PDA: Proactive Defense Approach for Black-Hole and DOS Attack Free Optimal Routing In Mobile Ad-Hoc Networks

kondeboina Srinivasa Kumar, M. Akkalakshmi

Abstract: ***The scope of the intrusions in mobile ad hoc networks is considerably proportionate to the growth of the mobile ad hoc network scope in the use of technology in general strategic facilities of the human life. The intruders intended to downgrade the performance scope of the target network often performs black hole attacks. The other frequent method of intrusion in ad hoc networks is denial of service, which is often evincing through the gray hole and warm hole attacks. The nodes compromised to perform these attacks are insensitive to identify. This manuscript contributed a novel evolutionary approach to establish an optimal route between source and target nodes that eliminates the scope of the nodes compromised to denial of service attacks through performing black hole, gray-hole and warm-hole activities. The performance of the contribution is scaled by comparing the experimental results of the proposal with other contemporary models.***

Keywords: wireless networks, Intrusion detection system, Mobile ad hoc network, RDIDS-WMAN, Fine Grain Analysis.

I. INTRODUCTION

The work [1] presents that the "wireless networks (WNs)" has vigorous nature because of which creates groups with the adjacent neighbor nodes. Any group of actions which try to compromise confidentiality, accessibility or integrity of resource is called intrusion. The "IDS (Intrusion detection system)" assists us to detect the malevolent activity conduct in "ad-hoc network". The IDS is largely categorized into 2 methods: IDS based on Anomaly & IDS based on Signature. The IDS which is based on signature utilizes attacks signatures for identifying intrusion, however, the IDS method which is based on Anomaly assists us to defend the destination networks & machine in averse to malevolent conduct. The "ad hoc network routing protocol" function is to create exact & effective route among neighbors such that messages might be forwarded within the time period [2]. Outdated way of protecting the network through firewalls & encoded models is not adequate. Hence, we suggested "Robot intrusion detection system" that might offer finest solution for "Mobile ad hoc network (MANET)" since its applications were directly associated to airports, military etc., Several researchers are contributing on "ad-hoc network" to offer finest solutions aimed at security, however we have to still effort on it.

Revised Manuscript Received on April 06, 2019.

Kondeboina Srinivasa Kumar, Research scholar, Rayalaseema University, Kurnool, India.

Dr. M. Akkalakshmi, Professor, GITAM University- Hyderabad, India.

And this article is structured in the following way: Segment-1 explores regarding MANET introduction, Segment-2 explores regarding review of literature of diverse researchers through the solutions,Segment-3 have entire design of the "RDIDS-WMAN", Segment-4 explores regarding the empirical outcomes and lastly Segment-5 is regarding conclusion.

II. RELATED WORK

There were several contemporary strategies that have been suggested by several researchers aimed at dealing through "selective packet dropping attack". The work [3] suggested a method which can identify the cooperative malevolent nodes chain that executes selective drop of packet in network. The confine of this method is having a maximum routing overhead because of several additional control packets & could not done the evaluation of the performance of suggested method.

The work [4] contributes special nodes known as the "IDS nodes" which are arranged in network that has capability to eavesdrop its neighboring transmission. And in this method, only target nodes are enabled to forward reply packet (RP) by receiving packet request & intermediate-nodes were prohibited to forward RP.

Even though this method is capable of identifying "black hole attack" and "gray hole attack which is based on sequence number" in network, however, it is unsuccessful in instance of "smart gray hole attack". The "smart gray hole node" performs exactly in discovering the route and also sends the RP because of which it will be not able to identify and therefore is the confine of this method.

The work [5] suggested a novel technique for justifying the "gray hole node" impacts through utilizing special nodes that is IDS in network. The confine of this method is that malevolent nodes will conduct normally after obtaining "query packet" and will send the "data packets" because of which IDS is not capable to identify it.

The method relied on the threshold of sequence number is suggested in [6] which execute mitigation of "gray hole attack" in this method, they have launched 3 diverse kinds of "gray hole" by utilizing false information of routing" that attracts congestion towards them and executes "selective packet drop in network".

The confine of this method is that will not mitigate "smart gray hole attack" that performs sincerely in network at the time of discovering the route procedure and forwards exact information in RP received either from target or any of the intermediate-node.

The work [7] presents a novel distributed & cooperative technique that contains of 4 security segments aimed at dealing with "gray hole attack". They have launched "simple gray hole" by utilizing inexact reply of route yet the "smart gray hole node" will not forward inexact reply of route and conducts normally at the time of discovery of route and "selective data packet dropping". Therefore, the strategy which is based in DRI also unsuccessful under "smart gray hole attack".

Many of the contemporary contributions deals with "mitigation of sequence number-based gray-hole attack" where the node provides inexact reply of route in esteem to attract congestion and "selective data packet dropping". And there will be no "smart gray hole attack" evaluation in diverse time intervals with esteem to mobility of node in the literature.

The confines of contemporary strategies motivated us for proposing novel technique that will deal through "smart gray hole attack" in "ad hoc network". And in this article, the concentration is on 2nd kind of above mentioned "gray hole attack" that is "smart gray hole attack" where the malevolent node performs normally at the time of discovery of route, executes "selective dropping of data packets" for some time and then alters its conduct into general state.

The "Fine Grain Analysis (FGA)" model is to assess rigorously the main reason for the loss of packet before announcing it as attack [8]. The "online algorithm" is to identify "gray hole attacks" utilizing the inherit information of time in the "PMU data packet" [9].

The techniques have been proposed for augmenting particular routing protocols such as [10], [11]. The model in [11] is to evade the "gray hole attacks" in "optimized link state routing (OLSR)" protocol has been proposed. As per paper, each node in network confirms its neighbors through specified rules set and upon inconsistency; then the node is evaded by neighbors. The novel parameter [10] called intensity of black-hole is determined in the article that quantifies the association among "sequence numbers of routing packet" in "ad hoc on-demand distance vector (AODV) routing protocol" and "black hole attack". The work [12] presents that the "extended data routing information (EDRI)" table will be added to the protocols for identifying and eradicating the "black hole attack". Many of the contemporary works concentrate on identification & detection of "black hole attack". And some these results to wrong alarms that lead to resources loss in the MANET. Therefore, we proposed the strategy for detecting and approving "black hole attack" in the MANET utilizing "Black-hole Attack Confirmation System".

In regard to deal the constraints stated from the contemporary methods of the recent literature, Chowdary A et al.,[13] portrayed a soft computing based intrusion detection method for mobile ad hoc network, Though the method evincing the extreme performance as reactive method, the process complexity of the "adaptive neuro fuzzy inference system (ANFIS) that used in the proposal is not fit to the mobile ad hoc network due to their constraints like infrastructure less, limited energy sources of the nodes, and the mobility. The mobility of the nodes is a critical constraint that downgrade the performance of the reactive methods.

III. METHODS AND MATERIALS

The methods and materials used in the prosed Proactive Defence Approach that optimizes the route discovery by avoiding the nodes compromised to black-hole and dos attacks is explored in this section. The proposal is an evolutionary approach that built by using the method called differential evolution, which intends to determine the best fit from the routes discovered during the route request process. The metrics RCRP [14] and RTFE [15] defined in our earlier contributions were used as fitness function of the differential evolution.

A. Model Definition

The routes discovered during the process of route request are considered as input to the deterministic evolution technique called differential evolution. Each pair of routes from this set of initial routes will be used as inputs to perform mutation on crossover (one or more nodes in sequence of the both input routes) of the input routes. The routes given as input and the routes newly framed are further filtered, such that the routes having degree of reputation greater than the given threshold (often it can be zero) and sorts the resultant routes in descending order of their relay transmission fitness and selects first two routes in the ordered list of resultant routes of the mutation process.

B. Proactive Defence Approach

The routes that are possible between given source and destination nodes are being portrayed by the bench mark method called reputation cognizant routing protocol (RCRP) [14] that focuses on the selection of all initial routes that are framed by the nodes having reputation, which is being assessed using varied metrics.

The Relay Transmission Fitness is a crucial metric devised in our earlier contribution [15] that enables to identify the routes having considerable reputation under RCRP protocol, but compromised in recent past. The method of route selection under relay transmission fitness that portrayed in our earlier contribution "Optimizing Reputation based Route Discovery by Relay Transmission Fitness Evaluation (RTFE)" [15], which is an extension to the RCRP protocol.

The method RTFE is an effective approach to select the route that is built by using the nodes having high degree of reputation and relay transmission fitness. The RTFE selects best among the initial routes discovered from route request process. However, the initial routes are not only possible routes which since many of routes would fail to be noticed during the route request process. Hence, the optimal route that recommended by the RTFE is often may not be the best. In regard to this constraint of our earlier contributions, the contribution of this manuscript adapted an evolutionary approach called Differential Evolution approach that determines the all possible best fit routes from the given initial routes. The fitness function of the Differential Evolution Approach is framed by using the Relay Transmission Fitness Metric.

a) Node Level Relay Transmission Fitness

Let the all possible nodes as unique set N, which are involved in one or more routes discovered during route request process under RCRP and portrayed as set R.

In regard to each node $\{n \exists n \in N\}$ that exists in one or more routes among the all possible routes R selected by route request process under the RCRP, the relay transmission fitness of the corresponding node n is estimated as follows.

For each cached route $\{c \exists c \in cR \wedge n \in c\}$ that contains the respective node n, the relay transmission fitness of the node n in regard to the route c is estimated as the ratio of the packets transmitted ep_c^n by the corresponding node against the number of ingress packets ip_c^n to be transmit in regard to the cached route c. Further, the relay transmission fitness of the corresponding node in regard to all possible cached routes will be considered as the absolute difference between the average of the transmission relay fitness of the node n in regard to the all cached routes existing in set cR and having the node n and their root mean square error. The formulation of the relay transmission fitness n_{trf} of the node n is as follows in (Eq 1):

$$rrt(n) = \frac{\sum_{i=1}^{|cR|} \left\{ \frac{ep_n^{c_i}}{ip_n^{c_i}} \exists n \in c_i \wedge c_i \in cR \right\}}{\sum_{i=1}^{|cR|} \{1 \exists n \in c_i \wedge c_i \in cR\}} \quad \ldots(\text{Eq 1})$$

//ratio of relay transmission fitness $rrt(n)$ of node n, which initially scaling the sum of ratio of egress packets against the total number of ingress packets for all the cached routes having the corresponding node n, then it scales the average of the relay transmission fitness observed from all eligible cached routes having the node n.

Further, depicts the root mean square error of these relay transmission fitness observed from all eligible cached route, which are having node n as follows in (Eq 2),

$$n_{rrt}^e = \frac{\sum_{i=1}^{|cR|} \sqrt{\left(rrt(n) - \left\{ \frac{ep_n^{c_i}}{ip_n^{c_i}} \exists n \in c_i \wedge c_i \in cR \right\} \right)^2}}{\sum_{i=1}^{|cR|} \{1 \exists n \in c_i \wedge c_i \in cR\}} \quad \ldots(\text{Eq 2})$$

Further, the relay transmission fitness of the corresponding node n can be scaled as $rtf(n) = rrt(n) - n_{rrt}^e$,

This is the absolute difference of the ratio of relay transmission of all eligible cached routes and the corresponding root mean square error.

The pseudo code representation of the proposed node level relay transmission fitness is listed in Table 1.

Table 1: Pseudo code representation of node level relay transmission fitness assessment

Let the set R represents the all possible routes selected by route request under RCRP
Let the set N contains all the nodes observed in one or more routes of the set R
Let the set cR contains the cached routes of the corresponding network having temporal validity under given threshold.
$\forall_{i=1}^{|N|} \{n_i \exists n_i \in N\}$ begin
  Let the notation $tr_{n_i}\{\}$ denotes the map that represents the relay transmission ratios observed from the cached routes
  Let the notation $atr(n_i) = 0$ indicates the aggregate of the relay transmission ratios observed from the cached routes
  Let the counter $ctr = 0$ denotes the number of cached routes contains the node n_i
  $\forall_{j=1}^{|cR|} \{c_j \exists c_j \in cR\}$ Begin
    $if\ (n_i \in c_j)$ Begin
      $ctr+=1$ // incrementing the counter by 1
      $tr_{n_i}\{c_j\} \leftarrow ep_{n_i}^{c_j} \times \left(ip_{n_i}^{c_j}\right)^{-1}$ // mapping the ratio of egress packets $ep_{n_i}^{c_j}$ against ingress packets $ip_{n_i}^{c_j}$ observed for node in cached route c_j
      $atr(n_i)+=tr_{n_i}\{c_j\}$ // aggregating the ratio of egress packets $tr_{n_i}\{c_j\}$ observed from each of the cached route
    End
  End
  $rrt(n_i) = atr(n_i) \times ctr^{-1}$ // finding the average of transmission ratio of the node n_i observed from the cached routes, which denotes the ratio of relay transmission $rrt(n_i)$ of the node n_i
  Let the notation $d = 0$ denotes the aggregate of the absolute distance between average of relay transmissions ratios $rrt(n_i)$ of the node n_i and the ratio of relay transmission tr_{n_i} of node n_i in regard to the cached routes of count ctr
  $\forall_{j=1}^{|cR|} \{c_j \exists c_j \in cR \wedge n_i \in c_j\}$ Begin
    $d+=\left|rrt(n_i) - tr_{n_i}\{c_j\}\right|$
  End
  $rrt_e(n_i) = d \times ctr^{-1}$ // estimating the relay transmission deviation error $rrt_e(n_i)$ of the ratio of relay transmission $rrt(n_i)$ of the node n_i
  $rtf(n_i) = rrt(n_i) - rrt_e(n_i)$ // finding the relay transmission fitness $rtf(n_i)$ of the node n_i
End

b) *Route Level Relay Transmission Fitness*

Depicting the route level relay transmission fitness is different that compared to our earlier contribution RTFE. This since to identify the sensitive difference between relay transmission fitness of the routes. The relay transmission fitness of a route can be defined as the distribution diversity between the relay transmission fitness values observed from the nodes involved in corresponding route and max possible relay transmission fitness of the corresponding nodes involved in given route. In order to identify the distribution diversity, we adapt KS-Test [16]. The route level relay transmission fitness is scaled as follows,

For each route $\{r \exists r \in R\}$ Discovered under route request process under RCRP, collect relay transmission fitness of all nodes $\{r \text{ I } N\}$ exists in both set N and route r as a vector av_r. Frame a vector that contains expected relay transmission fitness of each node in the corresponding route r as a vector ev_r. Then find the distribution diversity between these two vectors using KS-Test. The inverse of the distribution diversity observed for the given route r can be considered further as route level relay transmission fitness of the given route r. The following section describes the approach of KS-Test.

The potential ability of Kolmogorov-Smirnov test (KS-test) [16], i.e., Concluding the distribution miscellany amid two numeric vectors. Model has potential to detect the distribution diversity without knowing the data distribution type of target vectors and the size of the vector may vary. Therefore, the present work explores the model distance metric attracts. The process of KS-Test execution is described here.

The KS-Test is applied to verify the distribution diversity of two vectors av_r, ev_r and its formulation is as follows:

Consider the two vectors v_1, v_2 aggregated values are $\|v_1\|, \|v_2\|$. Now to find entries cumulative ratio shown in the sequence of the specified vectors is explained in the (Eq 3):

$$\left.\begin{array}{l} cr = 0 \\ \underset{j=1}{\overset{|v_i|}{\forall}} \{e_j \exists e_j \in v_i\} \, begin \\ cr = \dfrac{e_j}{\|v_i\|} + cr \\ CR_{v_i} \leftarrow cr \\ end \end{array}\right\} \text{...(Eq 3)}$$

The entire process is repeated for each vector v_i representing the cumulative ratio elements of the specified vector v_i. The process of iteration for every vector is taken from the sequence of an element present in the given vector v_i as element e_j ; calculates the element e_j ratio over the $\|v_i\|$ aggregate value of the target vector v_i. Further, these values are summed with cumulative ratio cr. Later, the elements cumulative ratios in given vector v_i are formed into a set CR_{v_i}. Hence, the aggregate ratios of the elements are in the target vectors v_1, v_2 are tested and saved CR_{v_1}, CR_{v_2} sets respectively, as per the cumulative ratio detection process.

After that, the KS-test process demonstrates the exact distance between the two vectors cumulative ratios denoted as a similar index in the two sets CR_{v_1}, CR_{v_2} ; saves in the set $diff(CR_{v_1} \leftrightarrow CR_{v_2})$ - shown in the (Eq 4):

$$\underset{i,j=1}{\overset{\max(|CR_{v_1}|,|CR_{v_2}|)}{\forall}} \{cr_i, cr_j \exists cr_i \in CR_{v_1} \wedge cr_j \in CR_{v_2}\} \text{ Begin}$$

//for each index i , values is in CR_{v_1} , CR_{v_2}

$$diff(CR_{v_1} \leftrightarrow CR_{v_2}) \leftarrow abs(cr_i - cr_j) \text{ ...(Eq 4)}$$

// shows the exact cumulative ratios distance present in the sets CR_{v_1} , CR_{v_2} on the index i and saves in the set $diff(CR_{v_1} \leftrightarrow CR_{v_2})$.

End

Furthermore, it shows the maximum value from the set $diff(CR_{v_1} \leftrightarrow CR_{v_2})$ which is considered as distance. The inverse of the corresponding distance is considered as the relay transmission fitness $rtf(r)$ of the given route r.

C. Differential Evolution

The functioning of this algorithm is almost same as the functioning of GA algorithm [17]. The essential difference between the two models is, both the parent and child chromosomes are assessed with respect to their fit to the proposed model, and if the later ones are observed to have high fit value, it remains, and the other group is disregarded. The vice-versa also remains true in the context. The fittest child substitutes the related parent.

The differentiated fitness processes and multiple cross-over approaches incorporated in DE algorithm marks the disparity between various DE strategies available in existing studies [18], [19], [20], [21]. One of the new DE approaches that fit best in this context has been put forward in the contemporary study [22].

D. Optimal Route Discovery

Find all possible routes between the source and destination nodes using the route request process. These are further used as input to the Deferential Evolution Algorithm. The process of the optimal route discovery with reserved paths is detailed in following description.

Let the set $R_{s\to t}$ is having multiple number of qualified routes discovered from route request process

Let T be the clone of all possible routes $R_{s\to t}$ depicted.

Let tR be the empty set used to store the routes formed by Differential evolution.

Identify cross over points, which are one or more common nodes in sequence (excludes source and destination nodes) of given two distinct routes.

DE-PROCESS

$\forall_{i=1}^{|T|}\{r_i \exists r_i \in T\}$ Begin//for each route r_i

$\forall_{j=1}^{|T|}\{r_j \exists r_j \in T \wedge i \neq j\}$ Begin // for each route r_j , which is not the other route r_i

For each node $\{n \exists n \in r_i \wedge n \in r_j\}$ begin

$cr_i^j \leftarrow n$ //Move the node to set cr_i^j that represents the crossover of the routes r_i, r_j

End

If the set cr_i^j is not empty, Begin

//prepare new routes r_m, r_n (children) from existing routes r_i, r_j as follows.

For each entry c of the set cr_i^j , the node sequence that be exists before the crossover point c in r_i and the node sequence that exists after the crossover point c in route r_j are allied with crossover point c that leads to new route r_m such that the route r_m which wasn't present in tR

$$r_m \leftarrow r_i$$
$$r_m \leftarrow r_j$$

The node sequence that exists before the crossover point c in r_j and the node sequence that exists after the crossover point c in route r_i are connected with crossover point c that forms new route r_n such that the route r_n does not exist in tR

$$r_n \leftarrow r_j$$
$$r_n \leftarrow r_i$$

Estimate the degree of reputation dr (see section III.B), also find the relay transmission fitness rtf (see sec III.a)&III.b)) of the of the resultant routes r_m, r_n

If $\left(\left(dr(r_m) > r\tau\right) \&\& \left(rtf\left(r_m\right) > rtf\left(r_i\right)\right) \&\& \left(rtf\left(r_m\right) > rtf\left(r_j\right)\right)\right)$ then $tR \leftarrow r_m$

// if fitness of the route r_m is qualified then add r_m to tR

If $\left(\left(dr(r_n) > r\tau\right) \&\& \left(rtf\left(r_n\right) > rtf\left(r_i\right)\right) \&\& \left(rtf\left(r_n\right) > rtf\left(r_j\right)\right)\right)$ then $tR \leftarrow r_n$

// if fitness of the route r_n is qualified then add r_n to tR

End

End

End

If $(T \neq tR)$ then Begin

$T \setminus T$ // delete all entries in the set T

$T \leftarrow tR$ // move all the entries of the set tR to the set T

Repeat the evolution process DE-PROCESS

End

End of DE-PROCESS

Hence each stable and optimal route is signified, and then under contextual requirements selects the route from tR

IV. EXPERIMENTAL STUDY

The suggested method "Proactive Defense Approach (PDA)" is carried out in several dimensions for execution assessment. There are some aspects for assessing the performance of route, "delay factors", "packet delivery ratio", precise in identifying malevolent nodes & other problems of sensitivity aimed at determining the discovery of nodes procedure and such other associated factors for detecting the procedure of "node sequence verification". The attained result from empirical study is measured through comparing with the contemporary model "adaptive neuro fuzzy inference system (ANFIS)" [13].

Examining the execution is conducted in the environment through "i5 processor configuration & 4GB RAM", for assessing the execution of routing. The simulation of network for the suggested PDA & existing ANFIS method is determined by utilizing NS2 [23].

The delays which are recognized in the ANFIS, the inconsistency has taken place in the instance of execution at 0.08 ratio-levels, nevertheless, delay which is denoted at greater ratio of the malevolent nodes (0.12, 0.16 & 0.2) has to be comparatively more than which is denoted in instance of the method PDA.

The linearity levels were predicted in tests of PDA for the evaluation of relay signifies the malevolent nodes (in Figure 1).

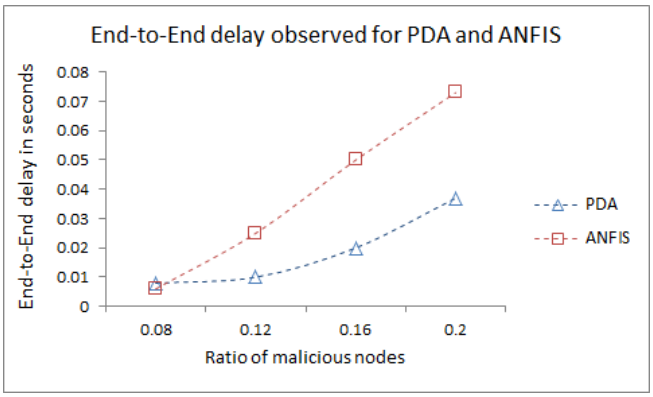

Figure 1: The end - end delay noticed for ANFIS & PDA

Figure 2 signifies the execution drop in the ANFIS for handling "optimal packet delivery ratio", through variance in malevolent nodes ratio that are shown in the PDA. And the constancy which is shown in optimal evasion aimed at malevolent nodes regarding discovery of route, in suggested method is optimal (in Figure 3).

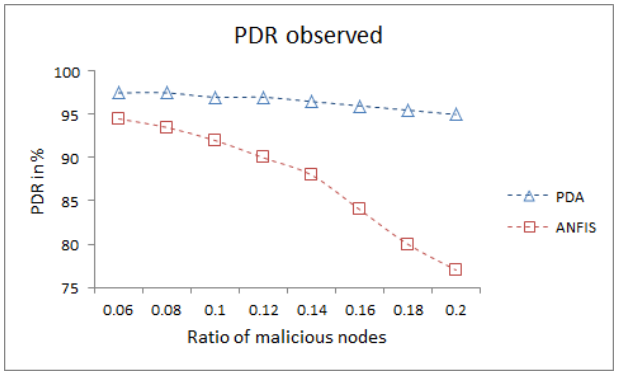

Figure 2: "Packet Delivery Ratio" noticed in ANFIS &PDA

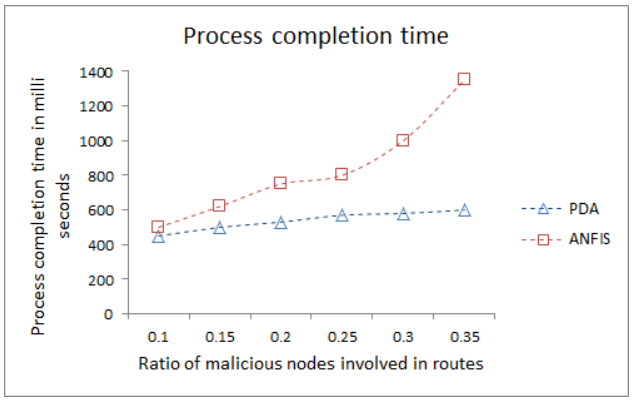

Figure 3: Completion time noticed for different ratio of malevolent nodes participation in the input routes

For evaluating the malevolent & normal nodes the evaluation procedure is executed utilizing 28 malevolent nodes & 145-normal that should be utilized by evaluating the sensitivity & accuracy. Concentrating on the routes input and nodes categorization in the form of "true-positives, false-positives, true-negatives & false-negatives" for the procedure, and the procedure intricacy is noticed in the PDA & the result displays the linear intricacy.

V. CONCLUSION

Proactive Defence Approach (PDA) to defend the block-hole and the nodes compromised to denial of service attacks such as gray-hole and worm-hole attacks in mobile ad hoc networks is the contribution of this manuscript. The proposed model is fine-tuned extension to our earlier contributions called reputation cognizant routing protocol (RCRP) [14] and the KS-Test based Relay Transmission Fitness evaluation for route discovery that enables to select route without the nodes compromised to black-hole attacks and the denial of service attacks. In order to find optimal route, the proposal PDAadapted the route level degree of reputation and the route level relay transmission fitness as the metrics used in fitness function of the evolutionary approach Differential Evolution. The experimental study scaled the performance of the proposal PDA by comparing with the contemporary model called "adaptive neuro fuzzy inference system (ANFIS)". The results obtained from the simulation study evincing that the proposed model PDF is significantly performed well that compared to the other contemporary model ANFIS. The future research can portray the degree of reputation and relay transmission fitnessmethods to determine the nodes that are prone to intrusion in other networks such as IOT and body sensor networks. The other dimension of research can extend the contribution of this manuscript to deal with the DDOS.

REFERENCES

1. J. Srilakshmi1, S.S.S.N. Usha Devi N2, "Secure and Efficient Multipath Routing Using Overlay Nodes", International Journal of Scientific Research. Computer Science and Engineering, 6.5 (2018): 16-19.
2. Bendale, Lubdha M., Roshani L. Jain, and Gayatri D. Patil. "Study of Various Routing Protocols in Mobile Ad-Hoc Networks." International Journal of Scientific Research in Network Security and Communication 6.01 (2018): 1-5.
3. Banerjee, Sukla. "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks." proceedings of the world congress on engineering and computer science. 2008.
4. Su, Ming-Yang. "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems." Computer Communications 34.1 (2011): 107-117.
5. Mohanapriya, M., and IlangoKrishnamurthi. "Modified DSR protocol for detection and removal of selective black hole attack in MANET." Computers & Electrical Engineering 40.2 (2014): 530-538.
6. Jhaveri, Rutvij H., and Narendra M. Patel. "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks." Wireless Networks 21.8 (2015): 2781-2798.
7. Sen, Jaydip, et al. "A mechanism for detection of gray hole attack in mobile Ad Hoc networks." 2007 6th International Conference on Information, Communications & Signal Processing. IEEE, 2007.
8. Khan, Muhammad Saleem, et al. "Fine-grained analysis of packet loss in MANETs." IEEE Access 5 (2017): 7798-7807.
9. Pal, Seemita, BiplabSikdar, and Joe H. Chow. "An online mechanism for detection of gray-hole attacks on PMU data." IEEE Transactions on Smart Grid 9.4 (2018): 2498-2507.
10. Panos, Christoforos, et al. "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks." Computer Networks 113 (2017): 94-110.
11. Schweitzer, Nadav, et al. "Contradiction based gray-hole attack minimization for ad-hoc networks." IEEE Transactions on Mobile Computing 16.8 (2017): 2174-2183.
12. Dorri, Ali. "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET." Wireless Networks 23.6 (2017): 1767-1778.

13. Chaudhary, Alka, V. N. Tiwari, and Anil Kumar. "Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks." International Journal of Soft Computing and Networking 1.1 (2016): 17-34.
14. Kondeboina Srinivasa Kumar &Dr. M. Akkalakshmi. "RCRP: Reputation Cognizant Routing Protocol for Secure Data Transmissions in Mobile Ad-Hoc Networks." Journal of Advanced Research in Dynamical and Control Systems. ISSN NO:2236-6124, 10.2 (2018): 1537-1545.
15. Kondeboina Srinivasa Kumar &Dr. M. Akkalakshmi. "Optimizing Reputation Based Route Discovery by Relay Transmission Fitness Evaluation". (2019).
16. Ghasemi, Asghar, and Saleh Zahediasl. "Normality tests for statistical analysis: a guide for non-statisticians." International journal of endocrinology and metabolism 10.2 (2012): 486.
17. Mitchell, Melanie, Stephanie Forrest, and John H. Holland. "The royal road for genetic algorithms: Fitness landscapes and GA performance." Proceedings of the first european conference on artificial life. 1992.
18. Brest, Janez, and MirjamSepesyMaučec. "Population size reduction for the differential evolution algorithm." Applied Intelligence 29.3 (2008): 228-247.
19. Qin, A. Kai, Vicky Ling Huang, and Ponnuthurai N. Suganthan. "Differential evolution algorithm with strategy adaptation for global numerical optimization." IEEE transactions on Evolutionary Computation 13.2 (2009): 398-417.
20. Mininno, Ernesto, et al. "Compact differential evolution." IEEE Transactions on Evolutionary Computation 15.1 (2011): 32-54.
21. Islam, SkMinhazul, et al. "An adaptive differential evolution algorithm with novel mutation and crossover strategies for global numerical optimization." IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics 42.2 (2012): 482-500.
22. Das, Swagatam, and PonnuthuraiNagaratnamSuganthan. "Differential evolution: a survey of the state-of-the-art." IEEE transactions on evolutionary computation 15.1 (2011): 4-31.
23. http://www.cs.tut.fi/kurssit/TLT-2707/lecture13.pdf