International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Penalty Based Reliable Cooperative Intrusion Detection System for Mobile Adhoc Network Environment

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

Abstract*: Intrusion detection is the process of finding the malicious behaviour happening in the network to enhance the network performance. This is the most focused research by various researchers to ensure the secured network to the users for increasing their satisfaction level. This is achieved in the previous work by introducing the method namely Cooperative intrusion detection system (CIDS). However this research method doesn't focus on selfish node presence which might affect the overall intrusion detection process. There is a chance of that monitoring node also can act as selfish node. This is resolved in the proposed work by introducing the method namely Penalty based Reliable Cooperative Intrusion Detection System (PR-CIDS). In this work, initially monitoring nodes are selected optimally by using modified artificial bee colony algorithm through which intrusion detection will be performed. Here intrusion detection is performed based on variation in the forwarded traffic. In order to avoid the selfish node presence, in this work unique secret keys are generated for each monitoring node by using which intrusion decision will be encrypted and then send to the third party node. Here third party node will authenticate the node and then will utilize the intrusion information to make the final decision. Third party node plays more important role in making the intrusion decision. Thus the most suitable third party node is selected by using Hybrid Ant colony with Genetic method. Based on this decision, penalty will be assigned to the selfish monitoring nodes. The overall evaluation of the research work is done in the NS2 simulation environment to prove their performance improvement.

Keywords: Penalty, Intrusion decision, cooperative decision making, third party node, monitoring nodes.

I. INTRODUCTION

Mobile adhoc network is the disconnected nodes with wireless communication to share the information [1]. Data sharing in the mobile adhoc network is more difficult task due to their non connectivity nature which should be focused more to ensure the reliable and successful data transmission [2]. Data sharing in MANET plays more critical role where there is no centralized node monitor the data transmission behaviour [3]. It is required to focus towards the reliable and successful data transmission in the wireless MANET which is effective in terms of reduced cost for equipment storage [4]. However successful data transmission in MANET will get affected by different factors [5]. One of the more frequently occurred factors is the presence of intruders who will interrupt the normal packet transmission behaviour to corrupt or steal the information present in the data [6]. Intrusion detection plays a more important role in the mobile adhoc network due to its infrastructure less nature [7]. There is a possibility of occurrence of various intrusion attacks in different forms which is more difficult to predict. The presence of intrusion activities will affect the normal data transmission behaviour which might lead to entire network failure [8]. Thus it is very essential to focus on prediction of intrusion activities. Intrusion detection is the most complex process which is focused by various researchers. An intrusion activity initiated by the malicious nodes who resides within the genuine network environment is more difficult task which needs to be done with more concern [9]. Simply intrusion activities initiated by the selfish nodes are more difficult to predict where it will compromise the genuine node information based on which communication will be performed. Cooperative intrusion detection is the better solution to detect the intrusion activities initiated by the selfish nodes [10]. In this intrusion detection process, decision about intrusion activity will be taken by cooperatively working with multiple nodes present within the environment. Cooperative intrusion detection is defined as the process of communicating cooperatively to make intrusion detection decision [11]. Cooperative intrusion detection process requires communication with the multiple data nodes which would cause increased computation overhead [12]. Thus it is required to take intrusion decision cooperatively with reduced computation overhead. Another problem frequently occurs in the intrusion detection activity is their continuous regeneration by not taking any punishment actions. Upon detecting the intruders, it is required to provide the punishment penalty to make sure the prevention from those intruders in the further data transmission processes [13]. This penalty decision needs to be taken with more concern to avoid the wrong decision which might lead to entire network performance degradation. This is focused in this research work by introducing the method namely penalty based reliable cooperative intrusion detection system. The main goal of this research work is to achieve the successful data transmission with increased network performance. This is achieved by introducing the various research techniques that can ensure the successful data transmission with increased network performance.

Manuscript published on November 30, 2019.
* Correspondence Author
Adilakshmi Yannam *, Research Scholar, CSE Department, JNTUK, Kakinada, India.
Dr.G.V.S.N.R.V. Prasad, CSE Gudlavalleru Engineering College, Gudlavalleru, India.

II. RELATED WORK

Abusitta et al [14] attempted to detect the intrusion activities happening on the cloud environment by introducing the deep learning network. This method tries to find the intrusion activities in the cooperative way to ensure the security level. This research work makes use of the historical feedbacks to ensure the successful decision outcome. This research work also considers the feedback to make sure the accurate decision making outcome. Hassanzadeh et al [15] introduced the resource constrained cooperative intrusion detection process which attempts to predict the intrusion activities lying in the environment with lesser computation cost and overhead. This is achieved by utilizing the multi objective problem formulations such as genetic algorithm. This work predicts the node as intruders in terms of small variation found in the daily fitness prediction value. Hajiheidari et al [16] analysed the role of intrusion detection techniques in the Internet of Things. IoT seems to increased in popularity due to its support more innovative and technological improvements. Along with the popularity improvement, security issues will also be increased considerably which needs to concerned more for the better secured environment. This research work provides the overview of different kind of attacks that are happening on the network and role of IDS system in the IoT. Wu et al [17] focused on the cyber industries whose main goal is to predict the frequent of intrusion activities happening on the network. This research work attempted to predict the correlation between the different cyber scenarios and the intrusion activities. In case of presence of intrusion activities, this research method attempts to generate the alert signal to the cyber security system, thus the proper actions can be taken in time. Here alert is forwarded with the help of intrusion detection message exchange format to ensure the reliable and immediate intrusion detection.Halder et al [18] also attempted to implement the intrusion detection system as like Wu et al [17] in the internet of things. This is done by implementing the methodology called the Gaussian based energy efficient intrusion detection system. This research work tends to consider the more network parameters to ensure the fast and accurate detection of intrusion activities. The overall evaluation of the research work is done in the network with many intruders based on which security level is enhanced. Jiayan et al [19] introduced the deep learning network to perform the intrusion detection process. The main goal of this research work is to enhance the security level of vehicles whose traffic information will be communicated with other nodes for the traffic decision making process. This research work attempts to reduce the vulnerability happening on the real time traffic analysis by preventing the intruders from accessing the vehicle state information. Han et al [20] adapted the game theory approach for the accurate intrusion detection outcome. This is improvised by hybridizing it with the auto regression model to ensure the error free accurate decision about the presence of intrusion activities. In this work defence rules are also generated to punish the intruders who are predicted with the help of neighbourhood information. The main aim of this research work is to perform the intrusion detection process with reduced energy consumption. Loukas et al [21] analysed the various rules and methods introduced for the intrusion detection purpose which is integrated in the vehicles. The main goal of this research work is to provide the overview of different intrusion detection methodologies that provide better outcome in the vehicular networks. This is done in different time period under consideration of different structural factors to make sure the accurate intrusion detection. This analysis work provides clear description of different classification methodologies that ensures the accurate detection of intrusion detection

III. PENALTY BASED COOPERATIVE INTRUSION DETECTION SYSTEM

In this research work, cooperative intrusion detection is performed with the concern of detecting the intruders accurately with reduced computation overhead and complexity. And also this research work tends to reduce the frequent intrusion attacks happening in the network by introducing the new method namely Penalty based Reliable Cooperative Intrusion Detection System (PR-CIDS). In this work, initially optimal monitoring nodes are selected based on trust and energy using modified ABC algorithm. Intrusion detection is done based on varying traffic patterns. And then separate key generation is done for the individual monitoring nodes to avoid the selfish or malicious node involvement. Trustable Third party node is selected for final decision making about intrusion detection – Hybrid ant colony with genetic method. Based on this decision penalty is given and as well rewards are given.

3.1. OPTIMAL MONITORING NODE SELECTION USING MODIFIED ARTIFICIAL BEE COLONY ALGORITHM

In this work, initially monitoring nodes are selected optimally by using modified artificial bee colony algorithm through which intrusion detection will be performed. In this work monitoring nodes plays biggest role which will monitor the ongoing data transmission and will predict the presence of intrusion activities. Thus monitoring nodes should be more efficient one with the capability of standing out for long time until data transmission completed. Particularly energy efficiency of the monitoring node should be better to support the long life and complete monitoring outcome. The node with more energy will be elected as monitoring node. Thus the final intrusion detection decision can be made effectively. In this work, monitoring node selection is done by using Modified Artificial Bee Colony algorithm (MABC). Generally artificial bee colony algorithm is based on the honey foraging behaviour of bees. This work might lack in its performance by searching only local solution. In case of honey lacks, this work would not support the new solution prediction. Thus in this work modified artificial bee colony algorithm is utilised which will chose the replacement monitoring node immediately with the performance degradation in the current monitoring nodes. In this work fitness value of MABC is taken as energy consumption. Energy consumption of the each node in the MANET will be calculated periodically to update the current energy status. The energy consumption of each node is calculated by using following equation 1 and 2.

$$E = \sum_{i=1}^{m} (P^s . t) \quad (1)$$

$$E \geq \alpha . \left(\sum_{i}^{m} d_i^2 + b^2 \right) . t \quad (2)$$

Where

m➔ total number of nodes

P^s ➔ transmitting power from the source node

t ➔ time

d ➔ distance between monitoring node and other nodes

b ➔ distance between monitoring node and third party node

α➔ energy constant

E ➔ transmitted energy level

Based on this calculated fitness value, most optimal monitoring node will be chosen. The pseudo code of monitoring node selection using MABC is given below:

Pseudo code: MABC based monitoring node selection

1. Initialize size of swarm as S, dimensionality as N

2. Initialize population X_i where i =1... SN

3. Begin

4. For every employed bee

5. Measure the velocity to generate new solution using equation 3

$$v_i = x_{ij} + \theta_{ij}(x_{ij} - x_{kj}) \quad (3)$$

6. Measure fitness using equation 1 and 2

7. Run Greedy selection

8. For every onlooker bee

9. Select the node x_i based on population

10. Generation new solution v_i

11. Run greedy selection

12. If any node is present this is not processed

13. Replace by using new solution using equation 4

$$x_j^i = x_{min}^j + rand(0,1)(x_{max}^j - x_{min}^j) \quad (4)$$

14. Repeat until end criterion met

By using the above equation, monitoring node will be chosen. The selected monitoring node will be utilized then for the intrusion detection.

3.2. INTRUSION DETECTION BASED ON TRAFFIC VARIATION

In this work intrusion detection is performed based on variation in the forwarded traffic. Each monitoring node in particular region will monitor the data transmission happening over there and intrusion detection will be performed. In this work SNORT rules are adapted for the accurate intrusion detection. Basically SNORT rules are defined as light weight intrusion detection system. This works based signature generated over the transmitted traffics. It enables users to generate signature over the each transmitted packet in the flexible way. However signature also plays more important role along with rules in intrusion detection process. Sample snort rule signature is given below:alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-CGI finger access"; flow:to_server, established; uricontent:"/finger"; nocase; reference: arachnids,221; reference:cve,1999-0612; reference:nessus,10071; class type: attempted-recon; sid:839; rev:7;)This SNORT will generate signature over the network traffic which will then be stored in the database. These stored rules will be utilized in the future to make intrusion detection outcome. Basically SNORT rules tend to have two components namely chain header and the chain options. Based on these components, detection engine will retrieve the more similar outcome. And also SNORT rules have supporting following actions namely pass, log or alert. With the help of these rules, any kind of intrusion attacks can be predicted and these results will be communicated with the third party node for the final decision making about the presence of the intruders.

3.3. SECURED DECISION SHARING

In order to avoid the selfish node presence, in this work unique secret keys are generated for each monitoring node by using which intrusion decision will be encrypted and then send to the third party node. Whenever the new monitoring node established it will send REQ packet to the third party node for generating the secret keys. The REQ packet format is given below:

REQ = {Source=monitoring node, Destination=third party node, RT||R_0||MAC (K_{BN}, monitoring node||RT||R0)}

Where source ➔ monitoring node address

Destination ➔ third party node address
RT ➔monitoring node identifier
R_0 ➔Random value

MAC ➔Message authentication code
K_{BN} ➔ Shared secret key
Upon reception of this REQ packet, third party node will check intruder node lists to analyse whether the corresponding monitoring node already present in intruder list or not. If it is present, then this packet will omitted. If not then third party node will analyse the MAC and will create the session key $K_{NR.}$ The format of session key is given below
K_{NR} = H (K_{BN}, monitoring node$||R_0||R_l$)
Where
H ➔ one way hash function
R_l ➔ random value generated by third party node
After generation of this session key, successful acknowledgement (SucAck) will send back to the sink node along with session key K_{NR}. The packet format of SucAck is given below

SucAck = {Source=third party node, Destination=Sink, E (K_{BT}, monitoring node$||R_0||R_l||K_{NR}$)}

Where
E ➔ Encryption method
K_{BT} ➔shared secret key
Upon reception of this SucACk, sink node will extract the session by decrypting it and secure information will be send back to the monitoring node.

Alert = {Source=Sink, Destination=Monitoring node, $R_0||R_l||$MAC (K_{NR}, Sink||monitoring node$||R_0||R_l$)}

This information will be utilised for sharing the intrusion detection outcome with the most recent session key received from the third party node.

The overall processing flow of this secured decision sharing work is given in the following figure 1.

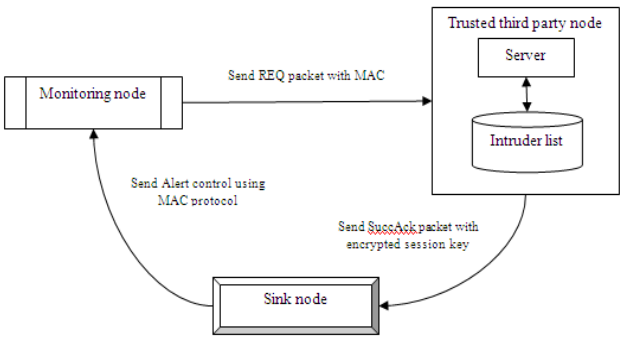

Figure 1. Overall flow of secured decision sharing scheme

3.4.THIRD PARTY NODE SELECTION AND AUTHENTICATION

Here third party node will authenticate the node and then will utilize the intrusion information to make the final decision. Third party node plays more important role in making the intrusion decision. In this work, third party node selection is done with the concern of trust level and available bandwidth. Because it is responsible for authentication purpose. Thus node should be trustable and also should have enough bandwidth to support efficient authentication process. Thus the most suitable third party node is selected by using Hybrid Ant colony with genetic method. We propose to join two meta heuristics, to be specific the GA and the ACO. The GA is a populace based technique where beginning populace is haphazardly created. Along these lines the haphazardly produced introductory arrangements are further hereditarily assessed. As observed over, the ACO calculation is a populace based too. The distinction, as contrasted and the GA, is that the ACO does not need beginning populace. The ACO is a helpful technique, in which the ants search for good arrangements guided by the parameter called the pheromone. Toward the starting the underlying pheromone is the equivalent for the all curves of the chart speaking to the issue. After each emphasis, the pheromone levels are refreshed (in all circular segments; in curves gone by the subterranean insect the pheromone level is expanding, while in relinquished bends it dissipating). As the outcome, the components speaking to preferable arrangements get more pheromone over others and become progressively attractive in a next cycle. In our half and half calculation the arrangements built (proposed) by the GA are treated as arrangements accomplished by the ACO in some past cycle, and we use them to determine the underlying pheromone level in the arrangement chart. After that we look for the arrangement utilizing the ACO calculation. In the trial, the exhibition of the proposed half and half technique is contrasted with the fundamental strategies, both GA and ACO. All things considered, a good chromosomal portrayal must be very much intended to be utilized by GA and GACO. Paired portrayal is in this way picked sensibly. These portrayals certification such arrangements, which are acquired by old style administrators, are legitimate. There is no compelling reason to characterize unique administrators for these portrayals.

1. Every chromosome comprises of (n-1) gatherings of quality.

2. The quantity of qualities in I th gathering is equivalent to (n-I) bit, with the goal that the absolute number of qualities (Ngen) in the chromosome pursues condition (1).

$$N_{gen} = \sum_{i=1}^{n-1} i$$

The handling stream of cross breed GA with ACO is given beneath:

1. Start

2. Introduce first hub of every insect

3. Finding the vitality level of every insect as indicated by condition 2 and for chromosome

4. Finding the hub with more vitality level

5. Update: Best hub of each cycle, best arrangement and pheromone lattice and next populace with GA administrator

6. n_cycles = n_cycles +1

7. Rehash till end criterion met

3.5.PENALTY ASSIGNMENT BASED ON INTRUSION DECISION

Based on this decision, penalty will be assigned to the selfish monitoring nodes. To keep our motivator conspire from being manhandled, we propose a notoriety based discipline offer component. In our discipline bid plot, every potential co-operator is appointed to a notoriety worth and we set a notoriety limit for every potential co-operator. In the event that a hub's notoriety score isn't more noteworthy than the given limit, at that point it is viewed as a noxious hub and has no privilege to collaborate any more. Thus, it cannot win more advantages. Along these lines every hub patterns to augment its utility just as keep its notoriety score

IV. RESULTS AND DISCUSSION

In this area, the execution investigation of the proposed system is done in the NS2 simulation in associate with the execution measurements for the PR-CIDS with the previous CIDS, TNK-CIDS and the past existing GT-CIDS. The correlation evaluation is performed between PR-CIDS, CIDS, TNK-CIDS and GT-CIDS. The reproduction esteems are appeared in the accompanying table 1, and 2.

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	CIDS	PR-CIDS	GT-CIDS	TNK-CIDS	CIDS	PR-CIDS	GT-CIDS	TNK-CIDS	CIDS	PR-CIDS
10	79.878	89	91	93	586.89	489	470	450	104.26	125	136	142
20	80.077	91	92.3	93.5	586.89	475	426	395	99.73	111.39	139	149
30	80.021	91.023	92.4	94.6	586.89	469.56	415	374	99.73	135	145	153
40	80.059	93.2	94.1	94.9	586.89	469.56	402	360	104.26	129.56	149	159
50	79.98	93.56	94.7	95.7	586.89	469.56	402	355	104.26	131.47	153	162
60	79.979	94.82	94.98	95.96	586.89	469.56	402	355	99.73	145	157	167
70	79.947	94.99	95.42	96.3	586.89	469.56	402	350	99.73	135	159	172
80	80.039	96.7	97.2	97.8	586.89	469.56	402	340	104.26	129.84	163	178
90	80.005	96.97	97.8	98.9	586.89	469.56	402	340	104.26	129.84	167	182
100	79.923	96.97	97.9	99.1	586.89	469.56	402	340	99.73	131.26	168	182

Table 2, Simulation metric values

Simulation time in ms	Performance Metrics							
	False positive Rate				Detection Rate			
	GT-CIDS	TNK-CIDS	CIDS	PR-CIDS	GT-CIDS	TNK-CIDS	CIDS	PR-CIDS
2	10	65	71	72	25	29	31	33
4	20	74	77	79	48	51	55	57
6	85	79	82	85	100	121	135	138
8	200	156	159	162	175	182	195	199
10	300	189	193	198	260	275	282	287
12	350	240	253	256	320	335	342	351
14	400	350	361	364	375	381	396	397
16	440	370	383	387	425	426	452	459
18	470	410	425	431	460	460	475	482
20	500	435	450	453	505	516	536	541

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:

$$PDR = \frac{\sum_{i=0}^{n} PR_i}{\sum_{0}^{n} PS_i} \quad (6)$$

Where PR → packets received.

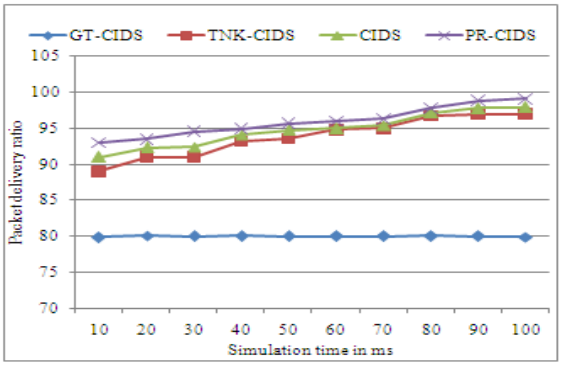

Figure 2. Packet Delivery rate

The PDR of the methodology that is to state PR-CIDS, CIDS, GT-CIDS and TNK-CIDS are related together. Subordinate upon this the result of PR-CIDS shows the upgraded execution contrasted with the other two methodologies as expressed by the figure 2.

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.

$$\text{Average Delay} = \frac{\sum_{i=0}^{n} PRT - PST}{n} \quad (7)$$

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

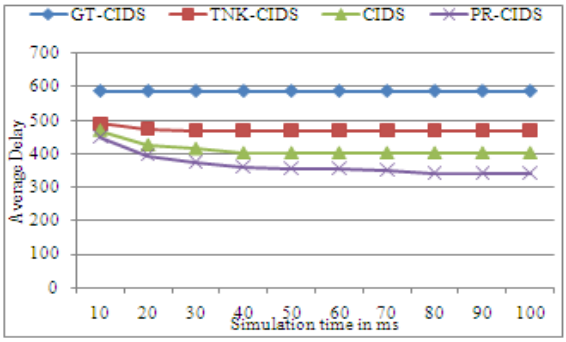

Figure 3. Average Delay

The normal deferral of the procedure called PR-CIDS, CIDS[23], GT-CIDS and TNK-CIDS[22] are coordinated up together. Subordinate upon this the result PR-CIDS shows the upgraded execution contrasted with the other two systems as showed in the figure 3.

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.

$$\text{throughput} = \frac{\text{number of packets moved}}{\text{total number of packets}} \quad (8)$$

This is exposed in figure 4.

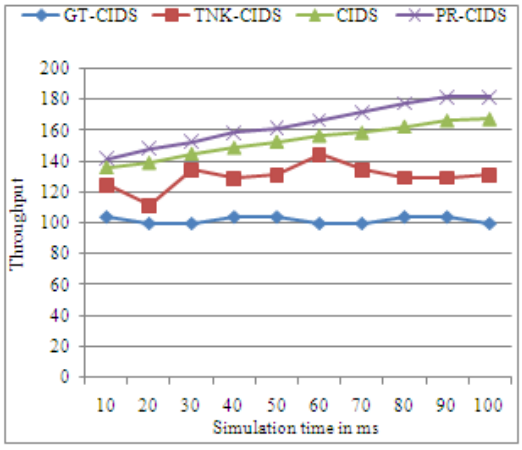

Figure 4. Throughput

The throughput of various strategies in re-enactment condition from the source to each objective hub is uncovered in Figure 4. Thus it demonstrates that the PR-CIDS would yield the improved results when coordinated with the standard PR-CIDS indicates expanded throughput execution.

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

$$\frac{FP}{N} = \frac{FP}{FP + TN} \quad (9)$$

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.

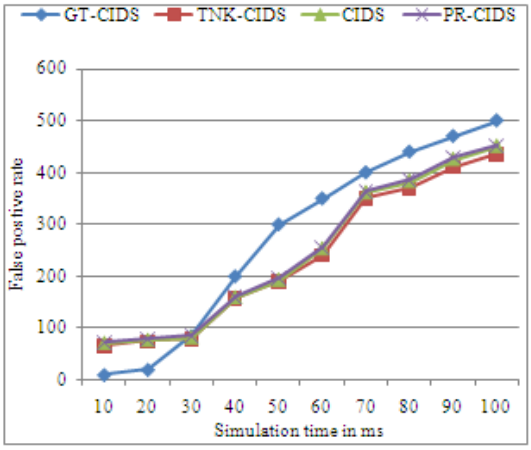

Figure 5. False Positive rate comparison

The false positive rate of various systems in recreation condition from the source to each objective hub is uncovered in Figure 5. Therefore it demonstrates that the PR-CIDS would yield the upgraded results when coordinated with the standard TNK-CIDS indicate lesser false positive rate execution.

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:-

$$DR = \frac{TP}{(TP + TN)} \times 100\% \quad (10)$$

Where

TP = amount of attack when it actually attack

TN = amount of normal detect when it actually normal

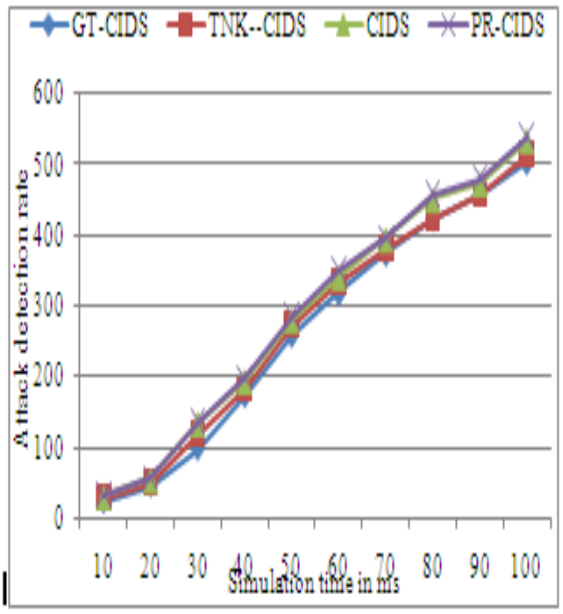

Figure 6. Attack detection rate

The assault location rate of various methods in reproduction condition from the source to each objective hub is uncovered in Figure 6. Thus it demonstrates that the PR-CIDS would yield the improved results when coordinated with the standard TNK-CIDS indicates expanded assault identification rate execution.

V. CONCLUSION

In this work, initially monitoring nodes are selected optimally by using modified artificial bee colony algorithm through which intrusion detection will be performed. Here intrusion detection is performed based on variation in the forwarded traffic. In order to avoid the selfish node presence, in this work unique secret keys are generated for each monitoring node by using which intrusion decision will be encrypted and then send to the third party node. Here third party node will authenticate the node and then will utilize the intrusion information to make the final decision. Third party node plays more important role in making the intrusion decision. Thus the most suitable third party node is selected by using Hybrid Ant colony with Genetic method. Based on this decision, penalty will be assigned to the selfish monitoring nodes. This overall penalty decision making process is learned by using the artificial neural network algorithm. The overall evaluation of the research work is done in the NS2 simulation environment to prove their performance improvement.

REFERENCE

1. Sarkar, S. K., Basavaraju, T. G., & Puttamadappa, C. (2016). Ad hoc mobile wireless networks: principles, protocols, and applications. CRC Press.
2. Sandholm, Thomas E., Anupriya Ankolekar, and Bernardo Huberman. "Sharing content between collocated mobile devices in an ad-hoc private social group." U.S. Patent Application 14/431,209, filed October 22, 2015.
3. Jamal, T., & Butt, S. A. (2018). Malicious node analysis in MANETS. International Journal of Information Technology, 1-9.
4. Jayaraman, S., Bhagavathiperumal, R., & Mohanakrishnan, U. (2018). A three layered peer-to-peer energy efficient protocol for reliable and secure data transmission in EAACK MANETs. Wireless Personal Communications, 102(1), 201-227.
5. Hemalatha, S., & Mahesh, P. S. (2018). Energy Optimization in Directional Advanced Intruder Handling AODV Protocol in MANET.
6. Wu, D., Zhang, P., Wang, H., Wang, C., & Wang, R. (2016). Node service ability aware packet forwarding mechanism in intermittently connected wireless networks. IEEE Transactions on Wireless Communications, 15(12), 8169-8181.
7. Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.
8. Zarpelao, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.
9. Anwar, S., Mohamad Zain, J., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions. Algorithms, 10(2), 39.
10. Shattil, S. J., & Sen, R. (2019). U.S. Patent Application No. 16/278,406.
11. Chiba, Z., Abghour, N., Moussaid, K., & Rida, M. (2016). A cooperative and hybrid network intrusion detection framework in cloud computing based on snort and optimized back propagation neural network. Procedia Computer Science, 83, 1200-1206.
12. Abusitta, A., Bellaiche, M., & Dagenais, M. (2018, February). A trust-based game theoretical model for cooperative intrusion detection in multi-cloud environments. In 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN) (pp. 1-8). IEEE.
13. Chakraborty, P., Majumder, K., & Dasgupta, A. (2016). A game theoretic model to detect cooperative intrusion over multiple packets. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 895-907). Springer, New Delhi.
14. Abusitta, A., Bellaiche, M., Dagenais, M., & Halabi, T. (2019). A deep learning approach for proactive multi-cloud cooperative intrusion detection system. Future Generation Computer Systems, 98, 308-318.
15. Hassanzadeh, A., & Stoleru, R. (2013). On the optimality of cooperative intrusion detection for resource constrained wireless networks. Computers & Security, 34, 16-35.
16. Hajiheidari, S., Wakil, K., Badri, M., & Navimipour, N. J. (2019). Intrusion detection systems in the Internet of things: A comprehensive investigation. Computer Networks.
17. Wu, M., & Moon, Y. (2019). Alert Correlation for Cyber-Manufacturing Intrusion Detection. Procedia Manufacturing, 34, 820-831.
18. Halder, S., Ghosal, A., & Conti, M. (2019). Efficient physical intrusion detection in Internet of Things: A Node deployment approach. Computer Networks, 154, 28-46.
19. Jiayan, Z., Fei, L., Haoxi, Z., Ruxiang, L., & Yalin, L. (2019). Intrusion Detection System using Deep Learning for In-vehicle Security. Ad Hoc Networks, 101974.
20. Han, L., Zhou, M., Jia, W., Dalil, Z., & Xu, X. (2019). Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. Information Sciences, 476, 491-504.
21. Loukas, G., Karapistoli, E., Panaousis, E., Sarigiannidis, P., Bezemskij, A., & Vuong, T. (2019). A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Networks, 84, 124-147.
22. Adilakshmi Yannam, G.V.S.N.R.V.Prasad "Trust Aware Intrustion Detection System to Defend Attacks in Manet"," International Journal of Innovative Technology and Technology Exploring Engineering(IJITEE)",ISSN:2278-3075,Vol-8,Issue-6,April-2019.
23 Adilakshmi Yannam,G.V.S.N.R.V.Prasad,"Cooperative Intrusion Detection System to Enhance The Security in MANET"," Journal of Advanced Research in Dynamical and Control Systems", ISSN:1943-023X Accepted for publication in Vol- 11 ,Issue-7 ,Septecmebt-2019.

AUTHORS PROFILE

Adilakshmi Yannam. 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 covers the Security Issues in MANETs.

Dr.G.V.S.N.R.V.Prasad is a Professor & Vice Principal at the Gudlavalleru Engineering college, Gudlavalleru. He received Ph.D in CSE from the University of JNTUK, Kakinada..He is the member of CSI,IE,SAEINDIA. His research interest cover the Data Mining and Analytics with Security issues over 50 publications.