Trust Aware Intrustion Detection System to Defend Attacks in Manet

Adilakshmi Yannam, G.V.S.N.R.V.Prasad

Abstract*: *Intrusion detection is a most concentrated problem in the MANET environment due to increased intruders who would interrupt the normal transactions. Intrusion detection has been performed in various existing works by adapting the different procedure. In our existing work namely Game Theoretic based Cooperative Intrusion Detection System (GT-CIDS), intrusion attacks that happens in the cooperative way is performed. However this research method failed to prevent the intrusion that is performed by the genuine nodes who are compromised. This is focused in this research method and introduced the method namely Trust and Novel Key based Cooperative Intrusion Detection System (TNK-CIDS). The main goal of this research work is to detect the intrusion attacks happening in the mobile node communication to ensure the successful data transmission without interruption. In this work initially monitoring node for intrusion detection is selected which can detect the malicious activities happening on the environment. This monitoring node selection is performed in terms of trust value where the mobile node with increased trust value would be chosen. After node selection data communication is performed between mobile nodes. In order to increase the security level here the data contents are encrypted where the encryption keys are generated using new secret key generation method. This increases the security level which can protect the data content from the hackers. Finally the involvement of the intruders is detected by finding the variation in the traffic flow which is transmitted between mobile nodes. This is measured by introducing the entropy metrics based on which malicious nodes can be detected. The overall assessment of the research work is conducted in the NS2 simulation environment in terms of intrusion detection ratio and ensured that the proposed TNK-CIDS is better than the GT-CIDS.

Keywords: Intrusion detection, cooperative attacks, trust evaluation, new secret key generation, authentication, entropy measurement.

I. INTRODUCTION

Mobile adhoc network is the group of mobile nodes distributed in the surrounding environment without any base [1]. This is known to be more flexible environment where the mobile nodes can be inserted or removed easily and also it supports the node movement in the efficient way [2]. At the time of data transmission the mobile nodes will generate the self route among the nodes distributed in the environment on their own based on routing requirement. The properties of mobile nodes to join or remove from the MANET make it as dynamic topology [3].

Revised Manuscript Received on April 06, 2019.

Adilakshmi Yannam, Research-Scholar,Department of Computer Science and Engineering,Jawaharlal Nehru Technology Univerisity, Kakinada, A. P. India

G.V.S.N.R.V.Prasad, Professor, Department of Computer Science and Engineering, Gudlavalleru Engineering College, Gudlavalleru, A. P. India

Whenever the nodes attempt to perform data transmission, routing will be initiated where every nodes present in the MANET environment will take their part to form the route path. Multi hop routing plays an important role in forming the multi route path between the mobile nodes to make the data transmission faster and reliable [4]. Different applications that utilize the MANET for different purposed due to their properties such as flexible baseless environment, scalability, etc., The applications where the MANET applied are military, public services, and emergency crisis environments [5].

Data transmission in the MANET environment would get affected by various issues such as security attacks, resource constraints and so on. Here increased security attacks in the MANET environment leads to the regular activity of the data transmission by dropping or losing the data packets. Here the cooperative attacks known to be most dangerous threat in the MANET where nodes present in the environment would cooperate with each other to interrupt the normal data transmission. This cooperating behavior of nodes would interrupt the data transmission by breaking the regular network operations [6]. In this cooperation attacks, the attacker node will compromise the genuine nodes from the information gathered from the packets received. This cooperation attack is most normal in the environment due to the property of MANET nodes where the nodes should cooperate with each other to form the strong route path [7]. In the collection of attacker nodes, genuine nodes might get compromised which needs to be concentrated more at the time of data transmission process to ensure the security level [8]. Detection and prevention of these malicious nodes is a most difficult task where the normal network operations would be affected [9].

In this research work, cooperation attack detection is concentrated to provide the most secured intrusion detection for MANET environment where the data transmission can be done successfully. The main goal of this research work is to introduce the system which can detect and prevent the cooperative attacks such as black hole and gray hole attacks [10]. This is done by integrating the proactive and reactive structure of MANET where the nodes can be established by making cooperating with each other. Here the addresses of the nodes present in the MANET will be gathered to establish the cooperative connection among them. This is done by preventing the malicious nodes to learn about the packet forwarding behavior by learning the RREP packets [11]. In this work, we considered that the alarm would be generated in case of continuous packet dropping ratio when it is transferred from the source node to the destination nodes. This will

be maintained efficiently by triggering the sudden reactive response [12].

The main goal of this research work is to implement the framework which can securely transmit the data packets to the destination nodes with guaranteed security enhancement. This is done by detecting and preventing the cooperative attacks happening on the network with the concern of dynamic topology of the network. This research method ensures the secured data transmission with ensured intrusion detection system.

II. RELATED WORKS

Various research methods have been introduced earlier for ensuring the security level of data communication in MANET. Each research methods adapt the different way of procedures to ensure the guaranteed data transmission. SYNERGY is the one of the method which tries to ensure the security level by dividing the nodes into sub partitions with the help of cooperative key where the nodes will be communicate with each other to guarantee the data transmission [13].

Wadbude et al [14] introduced secured framework to enhance the security while data transmission. This research method attempts to satisfy the security requirements to ensure the secure routing between source and destination nodes, thus the successful data transmission can be guaranteed. The protocol used in this work utilizes the techniques such as hashing, digital signature and security enhancement procedure for the ensured and successful data delivery.

Kuppuswamy et al [15] introduced the new method for intrusion detection namely Digital Signature Scheme for ensuring the security level. This is done by adapting the technique such as block cipher and hill cipher. This method is fundamentally known to symmetric key algorithm. The main contribution of this research work is to guarantee the security level by authenticating the documents successfully. This is done by adding the digital signature in the documents which will be compared then to acknowledge the genuine documents. However this method is most traditional method which might consists of some security issues.

Mamatha et al [16] attempted to detect and prevent the malicious nodes involved in the MANET environment by introducing the semantic security mechanism. This method ensures the guaranteed prevention of packet dropping attacks and the message tampering attacks happening on the network. This security method is known to most strong and tampered method where is more difficult to break down which ensures the high security level. The performance assessment of this research method ensured that the proposed research technique guarantees the detection and prevention of malicious nodes present in the environment.

Agalya et al [17] introduced the novel hybrid techniques which will integrate the working procedure of reactive and proactive architectures by cooperating their working procedures. This method extracts the addresses of the neighbour nodes which cooperate with each other which will act as the bait node for detecting the malicious nodes involved in the environment. Here the malicious nodes are detected by finding the addresses of the malicious nodes form the RREP messages by learning their identities. This method guarantees the ensured security level by learning the addresses of the nodes involved in the data communication.

Jadhav and Patil [18] introduced a method for detecting the DDOS attacks namely objective entropy based method. This method would predict the low rate DDOS attacks happening on the network by learning the different variation of the packets transferred between source and destination nodes. This method is proved to be better than the traditional methods for detecting the DDoS attacks. The main drawback of this method is that variation between the normal and attack traffic predicted is very small which leads to inaccurate intrusion detection. This method tends to have larger false positive rate.

Xiang et al [19] introduced the novel entropy based method to predict the trace back low rate DDoS attacks happening on the network. This method would measure the generalized entropy between the normal traffic and the attacks traffic in order to accurately predict the presence of low rate DDoS attacks. The numerical assessment of this method proved that the proposed method of this work is better than the working procedure of the Shannon entropy. The metrics that are considered in this work for the performance assessment are false positive rate and the distance gap. Here distance gap will be adjusted based on α value to ensure the accurate and reliable prediction of the DDoS attacks.

Bhuyan et al. [20] introduced the lightweight extended-entropy metric-based system whose main goal is to detect and prevent the DDoS attacks happening on the network. This method adapts the IP trace back value which will be measured by learning the extended entropy value. This method would measure the distance between the normal and attack traffic from which entropy value can be learnt efficiently.

III. TRUST AWARE COOPERATIVE INTRUSION DETECTION SYSTEM

Intrusion detection in MANET is a most concentrated research work by different authors to ensure the security level of users when they attempt to transmit their own data. This is concentrated in this work and introduced the method namely Trust aware cooperative intrusion detection system whose main goal is to prevent the intrusion attacks, thus the successful data transmission can be guaranteed. This is achieved in this work by selecting the trustable monitoring node which can monitor and detect the intrusion behavior happening on the network. Here the nodes with higher trust would be chosen for the monitoring purpose. The monitoring node will detect the intrusion behavior by finding the variation in the data which is transmitted by measuring the entropy values. And then secured data transmission is guaranteed by encrypting the data contents before transmission whose encryption keys are selected by using new key generation algorithm. This research work ensures the guaranteed intrusion detection thus the security can be enhanced whose working procedure is explained in detailed in the following sub sections.

3.1.HIERARCHICAL TRUST EVALAUTION FOR BAIT DETECTION

The trust value of the mobile nodes distributed in the environment will be evaluated by considering the multi facets. The main factors that are considered for the measuring the trust level of mobile nodes are communication trust, genuine trust, and information trust. These factors will be calculated for measuring the trust level of the MANET nodes.

3.1.1. COMMUNICATION TRUST

Communication trust $CT_{ij}(T)$is defined as the number of communication happened between the node i and node j within the time period T. This communication included every sending and receiving process of control packets, data packets and so on. It can be concluded that the nodes with more number of communication among them will be considered as trustable node. However there is a chance of involvement of intrusion activities such as bandwidth flooding attack with increased communication. This can be predicted by comparing the number of communication with the threshold value where if the number of communication exceeds the threshold value then trust value of corresponding node will be decreased. This communication trust is calculated by adapting the probability density function which is derived from normal distribution theory. This communication trust value will be normalized within [0, 1] range to predict the number of communication accurately. In this work, undirected weighted graph will be generate for the number of nodes present in the MANET where edge of the graph will be defines the communication between the corresponding nodes and the weight value will defines the number of communication happened. The calculation procedure of communication trust $CT_{ij}(T)$ is given as follows:

$$CT_{ij}(T) = \begin{cases} \left\lfloor 10 \times {w_{ij}}/{\max(w_{ij})} \right\rfloor, j \in G, w_{ij} \le \lambda\mu \\ \left\lfloor 10 \times \exp(-|w_{ij} - \mu|/\theta) \right\rfloor, j \in G, w_{ij} > \lambda\mu \end{cases} \quad (1)$$

Where $\lfloor x \rfloor$➔ highest integer value which is less than or equal to the value of x

μ➔ mean of number of communication happened between node i and node j

$\lambda\mu$➔ communication threshold range value

λ➔ maximum threshold for normal communication

θ➔ Important factor used to adjust the weight values

It is most important to consider the state of mobile nodes which plays an major role in the communication happening between them. Here the communication trust might be varies due to varying state of mobile nodes which is concentrated more in this research work for the accurate communication trust measurement. The weight value should be adjusted in the well defined way with the concern of state value to ensure the accurate communication trust measurement.

3.1.2. GENUINE TRUST OF MOBILE NODES

Genuine trust $GT_{ij}(T)$ is defined as the number of successful and unsuccessful communications happened between node I and node j within the time period T. Here successful communication is defined as the successful delivery of data packets from node j to next hop neighbour node involved in the route path which will be overheard by the node i. The unsuccessful communication is defined as failed data transmission of node j which overheard by node i. This unsuccessful data transmission consists of three cases. Those are

(i) node j failed to transmit the node to the next hop neighbour node involved in the route path within time period T

(ii) node j transmits data to the nodes which are not part of an routing path

(iii) node i doesn't receive any acknowledgement control packets from the node j

Based on these factors number of successful and unsuccessful communication will be measured. It is known that the routing path with intrusion activity would not deliver the data packets correctly which is known to be unsuccessful communication. Thus it can be concluded that node with more number of successful communication tends to higher trust value whereas nodes with more unsuccessful communication tends to have less trust value. Based on this information Genuine trust of node for the time period T can be calculated as like follows:

$$GT_{ij}(T) = \begin{cases} \lfloor 10 \times (s+1)/(s+f+2) \rfloor, \text{when } f = 0 \\ \left\lfloor 10 \times (s+1)/(s+f+2) \times f^{-1/2} \right\rfloor, \text{when } f \ne 0 \end{cases} \quad (2)$$

By using the above equation 2 genuine trust can be calculated accurately. From this equation it can be learnt that the node with more unsuccessful communication tend to have lesser trust value and node with more successful communication tends to have higher trust value. In case of node with no communication will be assigned with trust value as 0.5.

3.1.3. INFORMATION TRUST OF MOBILE NODES

Information trust is defined as the evaluation of trust level of mobile node based on information gathered from the neighbour nodes. The information gathered during routing process would expose more content regarding the data communication from which intrusion attacks can be learnt accurately. For example tampering attacks are most frequent attack which can be learnt from the routing information. To evaluate this information trust, initially data routing information will be observed and collected for the particular time period. This information will be analysed for the abnormal actions which can be found by using distance measures. In most of the tradition applications Euclidean distance metric is utilized for the information trust evaluation. In this trust evaluation process, information gathered from the multiple nodes should be concentrated for the trust evaluation where information observed by single node would not expose all routing information. The calculation procedure of information trust $IT_{ij}(T)$ for the time period T is given as follows:

$$TT_{ij}(T) = \lfloor 10 \times \exp(-ED_{ij}) \rfloor \quad (3)$$

$$ED_{ij} = \left(\sum_{k=1}^{d_m} (x_{ik} - x_{jk})^2 \right)^{1/2} \quad (4)$$

Where ED_{ij}➔ Euclidean distance measure which will calculate the distance between the information gathered from the node i and j.

d_m➔ multi facets of observed information

$x_{ik}$and x_{jk}➔ average of k dimension data observed by node i and j

The above equation 3 is used to measure the information trust level of mobile node which guarantees the accurate trust evaluation of the mobile node based on their routing behaviour. These information are utilized to measure the overall trust level of mobile nodes based on which optimal monitoring node which is having lesser chance of intrusion attacks.

3.1.4. MOBILE NODE TRUST EVALUATION

The overall trust level of mobile node j can be calculated by using the information gathered from the node i. Simply it is aggregation trust values of communication, genuine and information which ensures the accurate trust evaluation. The overall trust evaluation of the mobile nodes is mentioned in the following equation 5

$$MNT_{ij} = \lfloor \alpha CT_{ij} + \beta GT_{ij} + (1 - \alpha - \beta) IT_{ij} \rfloor \quad (5)$$

where α, β and $1 - \alpha - \beta$➔ weight values of mobile nodes in terms of communication, genuine and information trust value

Based on this trust value, monitoring node selection will be done. The node with higher trust will be elected as monitoring node. This node will be utilized for the detection of the malicious nodes present in the MANET environment. In this work authentication is performed by using the new secret key generation where the secured data transmission can be guaranteed along with guaranteed malicious node detection.

3.2. NEW SECRET KEY GENERATION FOR SECURED DATA TRANSMISSION

Encryption in the network is performed by encrypting the data contents by using secret keys. In the network multiple nodes, it is required to generate the secret key (SK) for every nodes. This key will be utilized by the tradition encryption algorithm to encrypt the data contents, thus privacy and security of the data contents can be generated. Thus the secret key plays an important role in the security of data contents which needs to be generated with more concern. This research work tends to generate the more secured secret keys by introducing the method namely new secret key generation algorithm. The main goal of this research work is to identify the malicious attacks based on modification present in the sequence number of control packets. In this work sequence of encryption will be carried out to secure the data content from intruders. Here each receiver node will apply the secret key to the packet received and that corresponding encrypting packet will be forwarded to next. This node will omit the packet received from the previous nodes to secure the data transmission. This process will be repeated in every receiver to ensure the security level of packet transmission.

In this work encryption is performed by using RSA algorithm where public keys for encryption will be generated based on two larger prime numbers and auxiliary value. Here prime number known to be secret for others and the receivers would utilize the pubic keys for the encryption purpose. Here security is guaranteed where only the user with prime values can decrypt the data contents. The working procedure of RSA encryption algorithm is given as follows:

1. Select the two unique large prime numbers s and t

To ensure the security level, these prime values are chosen randomly with different length.

2. Generate modular value MV = st.

Where MV is known to be modulus value of secret key pair whose length is represented as bits

3. Generate private value $\lambda(MV) = lcm(\lambda(s), \lambda(t)) = lcm(s-1, t-1)$

where λ ➔ Carmichael's totient function

4. Select the random integer value f where $1 < f < \lambda(MV)$ and $gcd(f, \lambda(MV)) = 1$; i.e., f and $\lambda(MV)$ are coprime.
5. Find d as $d \equiv e^{-1} \pmod{\lambda(MV)}$; i.e., d is the modular multiplicative inverse of f modulo $\lambda(MV)$.

Here f is known to be public key and the d is known to be secret key.

Encryption: Encryption is performed by using the public key f. Initially the plain text M will be transformed into integer value m which will be encrypted with f to generate the cipher text c. This process is given below:

$$c \equiv m^f \pmod{MV} \quad (6)$$

Decryption: Decryption is performed by using the private key d which is performed as like follows:

$$c^d \equiv (m^f)^d \equiv m \pmod{MV} \quad (7)$$

By applying the above equation 7 original data without any modification can be retained.

3.2.1. SHARING KEY (ShK) CREATION

Here monitoring nodes are responsible for finding the intrusion activities such as collaborative dropping attacks happening on the network. This is done by sharing the secret keys securely by using which geunity of mobile nodes can be checked efficiently. At the time of data transmission, sender nodes will generate random number and will share it with the destination node through some secured shortest path. With the help of this random number, secret keys will be generated by both source and destination nodes. At the time of data arrival each node will verify its secret keys from the header information encrypted data before accepting and forwarding them. Thus the secured data transmission can be guaranteed. In this work Artificial Bee Colony algorithm is utilized for secured secret key generation with the help of

personal identity information of users.

Algorithm 1 ABC optimization approach

1: Initialization Phase
2: **repeat**
3: Employed Bee Phase
4: Onlooker Bee Phase
5: Scout Bee Phase
6: Memorize the best solution achieved so far
7: **until** (Cycle = Maximum Cycle Number or a Maximum CPU time)

Figure 2: key selection method

The processing steps of ABC algorithm which is utilized for key selection is shown in the figure 2 and its processing flow is given below:

1. Initialize population: For the key selection process, we need to generate the food sources which consist of pool of keys. Here our main goal is to pick the food source with lowest possible number of keys. In this work M number of food sources will be generated where M is the number of available secret keys.
2. Present a key subset of sustenance sources to the classifier and use exactness as wellness: the key subset of every nourishment source is submitted t o the classifier, and precision is put away as the wellness of nourishment source.
3. Decide neighbors of picked nourishment supplies by utilized honey bees abuse alteration rate (MR) parameter: each utilized honey bee visits a sustenance source and investigates its neighborhood. For key choice, a neighbor is made from the bit vector of the first sustenance source. In the essential adaptation of basics rule, the area is sketched out by playing a small low irritation in minor partner degree enhancement parameter that makes union slower.

In the key choice, the streamlining parameters are spoken to by the bit vectors and their bother is performed by an annoyance recurrence or MR. For each situation of the bit vector or key, an arbitrary and uniform number R I is produced in the range somewhere in the range of 0 and 1. In the event that this esteem is lower than the annoyance parameter MR, the key is embedded into the subset, that is, the vector esteem at that position is loaded up with 1. Something else, the estimation of the b it vector isn't adjusted. This is communicated in Equation 8:

$$X_I = \begin{cases} 1 \text{ if } R_i \\ x_i \text{ otherwise} \end{cases} < MR \quad (8)$$

Where xi is the position I in the bit vector. After chose the ideal key this will be utilized as a common key and it will be shared just to the both sender and collector so if the aggressor hack oneself key encryption technique to hack the information this shared key strategy will be exceptionally valuable in assault recognition.

3.3. MALICIOUS NODE DETECTION BASED ON ENTROPY MEASURES

To separate the vindictive hub from real hub at the season of information correspondence entropy estimation is performed. In light of entropy esteems noxious hub location is ensured. The entropy measurements that are considered in this work are, "traffic stream metric, throughput metric, data transfer capacity designation measurements, transmission capacity deviation metric, Generalized Entropy (GE), Generalized Information Divergence (GID) measurements, Projected Entropy".

Traffic stream metric: This measurement figures the complete number of correspondences occurred in the system when we introduce the changed firecol framework in the system. The all out traffic stream at the worldwide IPDS is given by,

$$f(G_m) = \sum_{m=1}^{i} f_{out}(L_m) \quad (9)$$

wheref_{out}(Lm) is the total of all cordial traffic stream turning out from all the nearby IPDS. All work customer hubs needs to go through the neighborhood IPDS to send and get messages. Along these lines, the all out traffic stream at the neighborhood IPDS is acquired by including the complete approaching and active traffic stream at each work customer hub. The all out traffic stream at the nearby IPDS is given by,

$$f(L_m) = \sum_{n\in N} f_{in}(n) + \sum_{n\in N} f_{out}(n) \quad (10)$$

where f_{in}(n) is the customer hub's approaching traffic and f_{out}(n) is the customer hub's active traffic. The absolute traffic stream at the work customer hubs is given by,

$$f(n) = \sum_{c=1}^{i} f_c(n) + \sum_{d=1}^{i} f_d(n) \quad (11)$$

where f_c(n) is the customer hub's control stream traffic and f_d(n) is the customer hub's are the control stream traffic and information stream traffic at the work customer hubs. The control stream traffic at the work customer hub n is given by,

$$f_c(n) = f_{cin}(n) + f_{cout}(n) \quad (12)$$

wheref_{cin}(n) is the customer hub's approaching control stream traffic and f_{cout}(n) is the customer hub's active control stream traffic. The information stream traffic at the work customer hub n is given by,

$$f_d(n) = f_{din}(n) + f_{dout}(n) \quad (13)$$

wheref_{din}(n) is the approaching information stream traffic at the customer hub and f_{dout}(n) is the active information stream traffic at the customer hub. The complete number of control messages traded between the work customers, the neighborhood IPDS and the

worldwide IPDS are required to compute the correspondence overhead.

Throughput metric: The proposed framework ensures a base throughput of λ and all customer hubs ought to follow inside this throughput. i.e.,

$$\sum_{n\in N} b_n \leq \lambda \quad (14)$$

The throughput is influenced by the division of data transfer capacity assigned to every customer hub. The customer hubs for which the data transmission is assigned through the transfer speed allotment convention are considered for accomplishing remote work arrange throughput.

Transmission capacity portion measurements: bn is the division of transfer speed dispensed to every customer hub n∈N and $B_r = B - B_{mb}$ where B is the all out data transfer capacity apportioned to the system, B_{mb} is the data transfer capacity allocated for the neighborhood and worldwide IPDS and B_r is the data transfer capacity assigned to each work customer hubs who joins the system. The data transfer capacity imperative is given by,

$$b_n \leq B_r/N \quad (15)$$

Transfer speed deviation metric: The data transfer capacity deviation metric is given by,

$$\text{dev}\,(b_n, b_{n'}) \leq \varpi \quad (16)$$

Every customer hub is apportioned a transfer speed bn inside the system and they are allowed to use just their allocated data transmission. Hubs neglecting to utilize bn may have been digressed to bn'. The deviation of bn and bn' must not surpass ϖ whose esteem is 0.1. On the off chance that the deviation surpasses ϖ, at that point it prompts dismissal of that customer hub.

Summed up Entropy (GE): Entropy was acquainted with measure the vulnerability of an occasion related with a given likelihood conveyance X. The formal meaning of entropy as far as a discrete variable X, with conceivable results x1, x2, ...,xn can be characterized as:

$$H(x) = \sum_{i=1}^{n} p(x_i)\log_2 \frac{1}{p(x_i)} = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i) \quad (17)$$

where p(xi) = Prob(X = xi) is the likelihood of the ith result of X. A summed up entropy (GE) can be characterized as:

$$H_\alpha(X) = \frac{1}{1-\alpha}\log_2\left(\sum_{i=n}^{N} p_i(\alpha)\right) \quad (18)$$

By changing the α request, diverse sorts of entropy esteems can be acquired. At the point when α = 0, it demonstrates the most extreme estimation of the created data. Yet, when α = 1, it very well may be communicated as: $H_1(x) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$, which is named as Shannon Entropy (Esh).

The estimation of α increment the deviation between various likelihood dispersion when contrasted with (Esh) when α > 1. In high likelihood occasions the GE can create preferred and exact outcome over (Esh).

Summed up Information Divergence (GID) measurements: Let's two diverse likelihood dissemination are P = (p1, p2, ...,pn) and Q = (q1, q2, ..., qn). A summed up data uniqueness (GID) can be inferred as:

$$D_\alpha(P\|Q) = \frac{1}{1-\alpha}\log_2\left(\sum_{i=1}^{N} p_i^{\alpha} q_i^{1-\alpha}\right), \text{where } \alpha \geq 0 \quad (19)$$

Anticipated Entropy: According to for stochastic procedures the entropy rate H (x) of two irregular procedures are same

$$H(X) = \lim_{n\to\infty}\frac{1}{n}H(x_1, x_2, .., x_n) \quad (20)$$

In the event that H(x) <=th2, th2 is the threshold value which is taken as 0.5 in our work, Mark the stream as assaulted, raise a last alarm, dispose of the assault stream.

Assault discovery executive doles out a limit an incentive for bundles. Gather traffic stream in schedule vacancy. Compute Entropy H(x) for bundles, by methods for IP address, ports and stream measure as information. From this, standardized entropy is found. At long last contrast standardized entropy and that of doled out edge esteem. Whenever Normalized Entropy is littler than limit entropy at that point, the got parcel is from illicit client else examination is done against another edge esteem. For this situation bigger esteem reasons that parcel is gotten from lawful client. Setting a limit esteem isn't a simple errand. Edge esteem for the most part relies upon false positive rate.

IV. RESULTS AND DISCUSSION

In this area, the execution investigation of the proposed system is done in the NS2 reproduction condition in associate with the execution measurements for the TNK-CIDS with the past existing GT-CIDS. The correlation evaluation is performed between TNK-CIDS and GT-CIDS.

The reproduction esteems are appeared in the accompanying table 1, 2 and 3.

Table 1. Simulation comparison values in terms of simulation time

Simulation time in ms	Performance Metrics					
	Packet delivery rate in bps		Delay in ms		Throughput in kbps	
	GT-CIDS	TNK-CIDS	GT-CIDS	TNK-CIDS	GT-CIDS	TNK-CIDS
10	79.878	89	586.89	489	104.26	125
20	80.077	91	586.89	475	99.73	111.39
30	80.021	91.023	586.89	469.56	99.73	135
40	80.059	93.2	586.89	469.56	104.26	129.56
50	79.98	93.56	586.89	469.56	104.26	131.47
60	79.979	94.82	586.89	469.56	99.73	145
70	79.947	94.99	586.89	469.56	99.73	135
80	80.039	96.7	586.89	469.56	104.26	129.84
90	80.005	96.97	586.89	469.56	104.26	129.84
100	79.923	96.97	586.89	469.56	99.73	131.26

Simulation metric values

Simulation time in ms	Performance Metrics			
	False positive Rate		Detection Rate	
	GT-CIDS	TNK-CIDS	GT-CIDS	TNK-CIDS
2	10	65	25	29
4	20	74	48	51
6	85	79	100	121
8	200	156	175	182
10	300	189	260	275
12	350	240	320	335
14	400	350	375	381
16	440	370	425	426
18	470	410	460	460
20	500	435	505	516

4.1. PACKET DELIVERY RATE

Every hub advances bundles by using the steering conventions. The parcel conveyance rate is a level of the bundles acquired to those sent and is registered as such:

$$PDR = \frac{\sum_{i=0}^{n} PR_i}{\sum_{0}^{n} PS_i} \quad (21)$$

Where PR → packets received.

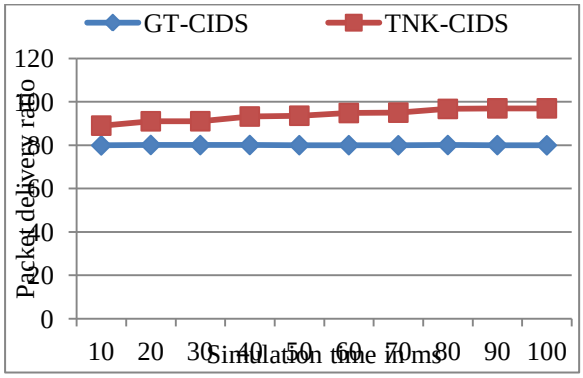

Figure 1. Packet Delivery rate

The PDR of the methodology that is to state GT-CIDS and TNK-CIDS are related together. Subordinate upon this the result of TNK-CIDS shows the upgraded execution contrasted with the other two methodologies as expressed by the figure 1. From this examination it is demonstrated that the proposed strategy TNK-CIDS accomplishes 17.29% expanded bundle conveyance proportion than the current GT-CIDS technique.

4.2. AVERAGE DELAY

The time contrast in the midst of the present parcels landing in and the earlier bundle internal bound is depicted as the normal deferral created at a hub. It is thought by the resulting condition 2.

$$\text{Average Delay} = \frac{\sum_{i=0}^{n} PRT - PST}{n} \quad (22)$$

Where PRT → packets received time and PST → packets sent time

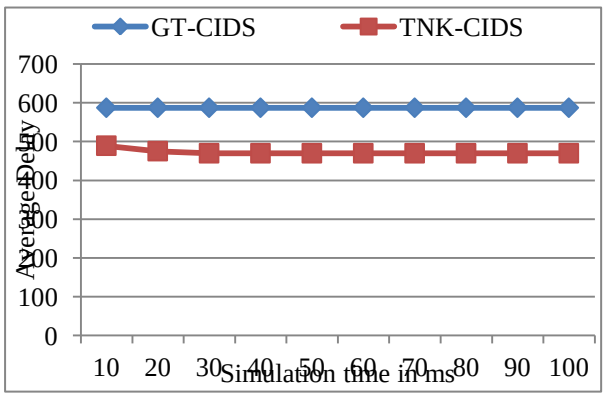

Figure 2. Average Delay

The normal deferral of the procedure called GT-CIDS and TNK-CIDS are coordinated up together. Subordinate upon this the result TNK-CIDS shows the upgraded execution contrasted with the other two systems as showed in the figure 2. The proposed strategy TNK-CIDS achieves 19.56% decreased postponement than the current GT-CIDS technique.

4.3. THROUGHPUT

It is one among the dimensional parameters of the system that gives the division of the strength used for profitable transmission picks an objective toward the beginning of the reproduction that is the data whether the information parcels are properly sent to the objective or not.

$$\text{throughput} = \frac{\text{number of packets moved}}{\text{total number of packets}} \quad (23)$$

This is exposed in figure 4.

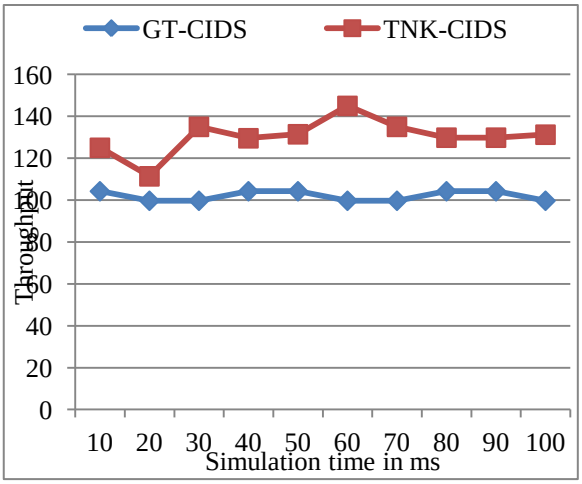

Figure 3. Throughput

The throughput of various strategies in reenactment condition from the source to each objective hub is uncovered in Figure 3. Thus it demonstrates that the TNK-CIDS would yield the improved results when coordinated with the standard GT-CIDS indicates expanded throughput execution. From this recreation diagram it is demonstrated that the proposed technique TNK-CIDS accomplishes 27.78% expanded throughput than the current strategy GT-CIDS.

4.4. FALSE POSITIVE RATE

In measurements, when playing out different examinations, a bogus positive proportion (or false caution proportion) is the likelihood of dishonestly dismissing the invalid theory for a specific test. The bogus positive rate (or "false caution rate") as a rule alludes to the anticipation of the bogus positive proportion. The bogus positive rate is

$$\frac{FP}{N} = \frac{FP}{FP + TN} \quad (24)$$

Where FP is the number of false positives, TN is the number of true negatives and N=FP+TN is the total number of negatives.

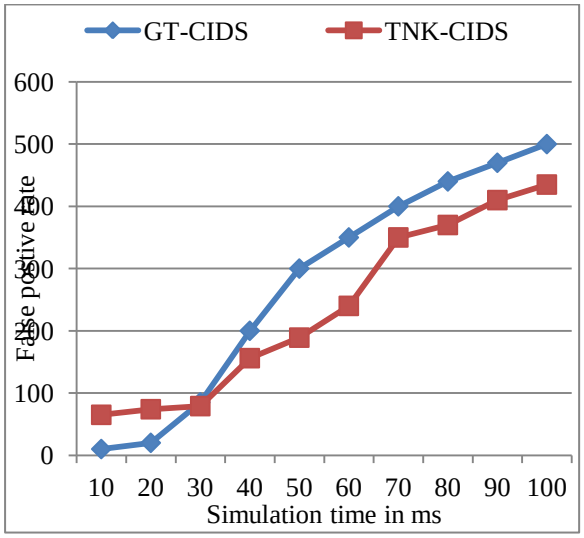

Figure 4. False Positive rate comparison

The false positive rate of various systems in recreation condition from the source to each objective hub is uncovered in Figure 4. Therefore it demonstrates that the TNK-CIDS would yield the upgraded results when coordinated with the standard GT-CIDS indicates lesser false positive rate execution. From this reproduction examination it is demonstrated that the proposed strategy TNK-CIDS accomplishes 14.66% less false positive rate than the current GT-CIDS technique.

4.5. ATTACK DETECTION RATE

Assault discovery rate is characterized as the proportion of assaults identified for the timeframes over the complete number of assaults occurring on the systems. Level of identification rate (DR) additionally can be determined dependent on disarray framework table by utilizing the accompanying recipe:-

$$DR = \frac{TP}{(TP + TN)} \times 100\% \quad (25)$$

Where

TP = amount of attack when it actually attack

TN = amount of normal detect when it actually normal

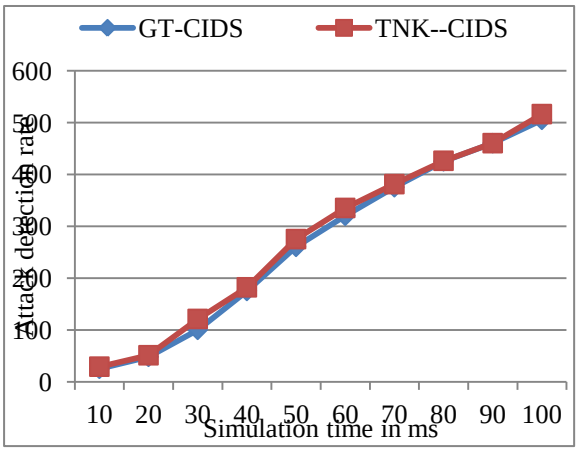

Figure 5. Attack detection rate

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The assault location rate of various methods in reproduction condition from the source to each objective hub is uncovered in Figure 5. Thus it demonstrates that the TNK-CIDS would yield the improved results when coordinated with the standard GT-CIDS indicates expanded assault identification rate execution. From this recreation correlation it is demonstrated that the proposed strategy TNK-CIDS achieves 3.08% expanded recognition rate than the current technique GT-CIDS.

V. CONCLUSION

In this work, optimal monitoring node selection is performed based on trust values in order to avoid the compromised attacks. The trust level of nodes is measured by using hierarchical trust evaluation procedure where any node present in the environment can decide their trust level. And then data communication is performed in the encrypted format to perform the authentication process where encryption is done by using new secret key generation. After authentication data communication will be performed. Here to differentiate the malicious node from genuine node at the time of data communication entropy measurement is performed. Based on entropy values malicious node detection is guaranteed. The overall evaluation of the research work is conducted in the NS2 simulation environment from which it is proved that the proposed research method tends to provide better performance than the existing methods.

REFERENCE

1. Singh, A. V., &Chattopadhyaya, M. (2015, September). Mitigation of DoS attacks by using multiple encryptions in MANETs. In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-6). IEEE.
2. Darabkh, K. A., &Judeh, M. S. (2018, June). An Improved Reactive Routing Protocol over Mobile Ad-hoc Networks. In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 707-711).IEEE.
3. Fakhfakh, F., Tounsi, M., Mosbah, M., Méry, D., &Kacem, A. H. (2017, May). A formal approach for maintaining forest topologies in dynamic networks.In International Conference on Computer and Information Science (pp. 123-137).Springer, Cham.
4. Umar, M. M., Mehmood, A., & Song, H. (2016). SeCRoP: secure cluster head centered multi-hop routing protocol for mobile ad hoc networks. Security and Communication Networks, 9(16), 3378-3387.
5. Negra, R., Jemili, I., &Belghith, A. (2016). Wireless body area networks: Applications and technologies. Procedia Computer Science, 83, 1274-1281.
6. Deny, J., Kumar, A. S., Sundarajan, M., &Khanna, V. (2017, February). Defensive against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. In 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) (pp. 1-5).IEEE.
7. Desai, A. S., &Gaikwad, D. P. (2016, December). Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA.In 2016 IEEE international conference on advances in electronics, communication and computer technology (ICAECCT) (pp. 291-294).IEEE.
8. Sharma, R., & Grover, J. (2015, September). Mitigation of byzantine attack using enhanced cooperative bait detection and prevention scheme (ECBDPS). In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-6). IEEE.
9. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. IEEE systems journal, 9(1), 65-75.
10. Nandhini, M., Sathya, J., Sundaridevi, T., Sivaprakash, G., Jaya, J., &Premalatha, P. (2016). Detecting and preventing malicious nodes using cooperative bait detection scheme. Front. Curr. Trends Eng. Technol, 1, 28-36.
11. Jan, Z., & Sharma, N. (2016). Detection and Avoidance of Black Hole Nodes in MANETs. International Journal of Engineering Science, 2564.
12. Aggarwal, R. (2018). A Survey to Improve the Network Security with Less Mobility and Key Management in MANET.
13. Sun, J., Chen, X., Zhang, J., Zhang, Y., & Zhang, J. (2014, April). SYNERGY: A game-theoretical approach for cooperative key generation in wireless networks. In IEEE INFOCOM 2014-IEEE Conference on Computer Communications (pp. 997-1005).IEEE.
14. Wadbude, D., &Richariya, V. (2012). An efficient secure AODV routing protocol in MANET. International Journal of Engineering and Innovative Technology (IJEIT) Volume, 1, 274-279.
15. Kuppuswamy, P., Appa, P. M., & Al-Khalidi, D. S. Q. (2012). A New Efficient Digital Signature Scheme Algorithm based on Block cipher. IOSR Journal of Computer Engineering (IOSRJCE), 7(1), 47-52.
16. Mamatha, G. S., & Sharma, S. C. (2010). A highly secured approach against attacks in MANETS. International Journal of Computer Theory and Engineering, 2(5), 815.
17. Agalya, A., Nandini, C., &Sridevi, S. (2015). DETECTING AND PREVENTING BLACK HOLE ATTACKS IN MANETS USING CBDS (Cooperative Bait Detection Scheme). International Journal of Modern Trends in Engineering and Research (IJMTER), 2(04).
18. Jadhav, P. N., &Patil, B. M. (2013). Low-rate DDoS attack detection using optimal objective entropy method. International Journal of Computer Applications, 78(3).
19. Xiang, Y., Li, K., & Zhou, W. (2011). Low-rate DDoS attacks detection and traceback by using new information metrics. IEEE transactions on information forensics and security, 6(2), 426-437.
20. ELDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric

AUTHORS PROFILE

AdilakshmiYannam is a research scholar at the Department of Computer Science and Engineering at the JNTUK. She received M.Tech Degree in Computer Science and Engineering from JTNUK. Her research interest cover the SecurityIssues in MANETs with over 20 publications.

Dr.G.V.S.N.R.V.Prasad is a Professor & Vice Principal at the Gudlavalleru Engineering college, Gudlavalleru.He is also Ph.D Candidate at the University of JNTUK.,where he futhere research on Big Data and Analytics. He is member of CSI. His research interest cover the Data Mining and Analytics with over 50 publications.