed to the particles past position. This system is reiterated until the point that some ceasing condition is met. Some normal ceasing conditions incorporate number of iterations of the PSO algorithm, a number of iterations since the past update of the global best candidate solution, or a predefined target fitness value. It optimizes the problem by continually trying it and enhances user solution associated to given measurement standards. The CL wander in an n dimension space for solution. Part from these CL is randomly moving and its position and velocity are updated according to mathematical expression. Each Part adjusts its coordinates according to its own suitability and the suitability of other Part. When the improved solution is found these will direct the movement of the CL. PSO is applied to find the best node in terms of fewer packets dropping behaviour and less network routing load (NRL). Nodes are classified into two groups on the basis of packet dropping behaviour as shown in figure.

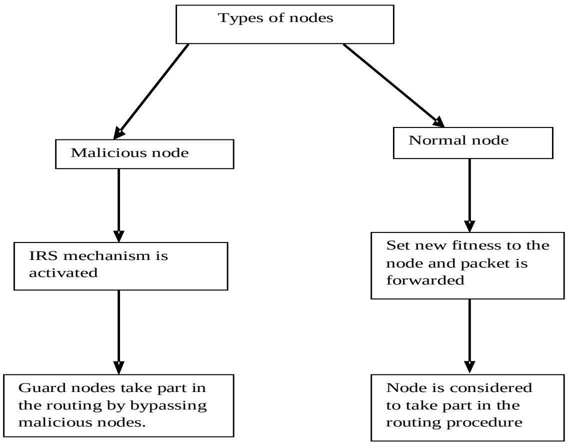

Types of nodes
Malicious node
Normal node
IRS mechanism is activated
Set new fitness to the node and packet is forwarded
Guard nodes take part in the routing by bypassing malicious nodes.
Node is considered to take part in the routing procedure

Fig. 1 Types of nodes

Identification of malicious nodes using proposed technique is briefed as below:

Abbreviations: Normal node: NN, attacker node: AN, Swarm Agents: SA, to differentiate between normal node and attacker node, Guard node: GN, to bypass the attacker node, Data packet: DP, Packet dropping behaviour: PDB, Network Routing Load: NRL, IR: Intrusion response, Mobile node: MN and AODV: ad-hoc distance vector, route establishment, NRP: Normal routing procedure.

```
Step 1: Route discovery is initiated using reliable MN.
Step 2: Route is established using AODV routing protocol.
Step 3: Attach SA to all MN in the network.
Step 4: DP is transmitted through the route.
Step 5: SA calculates PDB and NRL.
Step 6: If PDB and NRL < threshold
    {
      MN is declared as NN
      Velocity and position are updated
      Packet is forwarded;
      else
      MN is declared as AN
      IRS mechanism is activated
      MN is isolated or banned by GN;
    }
```

Step6: Finally the performance of IPSO-IDRS is evaluated.

The differentiation of nodes is totally dependent on PDB and NRL. If it is more than threshold value, the node is declared as black hole node. Packets are analysed by PSO agents using following parameters

1. NRL: It is determined as dividing the total number of routing packets conveyed by the source node to the total number of data packets arrived at the destination.
2. Number of dropped packets: When the data in the form of packets does not reach correctly at the destination and overloading situation of a network or a router in which is unable to accept extra packets at a given time.

Removal of malicious node using IDRS

The malicious nodes interrupt the usual routing of the Ad-hoc network. It is impossible to reach data to its destination without the help of nodes in that particular path. The malicious nodes in the route are identified by the IDRS based on PSO. Both types of nodes are present in the network that is normal nodes and malicious nodes. Few normal nodes are identified and extra responsibility is given to these nodes. Guard nodes inflict the following restriction in terms of forwarding of information and routing of packets. A preordained way of response to detection is to isolate or ban the identified attacker node. The attacker nodes are completely isolated or banned by the network nodes as a part of punishment. They are treated as non-existent for the network. The following restrictions are imposed by nodes in terms of forwarding of information and network routing service.

1. The intruding nodes generated packets are not forwarded by the nodes.
2. Data packets are not forwarded through the intruder.
3. The nodes are not allowed to send any routing packets to or through the attacker.
4. The routing packets originated from the attacker node are completely ignored.

Thus, the performance is elevated which was earlier degraded because of the nodes misbehaviour. The routing packets initiated from the black hole attacker are completely ignored by guard nodes. The major function of these nodes is to provide suitable paths for packet transmission by bypassing the malicious nodes and continuously monitors the adjoining nodes behaviour in the communication range. The nodes demand for information for routing and support from adjoining nodes in case of requirement.

Advantages of proposed mechanism

1. The main advantage of the proposed mechanism IPSO-IDRS is flexibility and adaptability capture of interdependencies. It uses less number of function evaluations and requires less time. It does not introduce additional communication overhead. It successfully detects malicious nodes due to black hole attackers which drop the packets and prevents the network from further dropping of packets.
2. The routes are established using AODV routing protocol and swarm agents are connected to every node for analysing the packet behaviour. Based on packet analysis, the nodes are categorized as active and malicious nodes. The updation of velocity and position in PSO are based on easy equations; it is efficiently applied on large data sets. PSO algorithm is better to find accuracy, iteration and requires less time.

IV. SIMULATION RESULTS

A. Simulation model and parameters

The performance of proposed mechanism is evaluated through NS-2 software. In the experiment, the performance metrics throughput and PDR are measured for the AODV protocol. The nodes are varied from 100, 110, 120, 130 and 140 randomly and the network of size 1200m x1200m region. The mobile hosts channel capacity is 2 Mbps.

5 cases have taken for assessing the network performance. In case 1, case 2, case3, case4 and case 5 network sizes are 100 nodes, 110 nodes, 120 nodes,130 nodes and 140 nodes respectively. 4 malicious nodes and 4 guard nodes are fixed for all cases. The threshold value of network routing load is 20 and number of dropped packets is 3000 for this simulation environment. If the values of NRL and number of dropped packets are greater than 20 and 3000 respectively, the mobile node is declared as the malicious node and for lesser value, the mobile node is declared as normal node. Table I is the summary of parameters used for simulation of network for our analysis. The transmission range of mobile nodes is 550m. In our simulation, the speed of nodes is varied from 1 to 100m/s. It is possible to see the impact of the particular velocity on performance metrics.

Table I Simulation settings

No. of Nodes	100, 110,120,130 and 140
Radio propagation model	Two way ground
Antenna model	Omni directional
Mac	802.11
Traffic source	CBR
Packet size	512
Radio range	550m
Routing protocol	AODV
No. of malicious nodes	4
No. of guard nodes	4

B. Result analysis

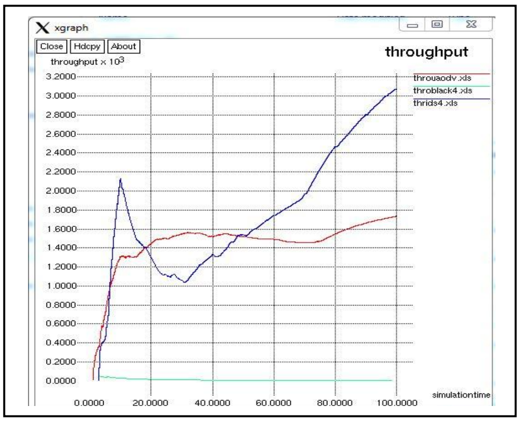
Based on number of nodes

Figure 2 to 6 shows comparison of throughput of normal AODV, AODV- malicious node in the situation when few nodes in the MANET network are made to exhibit malicious behaviour by dropping all data packets that come their way and proposed mechanism IPSO-IDRS.

C. Performance metrics

Throughput: Receiver takes successful delivery of total number of data packets transmitted by the transmitter.

Throughput is calculated for case 1 to 5 having fixed malicious nodes. Throughput of proposed mechanism is better in case of 1and 2 in comparison with normal AODV and AODV malicious node shown in figure 2 and 3. As in case of 3, 4 and 5, throughput is less than AODV but far better than AODV malicious node shown in figure 4, 5 and 6. Figure 7 shows the combined throughput for proposed mechanism in case of different number of nodes. As the network size expands from 100 to 140, the throughput linearly decreases due to the route length increase and non availability of route.



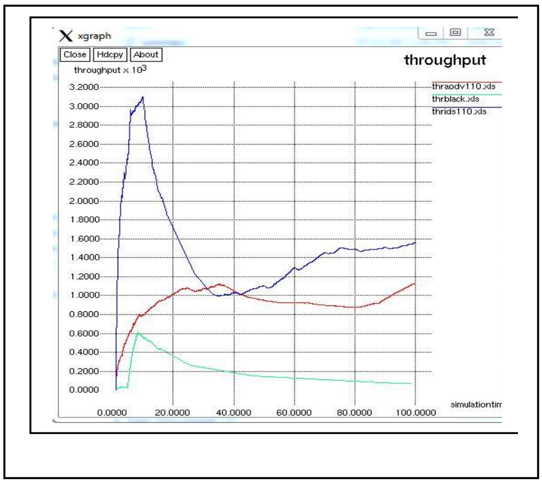


Fig. 3. Throughput for 110 nodes

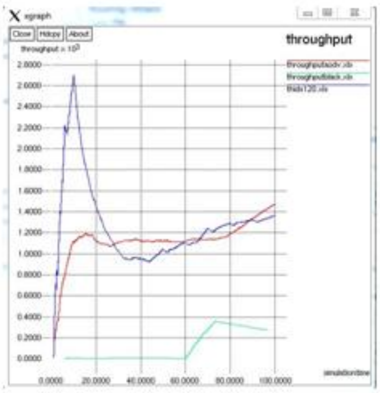


Fig. 4. Throughput for120 nodes

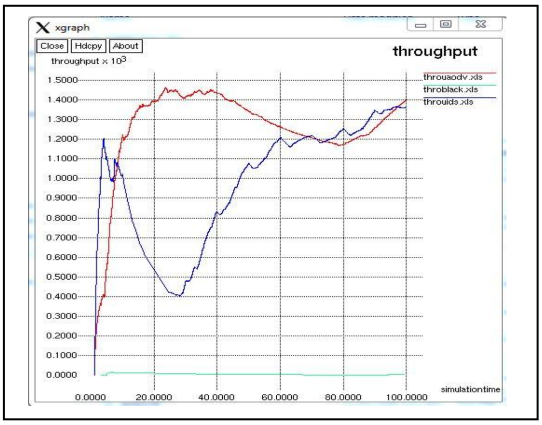


Fig. 5. Throughput for 130 nodes

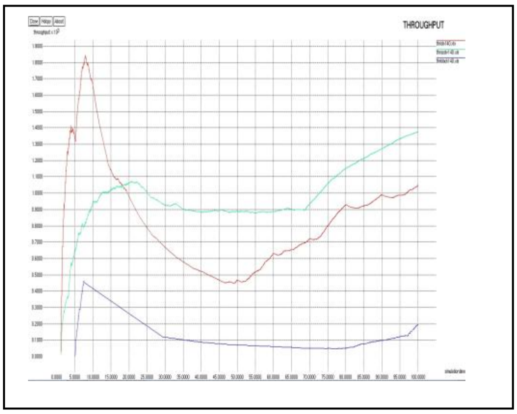


Fig. 6. Throughput for 140 nodes

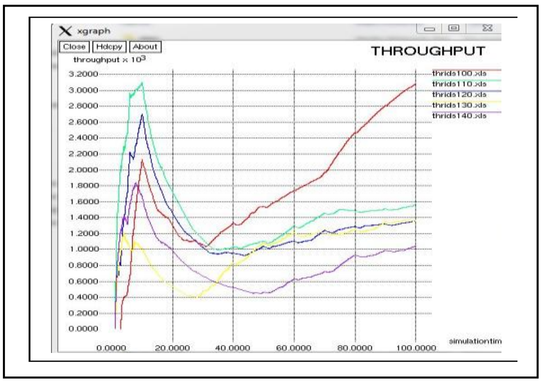


Fig. 7. Throughput for 100,110,120, 130 and 140 nodes

Packet Delivery ratio (PDR): It is the ratio of data packets received successfully by the target node to the number of data packets transmitted by the source node. Figure 8 shows the combined PDR for proposed mechanism in case of changed number of nodes. PDR linearly decreases as the network size expands. PDR is higher in all cases in comparison with PDR in black hole attack case.

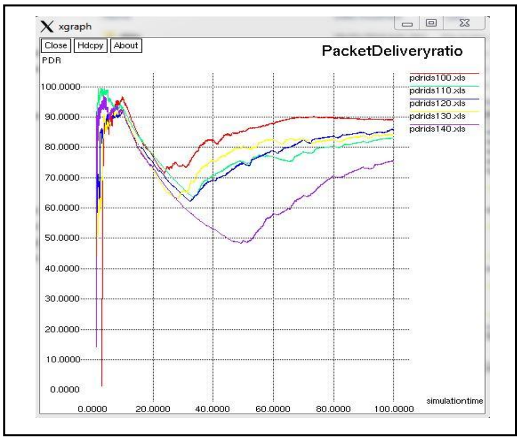


Fig. 8. PDR for 100,110,120,130 and 140 nodes

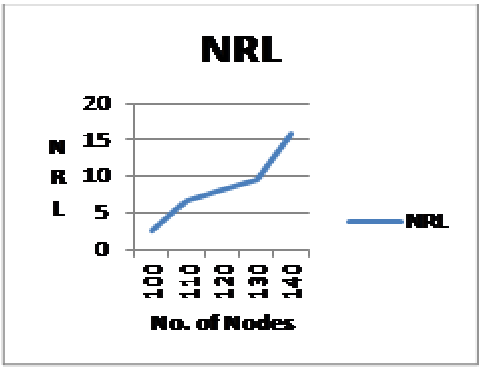


Fig. 9. NRL versus number of nodes

NRL of proposed mechanism is depicted in figure 9. As the network size increases from 100 to 140 nodes, NRL linearly increases as all the increased intermediate nodes are generating route reply. Table II shows NRL for AODV, network affected by black hole attack and proposed mechanism.

Table II NRL

Number of nodes	AODV	Black hole	Proposed mechanism
100	2823	4205	2184
110	2178	4089	1876
120	1703	4256	1399
130	3370	4241	1712
140	2864	4254	2211

NRL of AODV malicious is highest than the original AODV and IPSO-IDRS. Alternate routes are available for establishing connection between source and destination due to increased number of malicious nodes. Hence attackers would be avoided during subsequent route establishment.
Dropping of packets in case of proposed mechanism is reducing as number of nodes is increased from 100,110 and 120. But it is increased for 130 and 140 nodes due to increased availability of number of routes for fixed attackers and guard nodes as shown in figure 10.

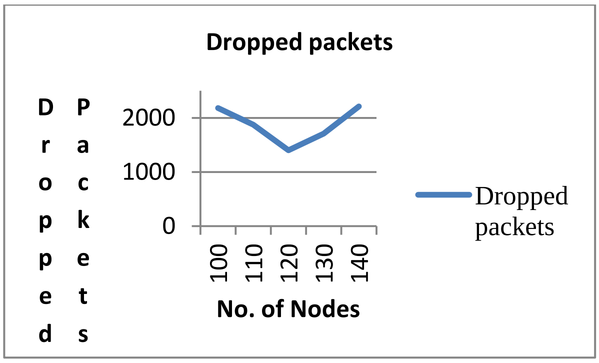


Fig. 10. No. of dropped packets

Table III Number of dropped packets

Number of nodes	AODV	Black hole +AODV	Proposed mechanism
100	1.34	454	2.26
110	3.6	52.2	6.65
120	2.66	15.56	8.07
130	2.36	1675	9.65
140	2.82	77.8	15.84

Table III shows number of dropped packets for AODV; network affected by black hole attack and proposed mechanism.

Impact of varying guard nodes on fixed node

In this experiment, the performance metric throughput is measured for the varying guard nodes for the fixed number of mobile node 120 for the AODV protocol. In the network of size 1200m x1200m, the nodes are moving randomly. 4 attackers are fixed and guard nodes are changed from 1, 2, 3 and 4 for assessing the network performance. The remaining simulation settings are same as discussed in the previous sections. Figure 11 shows comparison of performance metric throughput.

Table IV Throughput

Number of Guard nodes	AODV	Black hole	Proposed mechanism
1	1471.78	27.79	1164
2	1471.78	27.79	1193
3	1471.78	27.79	1297
4	1471.78	27.79	1495.99

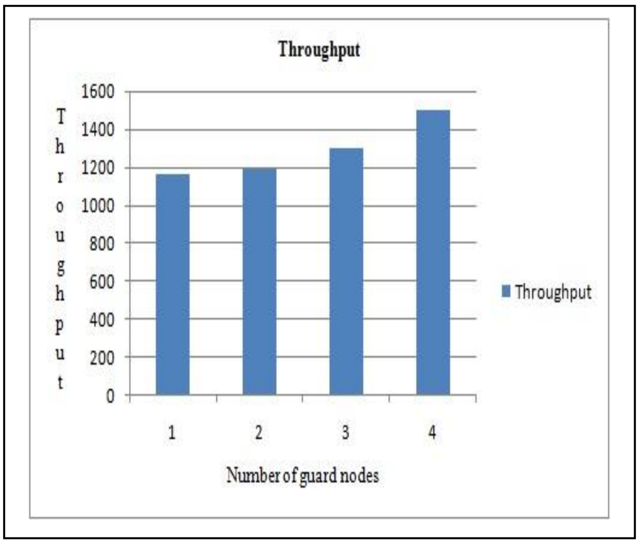


Fig. 11. Throughput versus number of guard nodes

Table IV shows the comparison of throughput for AODV, black hole attack case and proposed mechanism. Fig. 11 shows the graph between throughput and number of guard nodes. Throughput of proposed mechanism enhances as the number of guard nodes increases in the network. Overall network performance is uplifted which was degraded due to mobility of malicious nodes.

V. CONCLUSION

Normal routing in ad-hoc network is highly disrupted due to the activation of malicious nodes under the influence of black hole attack. A new technique, called IPSO-IDRS for identifying malevolent nodes and security mechanism against black hole attack is suggested. The implementation of varying size AODV, AODV for fixed number of attackers and IPSO-IDRS mechanism is evaluated for two qualities of service parameters throughput and PDR and compared also. As the network size goes on increasing, the performance of proposed technique for throughput and PDR is decreasing but higher than the normal AODV in case of 100 and 110 nodes but less than AODV in case of 120,130 and 140 nodes for fixed number of attackers. Performance metrics is always higher in all cases of black hole attack.

As the number of guard nodes increases from 1, 2, 3 and 4, there is increase in throughput. Alternate routes are available for establishing connection between source and destination due to presence of malicious nodes in the network. The suggested IPSO-IDS mechanism enhances the performance of AODV for throughput quality of service parameter. Future research can be further expanded to examine the robustness of ad-hoc networks for different kinds of routing protocols such as DSR, DSDV etc. and provide security to the neighbouring nodes. Developing a sound trust-based system and amalgamate it to the existing security methods, detection of new attacks as well as new preventive measures are the new directions for future research.

REFERENCES

1. Royer, E., & Toh, C. K. (1999). *A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks*. IEEE Personal Communications.
2. Liu, S., Yang, Y., & Wang, W. (2013). Research of AODV Routing Protocol for Ad Hoc Networks. AASRI Conference on Parallel and Distributed Computing and Systems, Elsevier.
3. Mohapatra, S., & Kanungo, P. (2012). Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator. International Conference on Communication Technology and System Design, Elsevier.
4. Tseng, F. H., Chou, L., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. *Human-centric Computing and Information Sciences, Springer*.
5. Kumar, V., & Kumar, R. (2015). An Adaptive Approach for Detection of Black hole Attack in Mobile Ad-hoc Network. International Conference on Intelligent Computing, Communication & Convergence, Elsevier.
6. Sharma, S., & Gupta, R. (2009). Simulation Study of Blackhole Attack in the Mobile Ad Hoc Networks. *Journal of Engineering Science and Technology*, 4(2), 243 – 250.
7. Anantvalee, T., & Wu, J. (2006). A survey on intrusion detection in mobile ad hoc networks. *Wireless/Mobile Network Security, Springer*, 170-196.
8. Shakshuk, E. M., Kang, N. & Sheltami, T. R. (2013). EAACK—A Secure Intrusion-Detection System for MANETs. *IEEE transactions on industrial electronics*, 60(3).
9. Kennedy, J., & Eberhart, R. (1995). Particle Swarm Optimization. IEEE.
10. Kolias, C., Kambourakis, G., & Maragoudakis, M. (2011). Swarm Intelligence in Intrusion Detection: A Survey. *Elsevier*.
11. Wei, Z., Tang, H., Richard, F., Wang, M., & Mason, P. (2014). Security Enhancements for Mobile Ad-Hoc Networks With Trust Management Using Uncertain Reasoning. *IEEE transactions on vehicular technology*, 63(9).
12. Trivedi, M. C., & Sharma, A. K. (2016). QoS Improvement in MANET using Particle Swarm Optimization Algorithm. Proceedings of the International Congress on Information and Communication Technology, Springer, 2.
13. Robinson, Y. H., & Rajaram, M. (2015) Energy-Aware Multipath Routing Scheme Based on Particle Swarm Optimization in Mobile Ad Hoc Networks. *Hindawi Publishing Corporation Scientific World Journal*.
14. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F., (2015). Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach. *IEEE systems journal*, 9(1).
15. Vhora, S., Patel, R., & Patel, N. (2015). Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET. *IEEE*.
16. Arathy, K. S., & Sminesh, C. N., (2016). A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET. *Procedia Technology, Elsevier*, 264 – 271.

AUTHOR PROFILE

Shruti Dixit is the research scholar in the Department of Electronics and Communication Engineering, University Institute of Technology, Rajiv Gandhi Prodyogiki Vishwavidyalaya, Bhopal, MP. She did her B.E degree from Government College of Engineering, Amravati, Maharashtra. She has done M. tech in Digital communication. Her favourite fields of interest are Networking, Ad hoc networks, Wireless Networking, Information Security etc. She is a life time member of IETE.

Dr. Rakesh Singhai is Professor in Department of Electronics and Communication Engineering, University Institute of Technology, Rajiv Gandhi Prodyogiki Vishwavidyalaya, Bhopal, MP. He did his PhD and M. tech from IIT, Delhi. He has more than 27 years of teaching experience of UG and PG students. He has published more than 40 papers in various International journals and Conferences. He has also received Best student award at IEEE 15th International conference on Software, Telecommunication and Computer Networks held at Spilt-Dubronik, Croatia in 2007.