AN ACCURATE IDENTIFICATION OF PACKET DROPPING ATTACKS USING CAT SWARM OPTIMIZATION (CSO) TO ENSURE BETTER INTRUSION DETECTION IN MANET ENVIRONMENT

Niyaz Hussain A M J, G Maria Priscilla

Abstract: ***Mobile Ad hoc Network (MANET), which is comprised of a number of self-organized and battery equipped mobile nodes, is used widely in different applications, like private sectors and military. However, security is a major issue in MANET routing, as the network is prone to attacks. The main objective of intrusion detection system is for categorizing normal and suspicious activities in network. This paper introduce the intrusion detection scheme for establishing the secured path in MANET. For mobile ad hoc networks, swarm optimization approach based novel intrusion detection system is proposed in this paper. The proposed system is based on Cat swarm optimization (CSO) for detecting, one of vey possible attack, i.e. packet dropping attack in mobile ad hoc networks. Also Failure node discovery can be optimized by considering nodes historical information along with the neighbor node information. Before using the swarm optimization for findingsensor node's trust values and for improving provenance data transmission security, an Extend the secure provenance scheme with Side Channel Monitoring – Information gaining ability (SCM) for detecting packet drop attacks staged by malicious data forwarding nodes is used. It assist in finding presence of selfish nodes as well as packet drop behaviours. With low false positive rate and high true positive rate, packet dropping attacks are detected effectively using proposed technique as shown in simulation results.***

Keywords- Mobile Ad hoc Network, swarm algorithm, Side Channel Monitoring, packet dropping attack, intrusion detection

I. INTRODUCTION

Because of high flexibility shown in communication between nodes, Mobile Ad hoc Networks (MANETs) gained huge attractiveness in recent days. They are not having any centralized management points or predefined infrastructure. Every node in MANETs performs the operation of router in addition to data packet transmission host. Because of this abilities, MATNETs are used in various applications like communication between groups of people in neighborhood networks or virtual conferences, military applications which requires a rapid deployment of network topology in battlefields, disaster relief management and various other fields with similar applications,

Revised Manuscript Received on October 10, 2020.

***** Correspondence Author

Niyaz Hussain A M J[1]*, Ph.D. Research Scholar, Department of Computer Science, Sri Ramakrishana College of Arts & Science (Formerly SNR Sons College), Coimbatore, Tamilnadu, India / Assistant Professor, Hindusthan College of Arts and Science, City Campus: Nava India, Coimbatore - 641028, Tamilnadu, India, amj.niyaz@gmail.com

Dr G Maria Priscilla[2]*, Professor & Head, Department of Computer Science, Sri Ramakrishana College of Arts & Science (Formerly SNR Sons College), Nava India, Coimbatore 641006, Tamilnadu, India, mariajerryin76@gmail.com

As like in wired networks, there is a vulnerability of security attacks in MANETs like spoofing and it is also prone various other attack types [1-3], because of cooperation between dynamic topology and mobile nodes, resource constraints like power and bandwidth, communication over wireless links. A black hole attack is highly concentrated in this paper, which is having high influence in operations of MANETs. On reactive routing protocols like AODV [4] routing protocol, this attack can be launched easily. In addition, all the data packets are attracted by black hole attacker by wrongly showing short as well as fresh route to destination node. There wont be any active path to specified destination and all the attracted data will be deleted. In view of security in MANETs, sufficient solutions are not provided by intrusion prevention methods like encryption and authentication for eliminating compromised nodes. For this reason in MANETs, it is necessary to have Intrusion Detection System (IDS) and it is termed as second defense line for any network. Based on the used detection method, IDSs are classified as, anomaly-based detection, specification-based detection and misuse or signature based detection [5]. In misuse based detection, for verifying intrusion existence, a comparison is made between network patterns signature and existing attack patterns signatures. Set of specifications are defined in detection based on specification, hat must be satisfied by the protocol. If an event is not matching with established conditions of good operation, an attack will be detected. Networks normal behaviour is considered in the anomaly detection, unknown activities are flagged and an alarm is generated based on this activity. For wired networks, various IDSs are developed and because of its complex characteristics, these IDSs cannot be used on MANETs. So, for MANETs domain, new IDSs are designed by researchers [6]. However, soft computing methods usage are enforced in this paper in MANETs. An emerging technique used in computing field is soft computing, where, notable potentiality of human mind for understanding as well as learning is exhibited in uncertainty as well as imprecision conditions [7]. In general, three major components are admitted in soft computing, which are named as genetic algorithms, fuzzy logic and neural networks. In wired networks, in intrusion detection fields, applicability of various soft computing methods are proven. In recent days, in MANETs, soft computing is used to detect intrusion by various researchers.

So, for MANETs, few soft computing method based IDSs are developed. A robust mathematical toll called fuzzy logic shown its applicability in IDSs [8]. Consequently for MANET, IDSs based on fuzzy systems are proposed by various researchers, human expert knowledge based fuzzy rules are used in majority of proposed fuzzy systems, which lacks in adaptation. For example, fuzzy system is explored in this paper due to its learning and adaptation abilities for designing intrusion detection system in MANET. Process of fuzzy system production is automated using Adaptive Neuro Fuzzy Inference System (ANFIS) [9] and Swarm Optimization (SO) [10] is used for optimizing our system [10]. From simulated network, a database is extracted for performing this, and then from this database, proper parameters are extracted. At last, with target output, mapping of these parameters are processed. Hence in this research extend secure provenance scheme with Side Channel Monitoring – Information gaining ability (SCM) for detecting packet drop attacks staged by malicious data forwarding nodes. Then a Cat swarm algorithm is applied to eliminate redundant record set and imputation method to handle missing value is introduced. Data clustering can be done by modified k-means clustering which can be used to in failure node discovery can be optimized by considering the historical information of the nodes along with the neighbor node information.

II. LITERATURE SURVEY

P. Joshi, et al. [11] proposed the Enhanced Adaptive ACKnowledgment (EAACK) scheme for detecting and preventing malicious attacks. The scheme handled the packet dropping and hacking issues prevailing in the MANET. The system ensured security by defining priority to each node for path establishment. Even though the model ensured improved security in MANET, all the weakness arising due to the watchdog was not handled efficiently. Khan, F.A., et al. [12] proposed the Detection and Prevention System (DPS) for handling the security alerts arising due to network attacks. The model employed some special nodes for monitoring the normal nodes in the MANET. If a change in normal operation was detected, then the special node declares the node to be suspicious. As the special node employed in the scheme does not involve in data transfer, it had enhanced battery life, but increases the network cost. N. Marchang, et al. [13] proposed the IDS for detecting the malicious nodes in MANET by reducing the overall active time of IDS. The model ensured secure data transmission over network even though the active time of IDS was reduced. The model ensured secure transmission in homogenous platform, but has failed in heterogeneous network. Shams, E.A. and Rizaner, A. [14] proposed the IDS based on SVM framework. The framework was specially trained to identify the effects arising due to the DoS type attacks. As the SVM architecture had simple structure, the scheme detected the attacks with less computation time. The scheme removed malicious nodes from the system, and established the secured routing path.

Gurung, S. and Chauhan, S. [15] introduced special nodes, namely Flooding-Intrusion Detection System (F-IDS) to eliminate flooding attacks effects. The special nodes deployed with MANET nodes ensured the detection and prevention of flooding attacks. The impact of address spoofing that raised during flooding was not addressed in the scheme. A trust based routing protocol is designed in [16] to cluster based MANET. During packet transmission to destination node from source node, highly reliable path is computed using this routing technique. In ad hoc network, malicious nodes which are acting as a real node are avoided in this mechanism. Trust score matrix computation by cluster head is explained in this paper based on max-min composition dependent fuzzy logic of highly reliable nodes.

An exact algorithm to detect insider attacker based selective packet drops are developed in [7]. For supporting detection decision, specified algorithm shows its truthful and publicly provable decision statistics. Even though, packet loss rate is caused by malicious dropping which can be compared with normal channel losses. Different correlation structures are exhibited by stochastic processed which explains these phenomena. Equivalently it explains various packet loss patterns. Between lost packets, to detect correlations, one can detect the nature of packet loss like due to malicious drop, or link errors or by both of these. Cross-statistics between lost packets are considered for composing a highly informative decision in this proposed algorithm of this paper. There is a sharp difference between this one and conventional techniques that confiding only on lost packets distribution.

III. PROPOSED METHODOLOGY

Development of a framework to be used with cat swarm based optimization technique for building binary classifier is concentrated in this proposed work. This framework can produce better results when compared with single soft computing techniques. Intrusion detection system based on proposed architecture is described in this section for MANETs, which is shown in Figure 1 and response, detection and data collection modules are included in this.

Proposed IDS system uses the features listed in Table 1 as in input. Input patterns are labelled with 0 and 1. In MANETs, from binary classifier's point of view, attack input data pattern are represented as 1 and normal are represented as 0. Intrusion detection system's two architectures based on proposed classifiers are described in this paper, i.e. cooperative, distributed and local. In network, every mobile node has an IDS agent in local intrusion detection system (L-IDS) and based on its own decision, attacks are detected without other nodes collaboration. However, there is an IDS agent in every mobile node of a network in distributed and cooperative intrusion detection system (DC-IDS) and based on communication with other nodes for information exchange, attacks are detected and this decision are shared and at last agrees on responses with other nodes. There will be a communication between nodes and its one hop away nodes for reaching decision regarding malicious activity presence or absence in MANETs in this proposed DC-IDS.

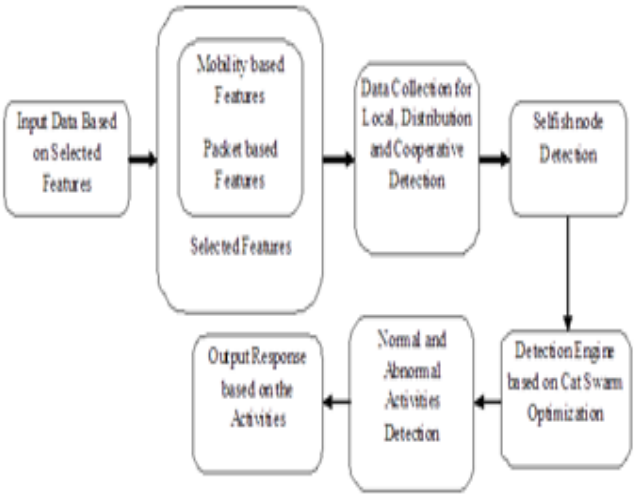

Figure 1: Proposed Architecture

a. Input Data Based on Selected Features

A spectacular attributes called features are used as an inputs in our suggested system. It is highly important to select appropriate features to produce better results. Features having relation with packet dropping attack are highly concentrated in this proposed system.

Table 1 illustrates our proposed features. In network, on every node, these features are asserted through AODV routing protocol. Through malicious nodes, packets dropping attacks are detected by this emphasized work. The proposed IDS methods efficiency is demonstrated by focusing on rich set of features.

Table 1: Selected feature set

Abbreviations of Features	Explanations
EnumdataPksInitd	Data packets count sent as data source by this node
numdataPksfwrd	Data packets count forwarded by this node
numdataPksrecvd	Data packets count sent as data destination by this node
Num rep recvdasSrce	RREP packets count received as source by this node
num rep initdasDest	RREP packets count initiated from destination by this node
num rep initdasIntermde	RREP packets count that are initiated from an intermediate node
num rep fwrd	RREP packets count that are forwarded by intermediate nodes
Num rep recvd	RREP packets count that are received by this node
numreqrecvdasDest	RREQ packets count received as a destination for this node
num err fwrd	RERR packets count forwarded by this node
num err initd	RERR packets count initiated as this node detect link break
num routes	Routes count added to route cache
num err recvd	RERR packets count received by this node
numreqinitd	RREQ packets count initiates by this node
numreqreceivd	RREQ packets count received to this node
NumbrknLinks	Total no. of broken links
Dropped datapkts	Calculates not forwarded data packets through this next node
numaddNbrs	Added neighborscount of node during simulation time
numrmveNbrs	Removedneighborscount of node during simulation time
numnbrs	Neighborscount of node during simulation time

According to two classes, features are collected. They are packet related and mobility related features. For every network or node, information about mobility node's reactions are devoted by mobility related features. However, node's mobility is directly reacted by few features like remove neighbors and added neighbors. Information about routing protocol control packets for sent (RREQ),received (RREP) as well as forwarded are admitted by packet related features at every time interval. However, particular attacks signature are definitely presented by some features e.g. Dropped data pkts" feature is used for detecting packet dropping attack [18]. During data collection, there is no need to have communication between mobile nodes, since totally selected features are local to every node [18].

b. Detecting Selfish Nodes by Side Channel monitoring scheme

For ensuring data protection, packet drops are observed in this proposed provenance technique, in addition to provenance preservation. Node activities are observed in this technique. For accumulating possessing capitals, packet forwarding are refuted by selfish nodes. This behavior shows that, selfish nodes are involved either in relay or routing data packets. Unallowable packet drops are produced by nodes selfish activities. Packet drop assaultby opponents are performed due to this nodes selfish characteristics or it may lead to internal divergence like node failure or overload. In these cases, protected packet transmission is not offered by this path assembling via selfish nodes. Network monitoring using local watchdogs is a technique used for noticing behavior of selfish node. A method called channel examining to notice selfish nodes and evading packet drop is used in this anticipated technique. Routing nodes misconduct is observed by a centralized contact based watchdog in this side channel matching technique. Data about every neighborhood node is gathered by this watchdog node, which are examined moderately examined using normal node's performance. Warning message is send to source node from watch dog, if nodes packet transmission performance appears as atypical one. In packet transmission, measured the deviation between packets counts acknowledged and packets count forwarded is noticed as exception cased. Neighboring nodes are discovered by forwarding control messages by new nodes. With nodes S, R1, R2, R3 and D, routing path is regarded to presume, where S is a source node and D is destination node as illustrated in [19].

Selected a centralized watchdog C, which is grounded on selection circumstances like connectivity and energy of all adjoining nodes (1- hop to every nodes in path).

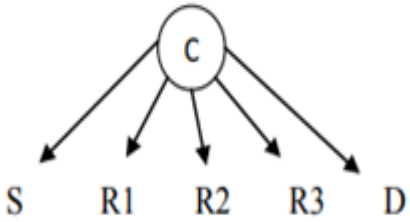

Figure.2. Routing path S-R1-R2-R3-D

All the nodes R1, R2 and R3 are observed using selected watchdog C [19]. The packets count acknowledged by routing nodes must be forwarded to next node. But, if this routing node is a selfish one, then there will be a difference between received and forwarded packets count. So, for instigating packet drops, alert message is propelled by watchdog node to S, if there is a difference.

Algorithm 1: Side Channel Monitoring

Source node S, Destination node D areinitialized
Route path ID list is generated by S.
Near path S-R1-R2-R3-D, watchdog C is positioned
Through path S-R1-R2- R3-D, data packets p are send to D from S.
Route path nodes R1-R2-R3 are analyzed
For every node
If (forwarded packets count< received packets count)
Node is finalized as malicious node
Warning message to S is initiated
Else
Packet transmission is performed
End if
End For

Source node, watchdog, destination node are initiated using suggested technique and routing path is figured out using it. In path ID list, accumulated every node's ID in that path which is source directed. For sustaining information about paths, every successive node upholds a list. Every node in watchdog C's neighborhood are observed by it. A node is termed as selfish node, if it receives more packets when compared to packets forwarded by it and this node is packet drop attack launching competent.

If these nodes notices a warning message instigated and from routing path, this exacting nodes are eliminated by source. After detaching the malicious node, path is maintained by source node by finding possible replacement node. If related path is not formed due to unavailability of accessible node, instigate the procedure of reconstruction. In packet transmission, security is enhanced using this anticipated approaches.

c. CSA for finding the packet dropping attack

The ad hoc on demand distance vector (AODV) is a widely used MANETs routing protocol [20]. In this research, AODV routing protocol is used. Packet dropping attack is a common type of attack in MANETs. In [6] elaborates about entire description of this attacks on MANETs. Packet Dropping Attack: A malicious node or an attacker drops data packets in packet dropping attack in order to disturb operation or service of network [6].

To achieve these objectives, attacker or malicious nodes are need to be in routing path or it should take part in routing operation. This makes the chances of RERR, RREP, RREQ packets dropping as a minimum one. In this research, assumption is made that, AODV routing protocol's RERR, RREP, RREQ packets are not dropped by attacker nodes. So, there will be a reduction in network performance because of data packets dropping and it requires to retransmits data packets or it needs effective discovery of new routes. In network, communication between nodes are prevented by this attack. During simulation of this research, data packets are dropped continuously by attacker nodes in every 1 sec intervals. Because of congestion, packets will be lost in wired networks in general. Because of complex characteristics of MANTEs, packets are dropped and it includes some other reasons like wireless links transmission error, mobility and congestion. On AODV, data packets are lost due to mobility as like in MANETs [10]. In MANETs, packet dropping due to malicious nodes and due to mobility are differentiated in this work and it's concentrated highly on it. Redundant record set are eliminated using CSA algorithm in this paper and introduced a imputation technique for handling with missing values.

From swarm intelligence algorithms like ACO and PSO, inspired the Cat swarm optimization (CSO) [21]. Chu and Tsai proposed this CSO algorithm and which is a high performance meta-heuristic algorithm and it is motivated from cats instinctive behavior. There exist a natural curiosity towards moving things in it and has better hunting skills.

Cats behavior can be modelled as two-sub-modals. They are tracing mode and seeking mode. Cats will be in resting position but they will be in alert position in seeking mode. At fixed position, they used to stay and will look around for next better move. Behavior of cat in target chasing is represented by tracing mode. Based on its velocity, they move to its next better positions. Various solution or position are exploited and explored by cats using tracing and seeking mode. Following steps are used for describing CSO process.

Algorithm 1:

Begin
Parameters are initialized and initial population is established
while (not termination-condition) do
while i ≤ P do
if (seeking mode $M_s$is assigned with cat X_i) then
seeking mode $M_s$is performed
else
tracing mode $M_t$performed
end if
end do
Cats are reassigned and best known cat $X_b$is updated
end do
output cat X_b
end

The above condition is checked by source node, if it is ready for transmission of a packet through optimized path. For energy and bandwidth, fitness value profiles of nodes are checked to forward packet and for optimum throughput, fitness value is checked. Available value is compared with energy and bandwidth's fitness values.

Here, position value is assumed as bandwidth and velocity value is assumed as energy value. When compared with profile value, throughput value must be high. If this condition is satisfied, packet can be transmitted using the respective node. A malicious node detected by source, further transmissions are discarded by it [22].

The original CSO algorithm is included with few modifications for making more effective as well as competent CSO algorithm for clustering problems. Enhanced k means clustering algorithm is used for enhancing CSO algorithms diversity nature and for rectifying local optima problem. Following describes these modifications in a detailed manner.

d. Cat swarm optimization K-means clustering (CSO-K) algorithm

The cat swarm optimization architecture is observed in proposed CSO-K algorithm. For enhancing clustering techniques convergence, seeking mode is integrated with one-step k-means algorithm and for avoiding local minima trapping, tracing mode is hybridized with annealing. The CSO-K algorithm's general description is given in Algorithm 1. In that, ith solution is represented as X_i, best known solution is given by X_b, seeking mode is represented as M_s, tracing mode is represented as M_t and population size is given by P.

Here, position Xi represents cat i, which is aith clustering solution. In this work, real numbers are used for creating clustering solutions, which are used to represent cluster center's coordinates. Then, solution's length is given by m×K, where, cluster count is represented as K, object attributes count is given by m. First cluster center's m dimensions are represented by first m elements, second cluster center's dimensions are given by next m elements and so on.

For example, assume m=2 and K=3, then three cluster centers {(3.7 4.8) (6.5 2.9) (2.5 4.7)} coordinates are represented as solution (3.7 4.8 6.5 2.9 2.5 4.7). From dataset, K distinct objects are selected randomly to initialize solution Xi and they are assumed as an initial cluster centers. Detailed report about design approaches are specified in this study.

Assignment of cats

Between seeking and tracing mode, cats are assigned randomly in initialization stage. That is, P_s cats are selected into seeking mode and P_t cats are selected into tracing mode in a random manner. Where, cats count in seeking mode is represented as P_s and in tracing mode is represented asP_t. They are given by,

$$\begin{cases} P_t = \lceil R_{mr} \times P \rceil \\ P_S = P - P_t \end{cases} \quad (1)$$

Where, mixture ratio used for tuning cats counts in two modes is represented as R_{mr}. Cats are normally used to spend huge time in resting and observing its environment. If they decided to move from resting, it is done in a slow as well as careful manner. Seeking mode is used for representing this behavior.Cats chasing to a target is modelled using this tracing mode. Very small amount of time is spend by cats in chasing as it requires high energy resources. So, for ensuring high observation and resting time of a cat, it should spend most of its time in seeking mode, for that small value is allocated to R_{mr}.

Seeking mode

During the rest period, cat is modelled using this model, but cat is being alert as well as looks it environment for next move. There are four factors in cat swarm optimization. They are, self position consideration (SPC), counts of dimension to change (CDC), seeking range of the selected dimension (SRD) and seeking memory pool (SMP).

For a specified solution $X_l, l = 1, \dots P_s$, created its neighboring solution X_r^l, by randomly adding or subtracting SRD percent and solution X_l's CDC dimension, where, $r = 1, \dots, N_{SM}$, SMP size is represented as $N_{SM}$and it represents neighboring solutions count.

For renewing solution X_l, selected one neighboring solution (Chu and Tsai, 2007). In clustering procedure, domain knowledge is incorporated for combining clustering problem under consideration with cat swarm optimization and for enhancing cat swarm optimization clustering techniques performance further. Solution X_l's neighboring solution is established first and for fine tuning these neighboring solutions k-means enhancement is designed. At last, proportional selection is employed for selecting neighboring solution for updating solution X_l.Following states the seeking mode.

Step 1: Neighboring solution generation. For a specified $X_l, l = 1, \dots P_s$, and neighboring solutions count N_{SM}, select cluster C_j to be modified in a random manner. Then object $x_i$belonging to cluster $C_j$is randomly selected as cluster C_j's new cluster center. At last, every objects are reassigned to corresponding nearest clusters. By this manner, generated the neighboring solution X_r^l. Until producing solution $X_l's$ every neighboring solutions, this process is continued.

Step 2: K-means enhancement. Among various clusters, object distribution is tuned by adopting one-step k-means algorithm based k-means enhancement, after the establishment of solution X_l's neighboring solutions for enhancing neighboring solution's performance. This technique is stated as: if the following conditions are satisfied, object x_i is re-assigned to cluster $C_j$for specified neighboring solution X_r^l.

$$\|x_i - c_j\|^2 < \|x_i - c_k\|^2, \quad (2)$$

where$i = 1, \dots N, j, k = 1, \dots, K$ and k≠j . After re-assigning every objects, new cluster centers $c_1', \dots, c_k'$will be

$$c_j' = \frac{1}{n_j} \sum_{x_i \in C_j} x_i \quad (3)$$

Where, objects count belonging to cluster C_j is represented as n_j. Modified solution is assumed as a neighboring solution X_r^l, after k-means enhancement. Until modifying every neighboring solution of solution X_l, this process will be continued.

Step 3: Solution X_l's update. A proportional selection is employed which is a genetic operator in genetic algorithm for renewing solution X_l and for computing candidate solution in this article. Selection probability of neighboring solution X_r^l is expressed as,

$$p_r^l = \sum_{u=1}^{N_{SM}} \frac{f(X_u^l)}{f(X_r^l)} \quad (4)$$

That is, decrease in of neighboring solution X_r^l's objective function, increases the probability of getting selected as a candidate solution and vice versa. The solution X_l is replaced with neighboring solution X_r^l after selecting neighboring solution X_r^l as candidate solution and updated solution $X_l$is returned.

Tracing mode In tracing targets, for modelling the case of cat, designed this tracing modes. After getting into tracing mode, cats moves based on its velocities in every dimension. Velocity and position update of cats is a major objective of tracing mode in cat swarm optimization. In this study, simulated annealing is integrated into tracing mode for acting as a selection criterion for promoting unvisited spaces exploration and maintaining diversified population.

Solution search trapping in local minima is avoided using tracing mode via acceptance of few based solutions of current population in next population based on simulated annealing selection parameter. Following describes the tracing mode.

Step 1: Velocityupdate.

For a specified cat $X_i, i = 1, \dots, P_t$, its child X_i''s velocity $V_i'$is updated as

$$V_{ij}' = V_{ij} + r_1 \times c_1 \times (x_{bj} - x_{ij}) \quad (5)$$

Where, $j = 1$, a random value is represented as $K \times m, r_1$and it takes the value between 0 to 1, constant value is given by c_1, cats velocity can be extended using this for moving in solution space, best known solution X_b's jth element is given by x_{bj} and solution X_i's jth element is given by x_{ij}.Here, value of $c_1$is set as 2.

Step 2: Renewal of position. Update child X_i' of solution $X_i$as

$$X_{ij}' = x_{ij} + v_{ij}' \quad (6)$$

Reassignment of cats

Cats are re-assigned between tracing mode and seeking mode after they are performed. Here based on mixture ratio R_{mr}, some cats are selected randomly into tracing mode and others are set with seeking mode. Following describes the cats re-assignment.

Step 1: Set 1=i after tracing mode and seeking mode, for a specified population.

Step 2: Based on mixture ratio R_{mr}, Cat $X_i$is assigned randomly to tracing node or seeking node.

Step 3: If$f(X_i) < f(X_b)$, then $X_b = X_i$and$f(X_b) < f(X_i)$. Set$i = i + 1$. If $i \leq P$, then move to Step 2, otherwise output objective function value $f(X_b)$, best known cat X_b and re-assigned population.

IV. EXPERIMENTAL RESULTS

Proposed DC-IDS systems performance is evaluated using NS-2 simulator in this section. In this simulation model network, within a 100 × 100 meters area, 100 nodes are randomly placed. In simulation, two nodes types are defined. They are malicious nodes and well-behaved nodes. In the simulated scenarios, attacks are launched using malicious nodes. There are unlimited energy in BS. For one interval, selected CH count is fixed to 10%.

Proposed system DC-IDS is compared with previous systems called L-IDS for evaluating the performance of proposed system. Table 1 specifies the parameters used to evaluate the security system in this research. Metrics like mean packet latency, end-to-end delay, energy consumption, packet delivery ratio and packet loss are used for evaluating the proposed DC-IDS system's performance.

Table 1 Parameters of Simulation

Parameters of Simulation	Values
Channel	Wireless Channel
Mac	802.11
Type of Antenna	Omni antenna
Routing Protocol	AODV
Energy in initial stage	100 joules
Type of traffic	CBR
Agent	UDP
Area of simulation	100X100 meters
Nodes count	100

Mean Packet Latency

Proposed DC-IDS selects shortest route having low hop count for data transmission, which results in low mean packet latency for those packets reaching destination. Because of reduced malicious attacks, proposed technique reduces mean packet latency. Figure 3 shows the mean packet latency's graphical representation.

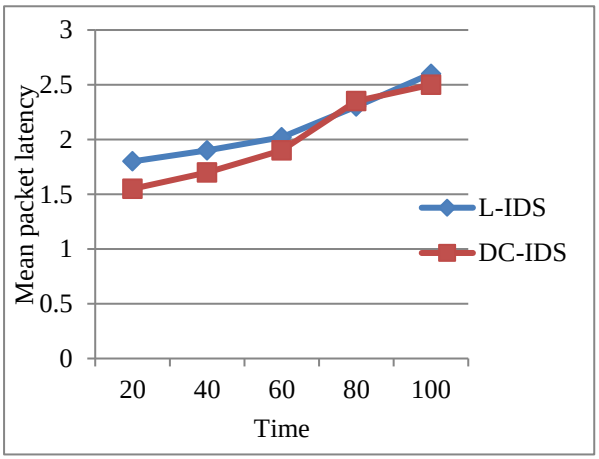

Figure 3 Mean packet latency

When compared with available L-IDS system, low packet latency is produced by DC-IDS. For data transmission, path with high hop to hop count distance is not selected in proposed DC-IDS system and this path is considered as an attack path.

Packet Loss

Total data packets count lost through malicious action or legitimately without any notification defines this. Packet loss rate's graphical representation is shown in figure 4. When compared to available L-IDS techniques, less packet loss rate can be achieved using this proposed DC-IDS technique.

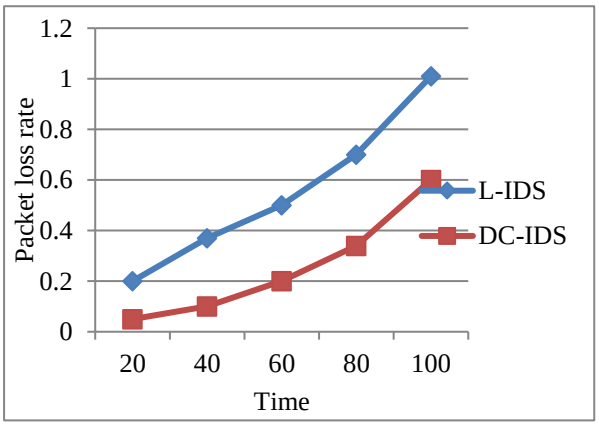

Figure 4Packet loss comparison in various trust model

Difference between malicious and genuine nodes are not considered in the existing system. Every node having high traffic deviation is considered as a malicious node in these existing systems.

According to variance and bias, individual malicious nodes are identified in the proposed algorithm. This avoids packet drop by genuine nodes. When compared with available L-IDS, less packet loss rate is exhibited by proposed DC-IDS as shown in experimental results.

Packet Delivery Ratio

Ratio between total data packets count received and total data packets count transmitted defines this packet delivery ratio. Level of data delivered to destination is illustrated using this.

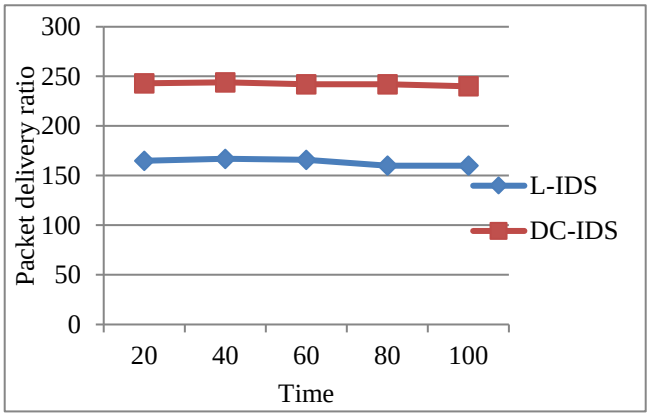

Figure 5Packet delivery ratio comparison of various trust system

Packet Delivery Ratio (PDR) and rounds count performance comparison between available L-IDS and proposed DC-IDS is illustrated in figure 5. At the destination, packets count which are received effectively without any packets loss or failure is high in the proposed DC-IDS, which leads to high PDR results.

Energy Consumption

During the specified simulation time, average energy consumed in every node is expressed in Joules (J).

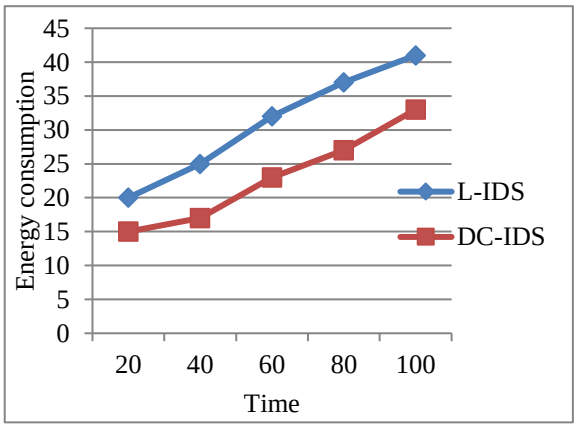

Figure 6Energy consumption comparison of various trust system

For various military applications trust models, energy consumptions graphical representation are shown in figure 6. When compared with available L-IDS system, low energy is consumed by DC-IDS technique.

End-To-End Delay

During the transmission to BS from source, delay experienced by the data packet is referred as delay, which includes propagation, queuing and processing delay. On military applications, performed the overall evaluation of this work. During path communication, high end to end delay is produced with high hop to hop count distance.In DC-IDS system, data transmission to destination from source is performed using this hop to hop count distance. This leads to reduced end to end delay. Path with high hop to hop count distance is not selected for data transmission in proposed DC-IDS system.

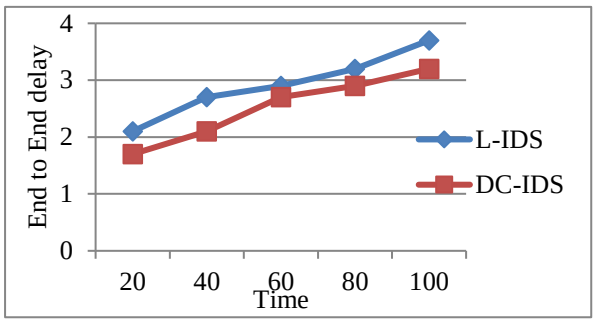

Figure 7 End-to-end delay comparisons of various trust system

When compared to available systems, minimum end-to-end delay is shown by proposed DC-IDS technique. For data transmission, path having high hop to hop count distance is not selected in proposed DC-IDS system and this path corresponds to attack path.

False alarm rate

In detection of an attack, false alarms count per total alarms or warnings count defines false alarm ratio and it is abbreviated as FAR. In the following figure false alarm rate comparison is shown against different number of attacker nodes presence in the environment.

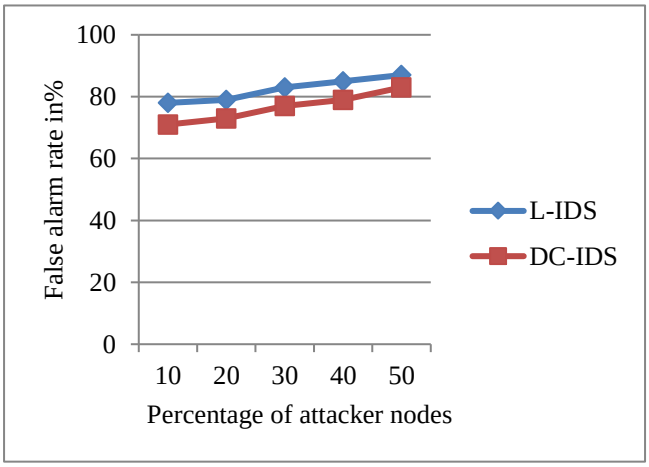

Figure 8. False alarm rate vs number of attacker nodes

False alarm rate comparison between existing and proposed techniques are illustrated in figure 8. From this comparison it is concluded that proposed method DC-IDSis having better performance than the previous methodologies with lesser wrong detection of attacker nodes.

False positive rate

Ratio between negative events count which are wrongly classified as positive, termed as false positive to total actual negative events count irrespective of classification defines this false positive rate.

Percentage of incorrect identification of attacker node by the algorithm is indicated using this false positive rate.

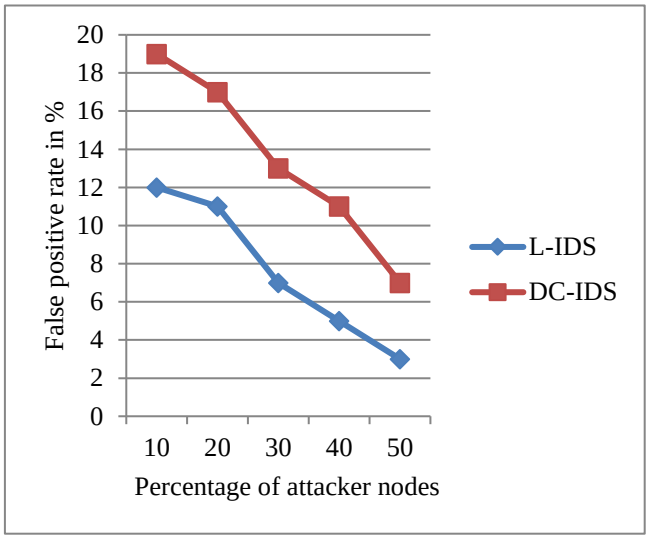

Figure 9. False positive rate vs percentage of attacker nodes

In figure 9, comparison evaluation of the false positive rate for the proposed and existing methodologies are given. From this comparison it is concluded that proposed method DC-IDSis having better performance than the previous methodologies with lesser wrong detection of attacker nodes.

Success rate Vs Ratio of colluding node

Success rate, which is the percentage that our algorithm can correctly identify the attacker nodes.

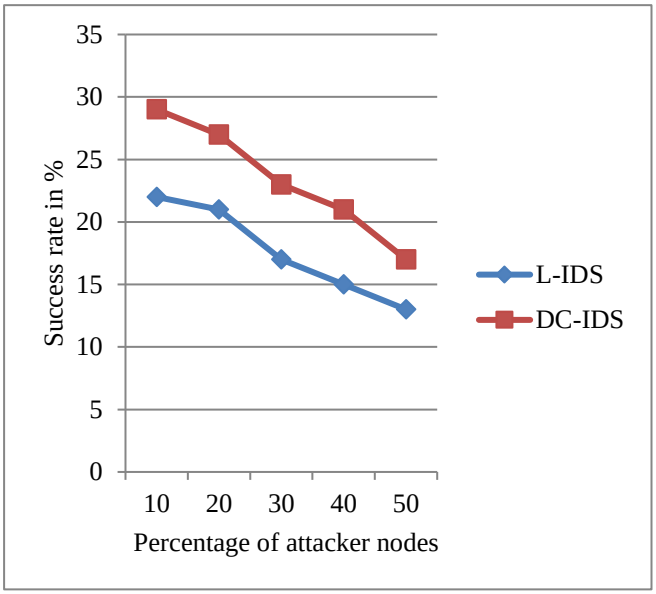

Figure 10. Success rate comparison

In figure 10, comparison evaluation of the success rate for the proposed and existing methodologies are given. From this comparison it is concluded that proposed method DC-IDSis having better performance than the previous methodologies with accurate detection of attacker nodes.

Attack probability Vs method

Attack probability is defined as the effectiveness of proposed algorithm to capture the present of attacks from total attacks count. Ratio between captured attacks count to total attacks counts in the environment defines this attack probability.

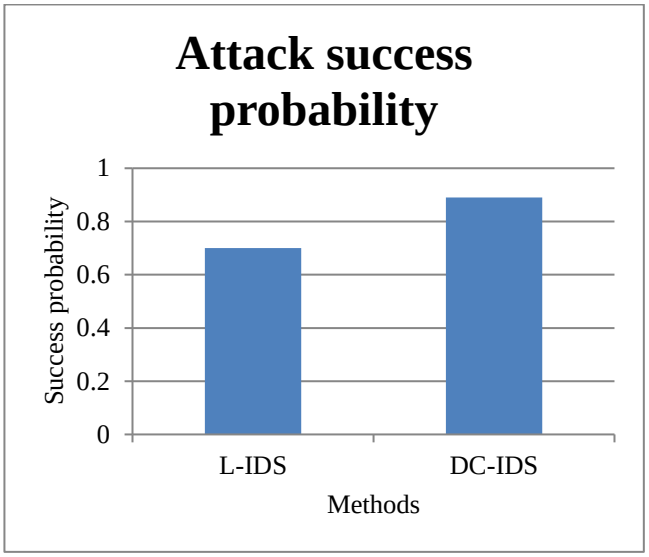

Figure 11. Sybil attack probability comparison

In figure 11, comparison evaluation of the success probability for the proposed and existing methodologies are given. From this comparison it is concluded that proposed method DC-IDSis having better performance than the previous methodologies with accurate detection of attacker nodes.

V.CONCLUSION

In mobile ad hoc networks, for packet dropping attack, binary formed novel swarm optimization based on intrusion detection system is propose in this work. Two types of architectures are described based on IDS architecture and proposed a cat swarm optimization, i.e. cooperative, distributed and local. In detecting packet dropping attack, better performance is exhibited using L-IDS and DC-IDS system as indicated in results. Output in binary form, either 1 or 0 is produced by proposed IDS architecture. Normal pattern are indicated using a binary value 0 and abnormal pattern are indicated using a binary value 1. In network, presence of malicious nodes are indicated using a binary value of 1. In MANETs environments, detection of all kind of attacks can be concentrated in future.

REFERENCES

1. H. Moudni, M. Er-rouidi, H. Mouncif, B. El Hadadi, “Performance analysis of AODV routing protocol in MANET under the influence of routing attacks,” In Electrical and Information Technologies (ICEIT), 2016 International Conference on. IEEE, pp. 536-542, 2016.
2. H. Moudni, M. Er-rouidi, H. Mouncif, B. El Hadadi, “Attacks against AODV routing protocol in Mobile ad-hoc networks,” In Computer Graphics, Imaging and Visualization (CGiV), 2016 13th International Conference on. IEEE, pp. 385-389, 2016.
3. B. Wu, J. Chen, J. Wu, M. Cardei, “A survey of attacks and countermeasures in mobile ad hoc networks,” In Wireless network security, Springer, Boston, MA, pp. 103-135, 2007.
4. C. Perkins, E. Belding-Royer, S. Das, “Ad hoc on-demand distance vector (AODV) routing,” No. RFC 3561, 2003.
5. A. Nadeem, M. P. Howarth, “A survey of MANET intrusion detection & prevention approaches for network layer attacks,” IEEE communications surveys & tutorials, Vol. 15, No 4, pp. 2027-2045., 2013.
6. S. Sen and J. A. Clark, Guide to Wireless Ad Hoc Networks: Chap. 17. Intrusion Detection in Mobile Ad Hoc Networks, pp. 427{454, Springer, 2009.

7. L. A. Zadeh, \Roles of soft computing and fuzzy logic in the conception, design and deployment of information/intelligent systems," in Computational Intelligence: Soft Computing and Fuzzy-NeuroInte- gration with Applications, NATO ASI, vol. 162, pp. 1-9, Springer, 1998.
8. J. Yen, R. Langari, "Fuzzy logic: intelligence, control, and information," Upper Saddle River, NJ: Prentice Hall, Vol. 1, 1999.
9. J. S. Jang, "ANFIS: adaptive-network-based fuzzy inference system," IEEE transactions on systems, man, and cybernetics, Vol. 23, No 3, pp. 665-685, 1993.
10. J. Kennedy, "Particle swarm optimization," In Encyclopedia of machine learning, Springer US, pp. 760-766, 2011.
11. P. Joshi, P. Nande, A. Pawar, P. Shinde and R. Umbare, "EAACK - a secure intrusion detection and prevention system for MANETs," In proceedings of International Conference on Pervasive Computing (ICPC), pp. 1-6, Pune, 2015.
12. Khan, F.A., Imran, M., Abbas, H. and Durad, M.H., "A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks," Future Generation Computer Systems, vol. 68, pp.416-427, 2017.
13. N. Marchang, R. Datta and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1684-1695, Feb. 2017.
14. Shams, E.A. and Rizaner, A., "A novel support vector machine based intrusion detection system for mobile ad hoc networks," Wireless Networks, pp.1-9, 2017.
15. Gurung, S. and Chauhan, S., "A novel approach for mitigating route request flooding attack in MANET," Wireless Networks, pp.1-16, 2017.
16. Huang, M., Ma, Y., Wan, J. and Chen, X., "A sensorsoftware based on a genetic algorithm-based neural fuzzy system for modeling and simulating a wastewater treatment process," Applied Soft Computing, vol. 27, pp.1-10, 2015.
17. Tao Shu and Marwan Krunz, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing
18. S. Sen and J. A. Clark, \A grammatical evolution approach to intrusion detection on mobile ad hoc net-works," in ProceedingsIn of the Second ACM Conference on Wireless Network Security (WiSec'09), pp. 95{102, 2009.
19. D. Sowmyadevi and K. Karthikeyan, "Merkle-Hellman knapsack-side channel monitoring based secure scheme for detecting provenance forgery and selfish nodes in wireless sensor networks," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, 2017, pp. 1-8. doi: 10.1109/ICECCT.2017.8117950
20. C. E. Perkins and E. M. Royer, \Ad-hoc on-demand distance vector routing," in Proceedings of the Second IEEE workshop on Mobile Computer Systems and Applications, pp. 90{100, 1999.
21. S. C. Chu, P. W. Tsai, and J. S. Pan, "Cat swarm optimization," in PRICAI 2006: Trends in Artificial Intelligence. Heidelberg: Springer, 2006, pp. 854-858.
22. Dr. G Maria Priscilla Niyaz Hussain A M J, "A Survey on Various Kinds of Anomalies Detection Techniques in the Mobile Adhoc Network Environment", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), Volume : 3, Issue : 3, pp. 1538-1541, 2018.

AUTHORS PROFILE

NIYAZ HUSSAIN A M J has finished his Bachelor of Computer Applications from Sankara College of Commence & Science, Coimbatore. He has completed his MSc Information Technology from SNR Sons College, Coimbatore. He has been awarded his MPhil in Networking from Bharathiar University during 2012. He was worked as an Assistant Professor in Sri Ramakrishana College of Arts & Science (Formerly SNR Sons College), Coimbatore for past ten years. He is working as an Assistant Professor of Information Technology in Hindusthan College of Arts & Science, Coimbatore. He is currently a regular part - time Research Scholar in Department of Computer Science at Sri Ramakrishana College of Arts & Science (Formerly SNR Sons College), Coimbatore, working towards his Ph.D.

Dr. G Maria Priscilla has finished her M.Sc. degree at Bharathiar University in 1999, she has been awarded M.Phil Degree at Bharathidasan University in 2004 and she has been awarded Ph.D at Mother Teresa University. Her area of interest is Computer Networks, She has 19 years of teaching experience in collegiate service. She is currently working as Head & Professor, Department of Computer Science in Sri Ramakrishana College of Arts & Science (Formerly SNR Sons College), Coimbatore. She has presented & published various papers in international & National conferences.