International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-11, September 2019

# An optimal Security Mechanism to Preventmulti-threat in MANET using Bee Algorithm

**Pooja Rani, Tanupreet singh**

***Abstract:*** ***The special characteristics of the Mobile and Ad hoc network (MANET) attract the users to access the services provided by the network. But, accessing these services such as high mobility also creates an issue of unstable routing which leads to packet dropping. To address this issue, the packet dump situation is considered in this document under normal and distortion mode. This paper also focused on black hole attack (BHA) and selective packet drop attack (SPDA) and has a threat prevention mechanism has been proposed. The whole paper is divided into three frames namely employing deployment model, the importance of intrusion and its prevention, and registration of new node through interpolation named as Chebyshev method. The prevention structure has been modeled using swarm and machine intelligence. In addition, the affected route has been detected using the Artificial Bee Colony (ABC) inspired Optimal Bee Behaviour (OBB) algorithm. The different parameters, such as, Delay, energy consumption,Throughput and Packet Delivery Ratio (PDR) are computed. The proposed work consumes less energy as the developed architecture compared with sate of art techniques which states that energy consumption revamped by 12%. The delay rate has been ameliorated by 69% and 10% in contrary to past studies. The proposed prevention structure provides 1.8% improvement for throughput in comparison to without prevention architecture. However, proposed model provides 0.94 PDR using the polynomial kernel in comparison to state of art techniques. The comparative analysis has been performed with the existing work and outperformance has been noticed in terms of QoS.***

***Index Terms*****: *MANET, ABC, SPDA, THROUGHPUT, PDR About four ommas.***

## I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) is known for its mobility and ad-hoc architecture. The nodes in the network move from one end to another end with a speed of 4-5 Km/hr and transfer the data from the source end to the destination end. MANET may support unicast and multicast routing architecture [1]. The unicast model routing architecture provides a single source and single destination roadmap whereas, in multicast routing architecture, there are more than one sources and more than one destination nodes. The nodes sense their nearby nodes and select appropriate nodes for communication and data transfer. Based on the routing architectures, MANET is divided into two sub-categories namely reactive and proactive routing set [2]. The proactive architecture discovers the route only once at the start of the simulation setup as for the first time no source and destination is set. Optimized Link Source Routing (OLSR) is an example of the same [3]. The proactive protocol suffers from excessive delays in case of any distortion in the network as they do not opt to research the routing path. This issue is resolved to an extent in reactive protocol architecture where the nodes are able to find different routes when they feel any distortion in the existing route frame. Ad-hoc On-Demand Routing protocol (AODV) is an example of a reactive routing protocol set. Researchers use the wireless ad-hoc network to handle high mobility nodes. The routing protocol has been proposed to direct the packets from source to destination. The different parameters such as PDR, delay and hop count has been considered to determine the efficiency. But, the paper still inefficient to attain the required results [4]. AODV has been widely used in past studies to manage attacks in the network. AODV protocol has been used to evaluate the results due to its unique architecture and robust structure. Both the architectures, reactive and proactive suffers from network intrusion issues as due to the mobile nature, nodes from another region may also enter into the defined region and they cannot be stopped from entering into any zone [5].The detection of intrusions in MANET is a challenging task. There may be many reasons for that like change in network topology, packet dropping, and noisy environment. It is difficult to present a cooperative system, where intruders do not harm the network. The accurate detection of conventional attacks and its specification depends upon the intruder attacking strength. The nodes enter into the region of the different network for various purpose. If that reason is to harm the network, then it must be a serious concern, which needs to be taken under proper attention. As shown in Figure 1, node n has initial coordinates (x, y) and it falls under region 1 as per the region boundary. After a certain time interval, it crosses its boundary and reaches to a point(x2, y2) which is outside of its original region. This situation may occur by mistake or intentionally. If it is by mistake, a network is safe but if it is done intentionally then the node n may cause harm into the network. In such a manner, the paper defines the network and its mobility through definition 1.

**Manuscript published on 30 September 2019.**
***Correspondence Author(s)**
**Pooja Rani,** PhD. Scholar, Computer Science Engineering , Lovely Professional University, Jalandhar, India .
**Tanupreet Singh,** Professor and Head, Amritsar Engineering collage, Amritsar, India

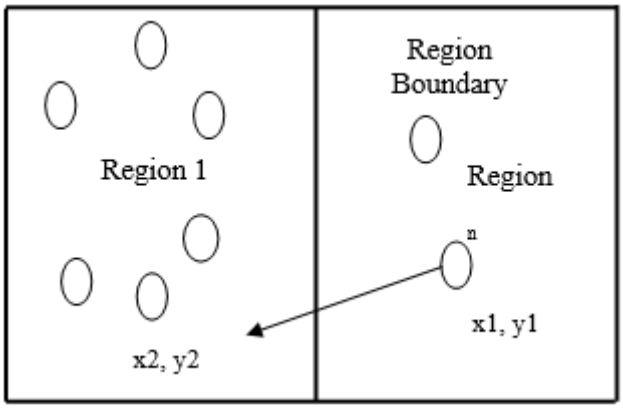


**Fig.1 Node regions and movement**

**Definition 1**: A mobile network MN (n, $n_{loc}$,esds, na) is made up of n number of mobile nodes with initial associated x and y locations defined in $n_{loc}$ . The estimated displacement of every node is defined through esds and the network administration is defined as na.

**Issue 1**: Each region in MN has its own na and when a node moves from one region to another, why the na of the second region would consider that node into its region.

This paper takes this issue very seriously and implements an interpolation method for such a situation. This situation also creates intra intrusion architecture. The intrusion or attack falls under two categories namely normal and smart. This paper addresses the issue of solving smart attackers as it takes a lot of manual effort to identify a smart attacker. Tracking a smart attacker not only requires a lot of physical resources but it also consumes a lot of power. This paper issues two different attacks in the proposed architecture namely Black Hole attack (BHA) and Selective Packet Drop attack (SPDA). There is already enough research in the literature regarding the black hole attack using different techniques [6]. But, due to rapid growth in technology, still, novel techniques are essential to mitigate the effects of the black hole attack. An authentic Optimal Behavioural Bee (OBB) algorithm has been designed with Artificial Neural Network (ABC) optimization algorithm. The process of monitoring is executed by following the OBB bees. Support Vector Machine (SVM) is used as a machine learning technique for the purpose of classification. QoS measures, such as, Throughput and Packet Delivery Ratio (PDR) are computed and the comparative analysis has been conducted to depict the efficacy of the presented work.

The rest of the paper is organized in the following manner. Section II presents the proposed work architecture and Section III evaluates the results for the same. Section IV concludes the paper

## II. Related Work

MANET is a network of nodes connected without any infrastructure. Nodes acting as a router and host which forwards the information from one node to other nodes. The topologies of the network changes due to the high mobility of nodes. Thus, a unicast routing protocol has been developed for the MANETS using proactive routing algorithm [7]. The main drawback of the developed approach is that it becomes inefficient to determine the throughput for a large number of simulations. Moreover, this approach does not manage the packet dropping issue. So, the homomorphism based approach has been used in the literature to detect the malicious attack. In addition, the distance vector has been used to determine the distance between the nodes and preventing the packet dropping [8]. The security is the other important aspect requires equal concern to enhance the performance. S. N. Mohammad et. alhas used the Micr technique to enhance the security level [9]. The network has been secured from the black hole attack using a key distribution system, which provides improved security level to the MANET. But, the distribution of secret key consumes large energy of the network which hampers the performance of the network. In addition, the fake concept has been introduced to confuse the attackers which helps in reducing the packet loss. But, the main drawback of the paper is that fake messages increases the energy consumption and performance reduces as security also compromised due to intruders attack [10]. Therefore, fuzzy-based approach has been developed to enhance the security level. The network performance varies depends upon the packet distribution between the nodes. The AODV protocol has been used to compare the results. But, the packet delivery ratio still not attainable and simulation time is more which limits the developed approach of the paper. The anonymity concept has been used to schedule the packets. Therefore, a scheduling algorithm has been presented in past studies to analyze the traffic. The fake source localization algorithm has been proposed to enhance the detection rate. The optimum routes have been detected by scheduling the packets using the developed algorithm. The fake packets have been used to confuse the intruder and fake paths have been constructed. In addition, packets have been transmitted from original paths. The fake paths intend the intruder to use this path and fake messages increases which results into an increase in energy consumption. The increase in consumption results in reducing the performance of the network. The energy consumption is an important parameter recognized by the authors in MANET. The trust-based mechanism secures the network and increases the efficiency of the network. Thus, the trust-based algorithm has been presented in past studies to detect the black hole attack. The optimization algorithm Artificial Bee Colony (ABC) has been used to enhance the results but still, this approach lacks the classification algorithm. The fitness function used in the optimization algorithms generate new solutions but the classification of these solutions becomes hard [11]. But, the fuzzy-based systems provide secure multicast routing using the authentication scheme. The active and passive attacks have been mitigated by understanding the nature of misbehaving nodes. The un-certification routing proposed in the past proves better authenticity and reduced energy consumption. The encryption technique used in this paper still requires modification as the complexity of data is more, which reduces the performance of the network [12]. The developed approach protects the network using the pseudorandom function to authenticate the system, which makes the system complex. Thus, a reactive approach has been used to prevent malicious attacks. The framework based on intrusion detection in a MANET. The developed approach does not attain the throughput and delay as per requirement. This paper lacks the optimization technique which may enhance the detection rate [13].

*Retrieval Number: K21450981119/19©BEIESP*
*DOI: 10.35940/ijitee.K2145.0981119*
*Journal Website: www.ijitee.org*



*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

Researchers propose the lifetime enhancement techniques using the LEACH protocol to improve the performance of the network. The more emphasis given on increasing the lifetime and consuming the less energy. The proposed work in this paper has been compared in the results section. This paper still insufficient to save the energy as the energy dissipates more when the data transmission taken place from source to destination nodes [14]. Therefore, scholars attempted to enhance the longevity of the battery using the metaheuristic approaches such Ant Colony Optimization (ACO) so that shortest path detected from source to destination. This helps to save the energy as concept of watchdog and digital signatures has been incorporated to avoid the black hole attack. The simulation results stated that the proposed work consumes the less energy and efficient than the AODV protocol. But, the main limitation of the paper is that routing detection increases the load as the number of attackers detected on that path is maximum. Thus, results of this paper has been discussed in the results to determine the performance of the proposed work [15].

### A. Problem Formulation

The main problem in the past studies is the intruder attack, which increases the packet loss problem and reduces the efficiency of the network. Researchers and practitioners proposed approaches in the literature lacks to achieve the satisfactory performance of the network. The packet loss still needs improvement to detect the intruders by developing a robust algorithm. In addition, it is seen that previous studies do not utilize the classification approach and optimization algorithm. Thus, an effort has been made to revamp the performance of the network by reducing the effect of intruders.

## III. PROPOSED WORK

The proposed work model is designed in frames. The first frame aims to deploy the network and to model it. The next frame shows the significance of the intrusions. This frame also contains the application of the prevention framework which is a hybridization of swarm intelligence and machine learning. The third frame is for the deployment of an interpolation method for a new node registration in the region. Figure 2 shows the flowchart of the proposed work. The different sections have been interconnected to obtain valid results. The sections in the developed flowchart have been explained in the entire paper.

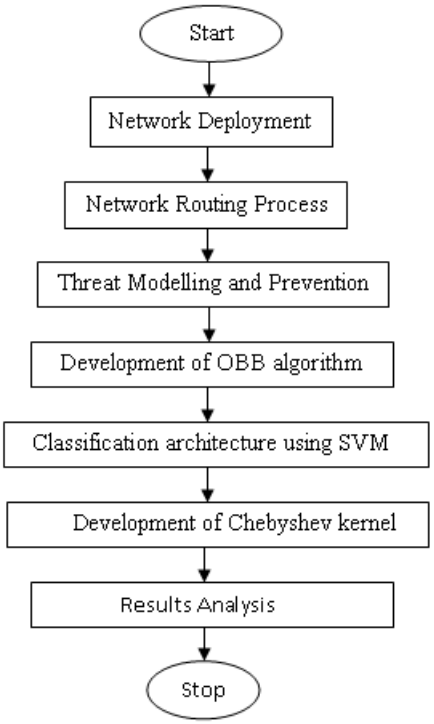


Fig.2 Flowchart of the proposed approach

### A. Network Deployment

Following ordinal measures are set for the network deployment.

Table 1. Ordinal Measures

| | |
|---|---|
| Node Range | 50-100 |
| Area of Communication | 1000 × 1000 m |
| Coverage Range | 25% of the existing location as per IEEE 802.11 |
| Model Type | Heterogeneous |

**Pseudo Code: Model Setup and Deployment**

$Model_{Height} = 1000$

$Model_{Length} = 1000$

$For\ each mobile\ node\ in the model$

$Initialize x and y location sof mobile nodes$

$Initial_{Bandwidth} = Associated_{Bandwidth}$

$Delay(In_{transmission}) = New(Delay_{Transmission})$

$Packet_{Dump} = Initialize$

$Deploy\ (Mobile\ node)$

$EndFor$

The proposed work model has considered a heterogeneous environment and different node properties and nodes are deployed with different values of similar attributes. As for example node, n1 will have 70% associated energy at the start whereas, in the same simulation, n2 will have 65% associated energy. Every network dumps some packets even if it is error or intrusion free.



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The proposed work model considers two situations of modeling namely dump under the normal situation and dump under distortion mode. Obviously, a node will dump more packets under distortion but what would be the drop count is unknown and hence the architecture has set a random behavior for the packet dumps and drops. The algorithm "Calculate Coverage" computes the communication range of the nodes.

**Algorithm 1: CalculateCoverage ()**

$Input: NodeList$

$Coverage = []$

$For_{every} node in Nodes$

$For_{every} node1 \; in Nodes$

$If node != node1$

$$dist = [sqrt((X_{loc}(node) - X_{loc}(node1))]^2 + (Y_{loc}(node) - Y_{loc}(node1))^2)$$

$$Coverage\ (node, node1) = Node(id_{list})\ (node1)$$

$End\ for$

$End\ for$

$End\ Algorithm$

The calculate coverage calculates the distance of one node (X1 to X2) to the second node by using the distance formula. If the node is covered in the distance region defined by 802.11, then it can be utilized for the communication with another node. The coverage of nodes has been initialized using the empty parenthesis. The nodes have been firstly initialized in node 1 as described in the designed algorithm. Figure 3 depicts the communication process and architectural result of Algorithm 1.The route discovery process after coverage evaluation is as follows:

**Algorithm 2: TheRoute definition (n, Coverage)**

$Input: Source, Destination$

$Output: Route$

$Route(1) = Source$

$Temp_{Source} = Source;$

$Source\_Coverage = Coverage(Temp_{Source});$

$Find(Source_{Coverage}, Destination)$

$IfFound, AddDestinationtoPath$

$Else$

$Temp_{Source} = Source\_Coverage.Nearest_{Node}$

$AddTemp_{Source} toRoute$

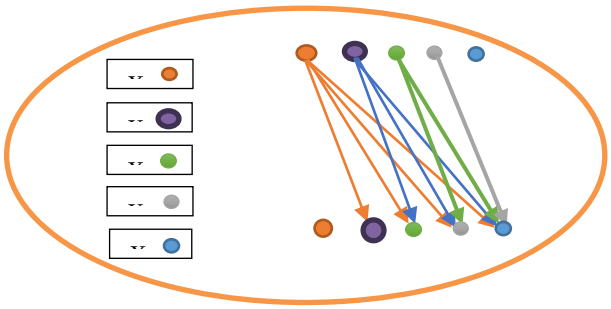

**Fig.3 Coverage Evaluation**

Algorithm 2 takes the source and destination node as input and extracts the nodes which are there in the coverage limit of the source node. The destination is searched in the coverage limit if a destination is found directly, no further routing is required and data transfer takes place. In other situation, the nearest node in the source's coverage list acts as the temporary source and the process keeps on repeating until the destination is not found. Once the route discovery process ends, the data transfer takes place and threat modeling and prevention comes into act.

### B. The Threat Modelling and Prevention

When the data transfer is initialized, the network may suffer intra or inter security threat [11]. The proposed model has considered two different attacks namely black hole and SDN. When the network will fall under intrusion, it will start showing its effect. Here the prevention architecture uses a dual identification and prevention mechanism. The proposed architecture understands the importance of nodes and hence directly the node is not pointed out as an intruder. The first phase is to identify the affected route of the entire simulation. To identify the affected route, the proposed solution designs a new Optimal Behavioural Bee (OBB) algorithm inspired by the Artificial Bee Colony (ABC) algorithm. There are many advantages of the OBB as the energy consumption reduces, better optimization, and delay also reduces. In addition, the proposed algorithm also reduces the delay introduced in packet delivery system and increases the throughput rate.

There are three types of bees in OBB. OBB has acting bee (AB), monitoring bee (MB) and Group-Head Bee (GHB). The functioning of all these bees different from one and other. There is one last bee that is termed as Queen Bee (QB). The monitoring process took place through these Bees. The MB monitors the food undertaken by AB with changes in the traveling time. When an AB brings food to MB, MB allows the AB to go for food search for the second time and deposits the food. The two-step collection is verified by GHB. If the food quality is verified by GHB, the food is preserved and MB is awarded rest and on the next phase of the food search, the awarded AB goes first for the food search.

*Algorithm 3: OptimalBeeBehaviour*

$Input: Simulation_{Routes},$

$Energy\_Consumption\_Route$

$Bee_{FoodDeposits} = Energy_{ConsumptionRoute} ForeveryRouteinSimulation_{Route}$

$OBB_{Population} = Bee_{FoodDeposit}.Element_{Count};$

$ForeveryBeeinOBB_{Population} Acting_{Bee} = OBB.Population.Bee$

$Forthenexttwobees, BeeFoodispreserved.$

$GHB.Threshold = Mean(Acting.Bees); Traveltime = RandomTravelTime.$

$IfGHB.threhold.travel_{time} > Acting_{Bee} Preserve_{Route} ElseSuspectRoute ++$

$AppendRoutevaluetoSuspected_{Route};$

The output of OBB provides the faulty routes which are further supplied to machine learning based Support Vector Machine. It is a classification technique, which classifies the data based on its nature. The SVM architecture takes two parameters as input. The first parameter is bandwidth consumption of every node in the affected node and the second parameter is the packet dump of the suspected nodes. The network preserves the packet dump by every node and by every route. The SVM outputs have been depicted in Fig. 4.

*Retrieval Number: K21450981119/19©BEIESP*
*DOI: 10.35940/ijitee.K2145.0981119*
*Journal Website: www.ijitee.org*



*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

The maximum misclassified node is termed as a final culprit in this case. The following parameters are evaluated for the process of comparison of the proposed framework.

The third part is the identification of a new node in a region through the Chebyshev method.The Chebyshev Polynomials (of the first kind) are defined as [16].

$$Z_m(y) = Cos[m \arccos(y)] \quad (1)$$

The Chebyshev polynomial has weight so that its nature is orthogonal is detected $v(y) = (1-y^2)^{-1/2}$ having an interval from $(-1\ to 1)$. The variables have been used to detect a new node to enter into a region. The interpolation order is used to determine the detection rate. On the other hand, variables such as $(s,t)$ than interval can be handled by modifying the variables such as $y \to \frac{1}{2}[(t-s)y + s + t]$. The information is not clear from definition 1 but still $Z_m$is a polynomial having degree m.

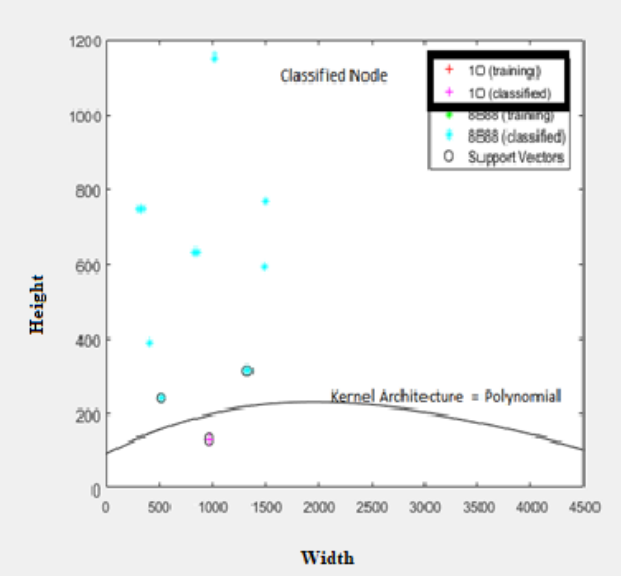


**Fig.4 Classification Architecture**

For the 1st node or order, the node representation in the polynomial form to register a node is:

$$Z_0(y) = Cos(0) = 1 \quad (2)$$

Similarly, for 2nd node registration, the obtained equation is

$$Z_1(y) = Cos(\arccos(1)) = y \quad (3)$$

***Algorithm 4: Chebyshev Polynomial***

Order=2; // Interpolation order
$My_{VALUE} = [\ ]$ // Initializing the key values to be Empty
For i = 1:3 // For 3 vehicles
counter = 1;
$Current_1$=$Node_{ID_I}$ // Taking the first node as initial reference
For j=1: Vehicles;
Current=$Vehicles_j$; // For each interpolation, there would be 2 Rest Nodes
If Current1~=Current // If nodes are not the same
Rest (counter) =current;
Counter=counter+1;
End If
End For
Calculate Cheb
$Shared_{key} = Share_{Current_1} \times My_{value}[i]$
End For

If the shares result into network key then the node is allowed to be a part of network else it is thrown out.

## IV. RESULTS AND DISCUSSION

This section discusses the result section in which throughput and PDR have been used to analyze the result. The experimental results based on a number of simulations have been presented in this section. The Chebyshev kernel using linear and polynomial kernel has been measured for PDR and throughput. In addition, it is essential to understand the comparative analysis and result in analysis of the literature studies using PDR and throughput parameters.

### A. Analysis of the proposed work

The proposed work describes the effectiveness of the developed technique. The following parameters are evaluated. The linear and polynomial kernel has been used to evaluate the results. The evaluation structure taken is before and after the attack. The evaluation is done by keeping the following constraints.

a) Delay

The end to end delay has been considered in the present research which is the ratio of total delayed packets as received by the destination to the packet count received by the destination. In other words, the mathematical representation of the incorporated delay given as:-

$$Delay = \frac{Total\ delayed\ packets\ received\ at\ the\ destination}{Number\ of\ packets\ received\ \ at\ the\ destination}$$

Table 2. End to end delay

| Number of nodes | Delay of Proposed work in seconds | Delay attained by Past Studies in seconds [11] | Delay introduced by [14] |
|---|---|---|---|
| 20 | 9 | 28 | 10.01 |
| 40 | 10 | 32 | 11.11 |
| 60 | 10.22 | 38 | 13.43 |
| 80 | 14 | 44 | 14.55 |
| 100 | 14.33 | 48 | 15.03 |

The comparison to end to end delayed packets given in table 2.The given table vivid that the introduced delay has been reduced for different sensor nodes.


Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The delay has been increased from 9 to 14.33 for 20 to 100 nodes. However, the introduced delay of the proposed method is less than the conventional approaches.

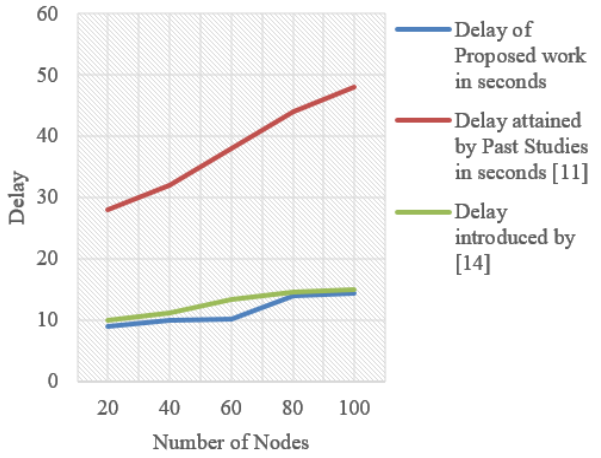


**Fig.5 End to end Delay computation**

The given figure clears that the proposed work introduces less delay than the past techniques. The delay has been increased as the sensor nodes incremented by 20. The average value of the delay for the proposed work is 11.51 and that of conventional approach, it is 38 for [11] and 12.82 for [15]. Thus, delay has been improved by $\frac{38-11.51}{38} \times 100 = 69\%$ for the proposed work in contrary to conventional technique [11] and 10% for [14].

b) Energy Consumption

Energy consumed by the nodes when the packets received from the neighbouring nodes and transmission of packets to the corresponding nodes. When the nodes consume less energy then the performance of the network increases.

It is clearly seen in the given figure that the proposed work consumes less energy consumption in comparison to [15]. The average energy consumed by the proposed work is 626250 and that of conventional technique, it is 713750. Thus, overall energy consumed by the proposed work improved by $\frac{713750-626250}{713750} \times 100 = 12\%.$

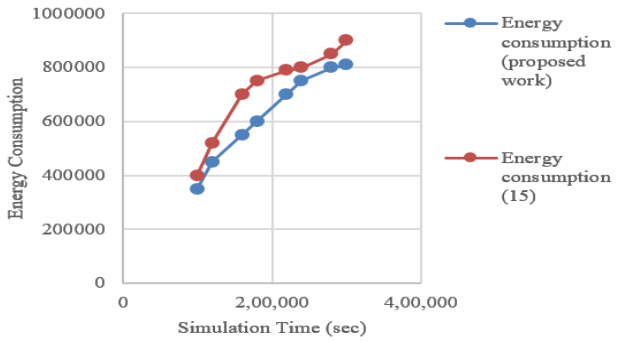


Fig.6 Energy Consumption

c) Throughput

It is defined as the ratio of total packets delivered to the destination per time frame. The total delivery of packets denoted by $T_{Pd}$, throughput is denoted by T, and time frame denoted as t.

$$T = \frac{T_{Pd}}{t} \qquad (4)$$

Table 3. Throughput

| Total No. of Simulations | Throughput with attack | Throughput with linear kernel | Throughput with polynomial kernel |
|---|---|---|---|
| 100 | 10000 | 20000 | 20000 |
| 200 | 20000 | 40000 | 40000 |
| 300 | 40000 | 60000 | 60000 |
| 400 | 57000 | 76000 | 77000 |
| 500 | 59000 | 81000 | 85220 |

Table 3 depicts the throughput of the proposed approach using linear and polynomial kernel. In the proposed approach, we are experimented the results using 500 simulations which are repeated to calculate the throughput value of the proposed approach. The results attained using the polynomial kernel has been better than the linear kernel. The maximum attained throughput of the proposed approach with linear kernel is 55400 and that of polynomial kernel, it is 56444. On the other hand, throughput without prevention is 37200. The results vivid that the throughput rate using polynomial kernel better than the linear kernel and without prevention system.

Fig.7 depicts the throughput of the proposed algorithm, which is tested with both polynomial and linear kernel. The performance of the proposed algorithm is obviously better than the values with the attack but going deeper, it is evaluated that the polynomial kernel acts a little better than that of the linear kernel.The average throughput rate obtained using the polynomial kernel is 56444 whereas for linear kernel, it is 55400. Thus, system throughput rate has been improved with the polynomial kernel for 500 simulation rounds is $\frac{56444-55400}{56444} * 100 = 1.8\,\%$. Under the effect of intrusion, the performance of the network is very low.

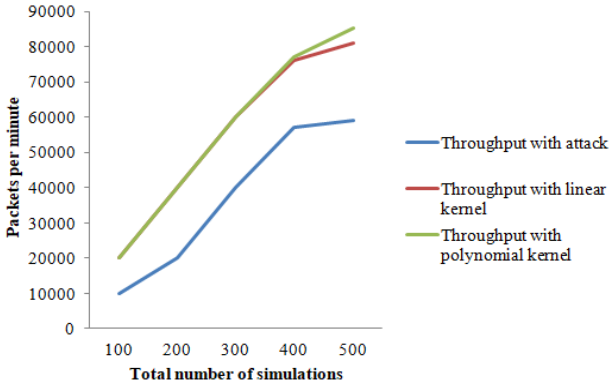


**Fig.7 Throughput Evaluation**

For the same simulation architecture set, the model only shows 37200 units of packets transfer per minute. The throughput under intrusion is low because the packet dump is high. High packet dump results into low PDR values and high bandwidth consumption.

d) Packet Delivery Ratio (PDR)

It is defined as the ratio of the total received Packets to the total number of transmitted Packets. In other words, Total received packets denoted by $T_{received}$ and transmitted packets denoted by $T_{transmitted}$.

$$PDR = \frac{T_{received}}{T_{transmitted}} \quad (5)$$

Kernel Types → Linear and Polynomial
Evaluation Structure → Before and After Attack

**Table 4. PDR**

| Total Number of Simulations | PDR under threat | PDR after prevention for linear Kernel | PDR after prevention for polynomial Kernel |
|---|---|---|---|
| 100 | 0.22 | 0.5 | 0.92 |
| 200 | 0.25 | 0.59 | 0.93 |
| 300 | 0.29 | 0.62 | 0.94 |
| 400 | 0.32 | 0.68 | 0.96 |
| 500 | 0.35 | 0.79 | 0.98 |

Table 4. depicts the PDR of the proposed approach using linear and polynomial kernel. In the proposed approach, 500 simulations have been experimented, which are further repeated to validate the results.

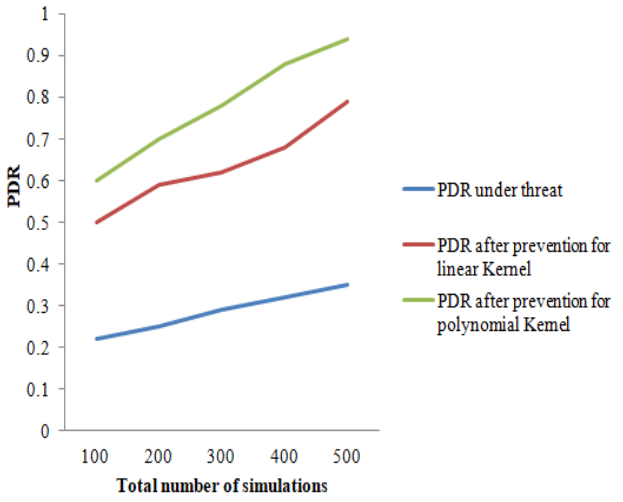


**Fig.8 .PDR Evaluation**

Fig.8 depicts the PDR of the proposed approach tested using linear and polynomial kernel. It is seen that the average value of PDR under threat approximates to 0.28. It lies in the range of 0.2 to 0.36, which is very low. The PDR after prevention with classifier SVM for linear kernel lies in the range of 0.5 to 0.8 is 0.636 for 100 to 500 simulations. However, in case of polynomial kernel, the average value is 0.94. This simply indicates that PDR for polynomial kernel improves after incorporating the prevention structure. Similarly, PDR using SVM prevention architecture for polynomial kernel lies in the range 0.6 to 0.94 for conducting an experiment from 100 to 500 simulations

## B. Comparative analysis of the proposed approach with conventional techniques

The packet scheduling algorithm developed in the past studies uses inter and intra approach to attain maximum PDR. The Anonymity based approach analyses the traffic by determining the fake paths. The maximum attained PDR is 0.9, which is less from the developed algorithm. The anonymity approach confuses the intruders by developing the fake paths so that intruders are confused. Table 4 compares the results of the proposed approach and literature studies.

**Table 5. Comparison of PDR of the proposed approach and past studies**

| Techniques | PDR |
|---|---|
| Proposed approach (OBB) | 0.94 |
| Path Observation based Physical routing protocol [4] | 0.9 |
| Security-Aware Packet Scheduling Algorithm [10] | 0.91 |
| Hybrid Trust based Weighted Algorithm [11] | 0.89 |
| Fuzzy approach [12] | 0.92 |

Table 5. depicts the comparison of the proposed approach with the previously studied techniques. It is clearly seen in the given table that the attained PDR value of the proposed approach is 0.94, while other techniques have PDR value less than the obtained value.

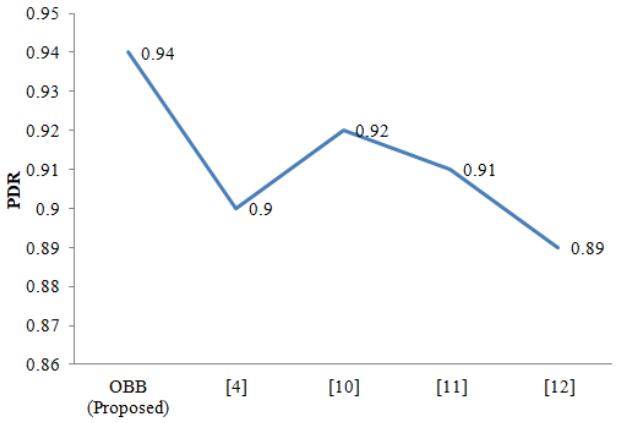


**Fig.9 Comparison of PDR with previous techniques**

Fig.9 depicts the graph of the proposed approach and the previous techniques viz. [4], [10], [11] and [12]. It is seen that the average value of PDR is 0.94, which is of the proposed approach. While contrast of proposed work with the [4], 4.2% improvement has been noticed in proposed work, 2.1%effectiveness has been noticed in proposed work while comparing it with [10], 3.1% efficacy has been drawn of proposed mechanism while comparing it with [11] and 5.31% efficiency has been addressed while comparing the proposed work with [12].



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Consequently, the designed approach proves better and improved results than the conventional techniques.

## V. CONCLUSION

This paper presents the threat and prevention architecture for safe packet transmission in MANET. The heterogeneous environment has been considered to avoid the attack from a malicious node. The architecture detects the malicious node by registering new nodes using the swarm intelligence based algorithm. The OBB algorithm detects the faulty nodes which are taken as input to SVM. The machine learning-based optimization determines the bandwidth consumption rate of the node and packet dumped by the affected nodes. In addition, an algorithm based on Chebyshev polynomial registers the new node. The results have been evaluated by determining the throughput rate, which is further tested using the constraints kernel. The detected improvement rate through polynomial kernel is 2.2%. In addition, PDR has been measured under three different conditions such as under threat, prevention using SVM linear and polynomial kernel.

The prominent results have been obtained which shows that polynomial kernel results such as PDR are better among three of them. Fruitfulness has been seen when the comparison has been addressed with the conventional methods for PDR comparison and around 4.2% of improvement has been noticed.

## REFERENCES


1. X. Wang, and X. Zhu, "Anycast-based content-centric MANET", IEEE Systems Journal, Vol. 12, No. 2, pp.1679-1687, 2018.
2. R. Alubady, M. Al-Samman, A. Habbal, S. Hassan, and S. Arif, "Performance analysis of reactive and proactive routing protocols in MANET", Journal of Engineering and Applied Science, Vol. 10, No. 3, pp.1468-1478, 2015.
3. S.R.Azzuhri, H. Ahmad, M. Portmann, I.Ahmedy, and R. Pathak,"An efficient hybrid MANET-DTN routing scheme for OLSR", Wireless Personal Communications, Vol. 89, No. 4, pp.1335-1354, 2016.
4. M. Rajesh and J. M. Gnanasekar, "Path observation-based physical routing protocol for wireless ad hoc networks", International Journal of Wireless and Mobile Computing, Vol. 11, No. 3, pp.244-257, 2016.
5. P. Gupta, P. Goel, P. Varshney and N. Tyagi,"Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET",In Smart Innovations in Communication and Computational Sciences, Springer, Singapore, pp. 271-279, 2019.
6. A.K. Jain, V. Tokekar, and S. Shrivastava,"Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks", In Information and Communication Technology, Springer, Singapore, pp. 39-47, 2018.
7. D.Tepsic, M. Veinovic, D. Zivkovic, and N. Ilic, "A Novel Proactive Routing Protocol in Mobile Ad Hoc Networks", Ad-hoc& Sensor Wireless Networks, Vol. 27, 2015.
8. K.Vanitha, andA.Z.Rahaman,"Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol", Cluster Computing, pp.1-9, 2018.
9. S.N. Mohammad, R.P.Singh, A.DeyandS.J. Ahmad, "ESMBCRT: Enhance Security to MANETs Against Black Hole Attack Using MCR Technique", In Innovations in Electronics and Communication Engineering, Springer, Singapore, pp. 319-326, 2019.
10. R.Nandakumar, and K. Nirmala, "Anonymity-based intra–inter and multiple layer service dependent security-aware packet scheduling algorithm (AIIMLSDSPS)", International Journal of Computers and Applications, pp.1-9, 2018.
11. V.Keerthika, and N.Malarvizhi, "Mitigate Black Hole Attack Using Hybrid Bee Optimized Weighted Trust with 2-Opt AODV in MANET", Wireless Personal Communications, pp.1-12,2019.
12. V. Brindha, T. Karthikeyan, and P. Manimegalai, "Fuzzy enhanced secure multicast routing for improving authentication in MANET", Cluster Computing, pp.1-9. 2018.
13. M. Rath, and B.K. Pattanayak, "Prevention of Replay Attack Using Intrusion Detection System Framework", In Progress in Advanced Computing and Intelligent Engineering, Springer, Singapore, pp. 349-357, 2019.
14. A.Y. Prasad and R. Balakrishna,"Implementation of optimal solution for network lifetime and energy consumption metrics using improved energy efficient LEACH protocol in MANET", Telkomnika,Vol. 17, No. 4, pp.1758-1766, 2019.
15. N. Panda and B. K. Pattanayak, "Energy aware detection and prevention of black hole attack in MANET", International Journal of Engineering and Technology (UAE), Vol. 7, No. 2.6, pp.135-140, 2018.
16. R. Kumar, and R. Singh, "Key management using Chebyshev polynomials for mobile ad hoc networks", China Communications, Vol. 14, No. 11, pp.237-246, 2017.


## AUTHOR PROFILE:

**Pooja Rani** is persuing its PHD from LPU.She has completed his M.Tech from GNDU Amritsar and having 12 yerrs of teaching Experience.

**Dr. Tanupreet Singh** working As Professor in Amritsar College of Engineering.He is a member of ISTE and CSI. He having a teaching Experince of 16 years.