A Novel Black Hole Attack Prevention System Based on Particle Swarm Optimization and Intrusion Detection System in MANET

Shruti Dixit [1], Rakesh Singhai [1]
[1] Department of Electronics and Communication,
UIT RGPV, Bhopal
(shrutikdixit@gmail.com)

Abstract- An ad-hoc network is the collection of cooperative wireless nodes without existence of any access point or centralized infrastructure. The nodes communicate independently through wireless network without any central control. Routing is the task of directing data packets from a source node to a given destination. The routing is complex procedure due to the dynamic topology, limited process, storing capability, bandwidth constraints , lack of the central control and so on cause the intrusion detection system(IDS) more complex. In this research work, swarm agents are attached to mobile nodes using Particle swarm optimization (PSO) for detecting malicious nodes in the established path and make routing more secure. Packet dropping behaviour of black hole attackers is analyzed with trust value in terms of network routing load and number of dropped packets. Each active node monitors its neighbour nodes within its transmission range and collects the trust value from all the monitored nodes. If the active node finds any node below a minimum threshold, then the node is discernible as malicious node. An IDS is activated by placing preventers in the network. Preventers carry out ideal routing by bypassing malicious nodes. Ad-hoc on demand distance vector (AODV) is used as the basic routing protocol to evaluate the proposed approach and give a performance analysis. This research has been carried out for analysing the impact of fixed mobile nodes, malicious nodes and preventers on varying velocity of nodes. The simulation study of proposed technique explains how it is better in terms of the performance metric throughput.

Index terms *– MANET; particle swarm optimization; trust value; active nodes and malicious nodes.*

I. INTRODUCTION

A set of wireless communication nodes performing self-configuration in a dynamic mode for the formation of network excluding fixed infrastructure or centralized supervision is termed as MANET [1]. This network is relatively a new communication paradigm, which contains a group of mobile devices communicating through a wireless medium. In addition to the role of a router, the nodes also play the role of an end host. [2] The routing protocol in such a network is authorized to determine the routes and provide communication among end points through intermediate nodes. MANET is well liked and attractive since they offer good communication in the changing infrastructure for the applications such as rescue operations, tactical operations, environmental monitoring, conferences etc. The nodes can setup communication with each other nodes through intermediate mobile nodes to relay data transmissions when the distance between the two nodes is beyond the communication range of their own. The routing protocols such as AODV and DSR [3] in such a network are authorized to determine the routes and provide communication among end points through intermediate nodes. MANET research has been conducted on various aspects such as routing, security, quality of service, IP addressing, multiple access, and management of these networks. A significant part of the research work has focused on providing security services for MANETs, because security is the main obstacle for the widespread adoption of MANET applications. MANETs are vulnerable in their functionality intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. The network layer is vulnerable to black hole attack because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, a lack of clearly defined physical network boundary and the transient nature of services in the network. PSO is a computational method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. PSO technique is applied on IDS to overcome the problems in the network in terms of attacks.

The starting section of this paper discusses about AODV routing protocol, black hole attack, concept of PSO and IDS. Later section discusses about previous established research work. Followed to which, proposed research algorithm is explained. Section 4 displays simulation results and a relevant performance analysis. Finally, Section 5 presents conclusion.

A. Theoretical Background

It is necessary to discuss the following subsections for understanding of the problem.

1. Overview of Routing protocol AODV

AODV [4] is a well-known on-demand routing for MANETs. It is an enhancement of proactive routing protocol destination-sequenced distance vector. Routes are established when they are required. It reduces the number of broadcasts by creating on-demand routes as opposed to proactive routing protocols. It maintains two procedures (i) route discovery and (ii) route

maintenance, which are briefly discussed in the following sections.

1.1 Route discovery

In this process, AODV entails flooding of route request (RREQ) packets generated by source node. These packets contain address of destination and are broadcasted by intermediate nodes. To find a path to the destination, source node broadcasts a RREQ packet. The neighbors in turn broadcast packets to their neighbors till it reaches an intermediate node or destination. Information of RREQ packet is forwarded by intermediate nodes which can be changed or modified on the basis of hop-by-hop procedure. This forwarded information is circulated by an intermediate node. Such node keeps this record in the routing table. In AODV, modified information is maintained by hop count, which is incremented by 1 at every hop that forwards RREQ. These RREQ packets hold sequence number to ensure that selected route is loop free, and it also ensures that intermediate node should reply only latest information (not duplicated/old information). A node discards packet, if it has been received already. This information is used to construct route reverse path for the route reply packet. As the route reply packet traverses back to the source, then intermediate nodes store this forwarded information into their tables.

1.2 Route maintenance

Besides route discovery process, the already set up routes need to be repaired when the promised provided route cannot be guaranteed. When there is disconnection of a link on the route, e.g. some transient node may move out of range, the neighbor nodes will notice the absence of this connection. If so, the neighbor nodes will check if there is any route in its routing table which the next hop is this disconnected neighbor. So, source can reinitiate route discovery if needed.

2. Black hole attack

MANETs are exposed to both passive and active attacks [5, 6]. During active attacks, the attacker may be directed to disrupt the normal operation of a specific node or target the operation of the whole network adversary does injecting packets to invalid destinations into the network, deleting packets, replication, alteration and removal of swapped data, while passive attacks are not disruptive but are information seeking and attacker listens to the channel and packets containing secret information which may be critical in the operation of a protocol. It results in eavesdropping of data.

Routing protocols are exposed to a variety of attacks. [7] Black hole attack is one such attack and a kind of Denial Of Service (DoS) in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires.

3. PSO

Particle swarm optimization (PSO) is a stochastic optimization technique developed by the inspiration of the social behavior of bird flocking or fish schooling. In PSO, each single solution is a 'bird' in the search space (particle). The strength value is combined with each particle, which is calculated by the fitness function to be optimized, and it has the velocity, which expresses the flying of the particle. The particles will fly in the search space and will adjust with the velocities dynamically according to their historical behaviors. This process will guide the particles to fly toward the better search area in the search space. In MANET, the work of sending the packets from source to destination is difficult because of the mobility of the elements and there is no central control. To solve these problems, the swarm intelligence concept can be applied. The PSO algorithm was initially introduced by Kennedy and Eberhart (1995) in terms of social and cognitive behavior. This technique resolves the problems in various fields such as engineering and computer science [8, 9].

4. IDS

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations of computer security policies, acceptable or standard security practices. When a mobile node integrity, confidentiality, or availability is attacked by a set of actions intrusion prevention techniques can be taken into account [10, 11]. ID is a method of identifying and responding to malicious and hostile activities targeted at computing and networking resources. Systems that are assigned to perform all the procedures related to intrusion detection are called IDS. IDSs achieve detection by continuously monitoring the network for unusual activity and taking direct preventive measures such as blocking a suspected connection. It can be run on each mobile node to check local traffic and local intrusions. Each node has local IDS that by this, node can connect to network and local IDS checking all send or receive data in/out node. There are three main components of IDS: data collection, detection, and response. The data collection component is responsible for collection and preprocessing data tasks: transferring data to a common format, data storage and sending data to the detection module.

The alarm part Intrusion detection can be classified into three broad categories: anomaly detection, signature or misuse detection, and specification based detection.

The first detection method examines the activity of the entire infrastructure for patterns of misuses known beforehand, usually referred to as "attack identities". On the opposite, anomaly detection approaches analyze the behavior of the protected system over time toward extracting an approximate estimation of what behavior is considered normal (or legitimate). A baseline profile of normal system activity is

created. Any system activity that deviates from the baseline is treated as a possible intrusion. Specification based detection method describes the correct operation of a program or protocol. It sets the constraints and monitors the execution of the program with respect to the defined constraints. These two criteria have been associated with two performance evaluation variables: (i) Detection Rate (DR), which is defined as the ratio of the number of correctly detected attacks to the total number of attacks, and (ii) the False Alarm Rate (FAR), or false positive rate, which is the ratio of the number of normal connections that are misclassified as attacks to the total number of normal connections. An IDS maintains high detection rates and false alarm rates as low as possible

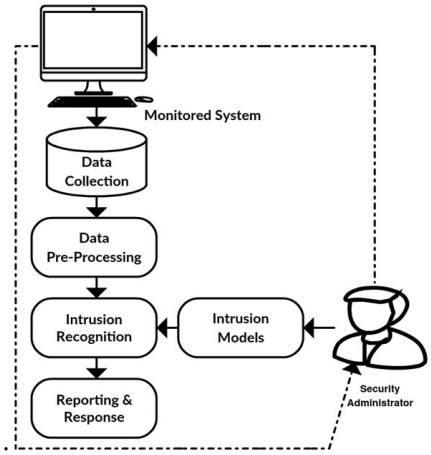

Fig. 1 IDS system

II. Literature review

The quality of service of the network is enhanced in terms of packet loss by exclusion of Black hole node from route establishment process [12]. Each node trust value is calculated and this value will be increased depending upon the ability to forward packet and ability to forward route request. The paths are established at the time of route discovery where more trusted nodes are involved. First calculated trust values are saved in the routing table and thus the route establishment is done.

An algorithm [13] based on PSO algorithm helps in improving QoS metrics such as end to end delay, NRL and PDR of AODV protocol.

[14] Energy aware multiple paths routing scheme is proposed in view of PSO which ascertain the best route to decrease the directing overhead which upgrades the reliability of the system as far as transmission cost, energy and traffic ratio.

[15] This paper proposed a novel approach for enhanced intrusion detection system for malicious node to protect against attacks in ad-hoc on demand distance vector routing protocol. It leads to identify malicious node, less conservation and less communication breakage in ad- hoc routing. This approach has been found advantageous for identifying malicious nodes in black hole attack, neighbor attack, sequence number attack and packet forwarding attack up to 700 nodes.

[16] A swarm based efficient distributed IDS for MANET was proposed. The nodes with highest trust value, residual bandwidth and residual energy are selected as active nodes by utilizing swarm agents. Each active node collects the trust value from all monitored nodes. The active nodes adaptively change as per the trust thresholds. Upon collaborative exchange of the trust values of the monitored nodes among the active nodes, if the active node finds any node below a minimum trust threshold, then the node is marked as malicious.

[17] Machine learning techniques like Neural Network (NN), Support Vector Machine (SVM) and Rough Set etc. are proposed for an efficient and Intelligent Network IDS. There is an immediate need to combine all security technologies under a complete secure system that integrates the strength of these technologies. In this research work, researchers have combined PSO and its variants with various machine learning techniques used for anomaly detection in network IDS so as to enhance the performance of IDS.

[18] The research article recommends and determines the most productive methodology for each node to decide the retransmission probability likelihood as indicated by its neighborhood density, available bandwidth and remaining energy of a node. The proposed PSO probabilistic broadcasting (PSOPB) scheme outperforms the other probabilistic broadcasting methods based on artificial intelligence, multi-objective problem, fuzzy logic and binary evolutionary algorithm.

[19] The routing behavior of the network for identifying the malicious paths for prevention against packet drop attack is analyzed.

[20] Intrusion detection system based on trust authentication routing and bio-inspired approach called TRAB-IDS introduced a method in which deep packet inspection (DPI) and trust algorithm is integrated in order to provide protection against severe intrusions. The simulation results evaluate the performance of the proposed TRAB-IDS in terms of delivery ratio, delay, security cost, and misdetection ratio.

[21] The research paper proposes and implements a novel IDS named Adaptive three Acknowledgments (A3ACKs) that takes care as well as solves three critical issues of Watchdog technique, which are receiver collision, restricted transmission power and collaborative attacks. The A3ACKs technique is based on Dynamic Source Routing which is an acknowledgement-based scheme. The proposed system implements and tests under different networks with various mobility speeds.

III. PROPOSED ALGORITHM

In this paper, a particle swarm optimization based Intrusion Detection System for MANET is proposed. The PSO algorithm helps in identification of the active nodes and malicious nodes. The route is established as per the AODV routing protocol. The overall network performance is degraded due to the activation of black hole attackers. The behavior of the attackers is identified by dropping of routing packets. In selected route, random initialization of neighboring nodes, collect neighboring information from all monitored nodes within its transmission range. The nodes are evaluated on the basis of trust values. Trust parameters are network routing load and number of dropped packets. The nodes with highest values are identified as malicious nodes. This is done to carry out the process of intrusion detection. The node changes adaptively as per the trust thresholds. Then the active nodes collaboratively exchange the trust values with its neighboring active nodes. If trust value

is less, the node will be declared as active node and allows to forward packet. The node maintains the trust value and stored it in the forward table. Upon detecting the malicious node having higher values of network routing load and dropped packets, the active node sends an alert message to the source node. The source then deploys a defense mechanism IDS to filter the malicious nodes from the network.

Packets are analyzed by PSO agents using following parameters

- Network routing load (NRL): It is calculated as dividing the total number of routing packets delivered by the source node to the total number of data packets arrived at the destination.
- 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 it is not able to accept extra packets at a given time.

IV. SIMULATION RESULTS

A. Simulation model and parameters

The performance of proposed technique is evaluated through NS-2 software. In the experiment, the performance metric throughput is measured for the AODV protocol. The mobile nodes are 100 and moving randomly in the network of size 1200m x1200m region. In our simulation, 2 Mbps is the channel capacity of mobile hosts for our simulation environment.

AODV routing is simulated and compared for 3 different conditions1. Normal AODV, 2. AODV attacked by black hole attackers 3. Proposed algorithm. These 3 different conditions are analyzed for 5 velocities such as 5,10,15,20 and 25m/s in order to assess the network performance. 4 malicious nodes and 4 preventers are fixed for all cases. In table 1 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.

Table 1 Simulation settings

Number of nodes	100
Radio propagation model	Two way ground
Antenna model	Omni directional
Mac layer	802.11
Traffic source	CBR
Packet size	512
Radio range	550m
Routing protocol	AODV
No. of attackers	4
No. of preventers	4

B. Result analysis

1. *Based on varying velocity of mobile nodes*

The network animator for proposed algorithm is shown in figure 2 in which black hole nodes and preventers are shown separately.

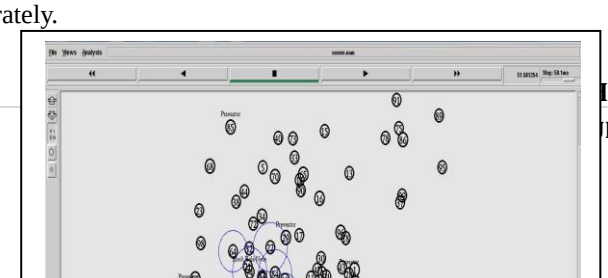

Fig. 2 NAM for velocity 10m/s of proposed algorithm

Figure 3 to 7 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 behavior by dropping all data packets that come their way and proposed algorithm.

Throughput: Receiver takes successful delivery of total number of data packets transmitted by the transmitter. Throughput is calculated for different velocities of mobile nodes having fixed malicious nodes. Throughput of proposed technique is better for all velocities in comparison with normal AODV and AODV malicious node.

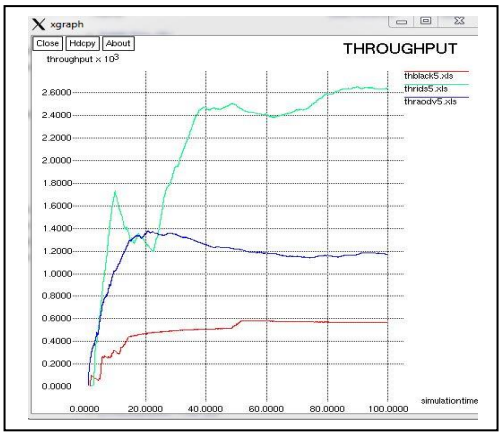

Fig. 3 Throughput for velocity 5m/s

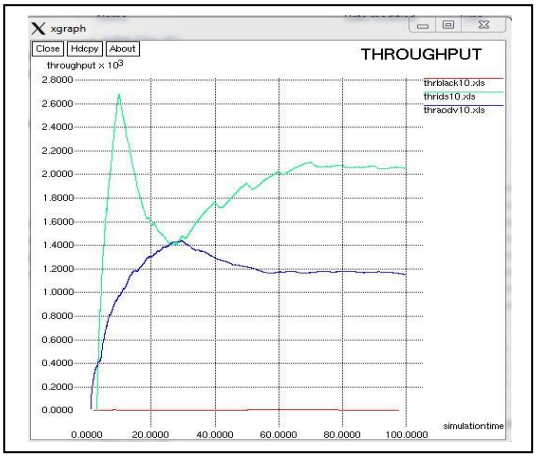

Fig. 4 Throughput for velocity 10m/s

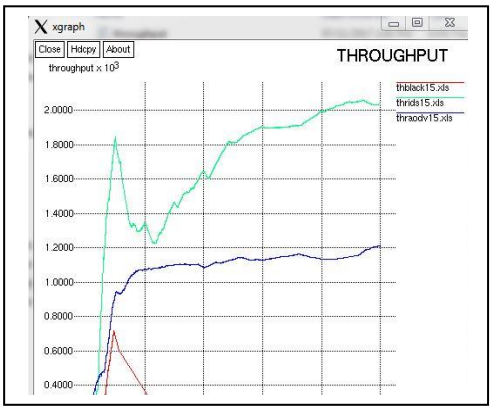

Fig. 5 Throughput for velocity 15m/s

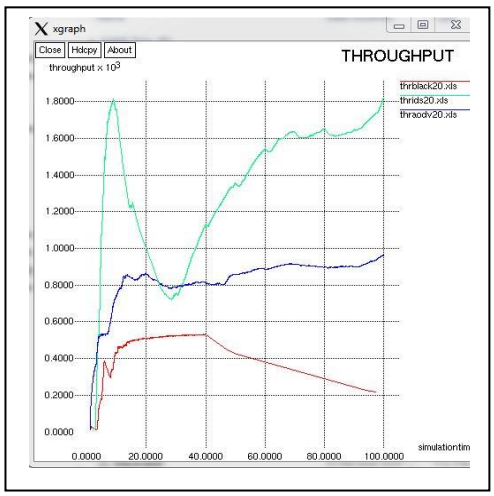

Fig. 6 Throughput for velocity 20 m/s

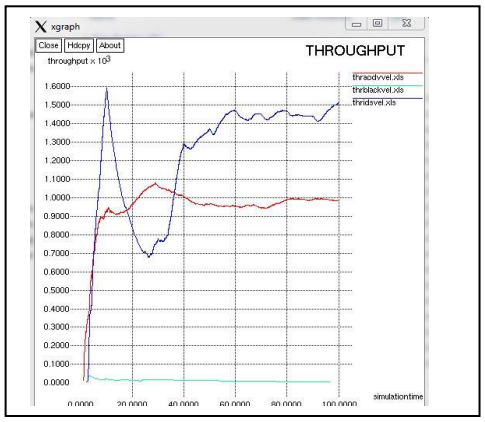

Fig.7 Throughput for velocity 25m/s

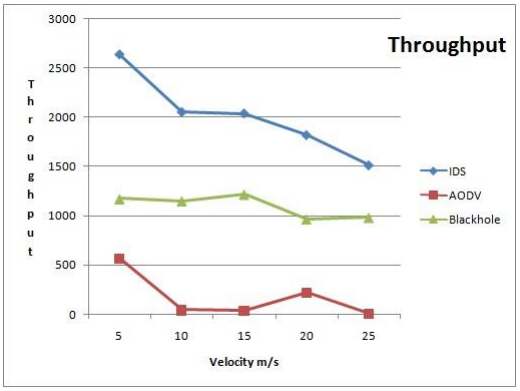

Fig. 8 Throughput versus velocity

Fig. 8 shows throughput versus velocity graph. Throughput is goes on decreasing as the velocity of nodes increases but throughput of proposed algorithm is maintained higher than normal AODV and black hole case.

Fig. 9 PDF versus velocity

Fig. 9 shows PDF versus velocity in m/s for proposed algorithm. Packet delivery fraction for proposed algorithm linearly increases for 5, 10 and 15 m/s velocity of mobile nodes but for 20 and 25 m/s velocity it abruptly reduces. Due to high mobility the preventers are unable to provide substitute paths for transmission of data and malicious nodes drops the packets.

V. CONCLUSION

MANETs are more susceptible to security attacks rather than wired networks. If the node is outside the transmission range it is communicated via intermediate nodes in this way multi-hop scenario is formed. Non-cooperation by this nodes may occur which can severely degrades the performance of network. The misbehavior of the malicious node is a major problem in

MANET. The malicious nodes are not primarily concerned with power or any other savings but interested in attacking and damaging the network. These misbehaviors of the malicious nodes will impact the efficiency, reliability and fairness. So it is essential to detect the malicious nodes in MANET. This research work proposes an algorithm based on PSO and IDS. It uses trust value of each node in the path based on NRL and number of dropped packets to detect malicious nodes in an efficient manner and these malicious nodes are bypassed using IDS which enhances the performance of MANET. Future research can be further expanded to implement proposed algorithm for DSR and DSDV routing protocols.

REFERENCES

[1] Basagni, S., Conti, M., Giordano, S. (Eds.). Mobile Ad Hoc Networking. Canada: John Wiley & Sons, Inc. (2004).

[2] Anuj K. Gupta, Harsh Sadawarti, Anil K. Verma "A Review of Routing Protocols for Mobile Ad Hoc Networks", WSEAS transactions on communications, Issue 11, Volume 10, November 2011.

[3] S. Ahmed and M. S. Alam, "Performance Evaluation of Important Ad-hoc Network Protocols", EURASIP Journal on Wireless Communications and Networking", Hindawi Publishing Corporation, pp. 1–11, 2006.

[4] S. Mohapatra, P.Kanungo, "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator", International Conference on Communication Technology and System Design, Elsevier, 2012.

[5] Nichols, R. K., and Lekkas, P. C. Wireless Security Models, Threats, and Solutions. McGraw–Hill, 2002, ISBN: 0-07-138038-8.

[6] S. A. Arunmozhi a & Y. Venkataramani , "Black Hole Attack Detection and Performance Improvement in Mobile Ad-Hoc Network", Information Security Journal: A Global Perspective, taylor and franchis , pp. 150–158, 2012.

[7] Parvinder Kaur, Dalveer Kaur, Rajiv Mahajan, "_ Simulation Based Comparative Study of Routing Protocols Under Wormhole Attack in Manet", Wireless Personal Communication, Springer, 2017

[8] James Kennedy and Russell Eberhart, "Particle Swarm Optimization", IEEE, 1995.

[9] C. Kolias, G. Kambourakis, M. Maragoudakis, "Swarm intelligence in intrusion detection: A survey", Elsevier, 2011.

[10] Sunil Kumar and Kamlesh Dutta, "Intrusion detection in mobile ad hoc networks: techniques, systems, and future challenges", security and communication networks, Willey online library, 2016.

[11] Tiranuch Anantvalee, Jie Wu, "A survey on Intrusion Detection in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer , pp. 170-196, 2006.

[12] Radha Krishna Bara, Jyotsna Kumar Mandal and Moirangthem Marjit Singh, "QoS of MANET Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack", International Conference on Computational Intelligence: Modelling Techniques and Applications , Elsevier, 2013.

[13] Munesh Chandra trivedi, Anupam kr. Sharma, "QoS Improvement in MANET Using Particle Swarm Optimization Algorithm", Proceedings of the International Congress on Information and Communication Technology, Springer, Volume 2, June 2016.

[14] Y. Harold Robinson and M. Rajaram, "Energy-Aware Multipath Routing Scheme Based on Particle Swarm Optimization in Mobile Ad Hoc Networks", Hindawi Publishing Corporation Scientific World Journal, 2015.

[15] S. Umang, B.V.R. Reddy and M.N. Hoda, "Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption', The Institution of Engineering and Technology, Vol. 4, Iss. 17, pp. 2084–2094, 2010.

[16] G. Indirani and K. Selvakumar , 'A swarm-based efficient distributed intrusion detection system for mobile ad hoc networks (MANET)' International Journal of Parallel, Emergent and Distributed Systems, Taylor and francis ,Vol. 29, No. 1, pp. 90–103, 2014.

[17] Khushboo Satpute, Shikha Agrawal, Jitendra Agrawal, Sanjeev Sharma,"A Survey on Anomaly Detection in Network Intrusion Detection System Using Particle Swarm Optimization Based Machine Learning Techniques", Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), Springer , pp. 441-452, 2013.

[18] Sumit Kumar, Shabana Mehfuz, "Intelligent probabilistic broadcasting in mobile ad hoc network:a PSO approach", J Reliable Intell Environ, Springer, 2016.

[19] Sumaiya Vhora, Rajan Patel, Nimisha Patel, "Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET", IEEE, 2015.

[20] Anusha K and Sathiyamoorthy E , "A new trust-based mechanism for detecting intrusions in MANET", information security journal: a global perspective, Taylor and Franchis, June 2017.

[21] Abdulsalam Basabaa, Tarek Sheltami and Elhadi Shakshuki, "Implementation of A3ACKs intrusion detection system under various mobility speeds", 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014) , pp. 571 – 578, 2014.

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.