ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

DYNAMIC RULE GENERATION IN THE CLUSTER HEAD BY ONLINE COLLABORATED MALICIOUS NODE DETECTION

Dr. M. Renuka Devi

Associate Professor, Dept of BCA, Sri Krishna Arts and Science College,

D.Shona,

Part time Research Scholar, Bharathiar University

ABSTRACT

Security in Mobile Ad hoc Network (MANET) is one of the key challenges due to its specific features such as dynamic topology, hop-by-hop communications, and open network boundary. A Collaborated Malicious Node Detection (CMND) was proposed as a combination of black hole, grey hole, wormhole and flooding attack detection method. In CMND, various types of attackswere detected by proposed Trust point node, Observer node, and Source node based Black hole Attack detection (TOSBA), Enhanced Gray hole-Intrusion Detection System (EG-IDS), Enhanced Wormhole Detection (EWD) and Security upgraded Trust based Flooding Attack Detection (ST-FAD) mechanisms. Theinformation obtained from these mechanismsare trained by Replicator Neural network with decision tree (RNTree) , which generated rules and it was updated in the cluster head in MANET. Based on the rules,the black hole attack, grey hole attack, wormhole attack and flooding attack in MANET were detected. The generated rules are static in nature which was created based on a set of data and it would remain same for all data transfer and if any new attack comes the static rule won't be able to detect. In order to dynamically update the rules in the cluster head,a static agent is deployed in all nodes. The static agent takes the task of collecting each attack mechanism information such as node id, hop-length, total number of packet forwarded and received, total number of packet drop, total number of packets in communication, mean received signal strength and standard deviation in all nodesThen, clusters are formed based on the distance between the nodes. A cluster head is selected in each cluster based on the residual energy and connectivity degree of nodes. The information collected by the static agent is trained by RNTree which generates dynamic rules for detection of malicious nodes in the network an Online Collaborated Malicious Node Detection (OCMND) is proposed in this paper. It improves the accuracy of Online Collaborated Malicious Node Detection (OCMND).

Keywords: MANET, cluster head selection, agent-based data collection, Collaborated Malicious Node Detection, RNTree.

1. INTRODUCTION

The traditional wireless networks need fixed infrastructure, central control and important requirements for their operation whereas in Mobile Ad hoc Networks (MANETs) can exist without having fixed infrastructure. Due to the frequently changing mobility and dynamic property of node in MANET, it is vulnerable to various attacks such as black hole, gray hole, wormhole and flooding attacks etc. Securing MANET is a challenging one. An Intrusion Detection System (IDS) plays an important role in identification of attacks in MANET. IDS continuously analysis and monitors the network activities for detection of attacks in the network.IDS run on each mobile node in MANET to detect the local intrusions and local traffic. Generally, IDS are categorized as knowledge based IDS, behavior based IDS and machine learning based IDS.

Knowledge based IDS [1]is dependson a database of known attack signatures. It tries to match the data with signature pattern. If it matched with signature pattern, the IDS register that an attack has happened or is happening and respond with an alarm, alert or modifications. However, the effectiveness of knowledge based IDS is depends on the signature database. In behavior based IDS, IDS try to model the behavior of network traffic. A packet is flagged as malicious when it is deviated from this model and an alert message is sent. However, this type of IDS generates a lot of false positive alarms. Machine learning based IDS [2] used machine learning techniques such as Support Vector Machine (SVM), Naïve Bayes, Decision Trees, Fuzzy logic and BayesNet for intrusion detection. It minimizes the false alarm rate behavior based IDS.

A collaborated Malicious Node Detection (CMND)[3] was proposed detection of multiple attacks in MANET. Trust point node, Observer node and Source node based black hole Attack detection (TOBSA) mechanism was introduced for black hole attack detection based on the analysis of the sequence number of route reply. An Enhanced Gray hole-Intrusion Detection System (EG-IDS) was introduced to detect gray hole attack by using Bayesian Bernoulli behavior classifier. An Enhanced Wormhole attack Detection (EWD) mechanism was introduced to detect the wormhole attack based on the calculation of suspicious value of each node. A Security upgraded Trust based Flooding Attack Detection (ST-FAD) mechanism was introduced to detect the flooding attack in the network based on the trust value of a node.From

the detection of black hole, gray hole, wormhole and flooding attack various information were collected and those information was trained by using Replicator Neural Network with Decision tree (RNTREE). It generated rules and based on it multiple attacks were detected in MANET.

In CMND,a MANET network was created with a set of nodes and the rules were generated based on the data in the created MANET network. The generated rules were updated in the cluster head. However, the generated rules are best suited for the created MANET. An Online Collaborated Malicious Node Detection (OCMND) is proposed in this paper where the dynamic rules are created by using static agent in the network. Initially, static agents are deployed in all nodes in the network. A number of clusters are formed in the network based on the distance between the nodes. Then a cluster head is selected in each cluster based on the residual energy and connectivity degree of nodes. The CMND is processed in all the nodes and the node id, pop-length, a total number of packet forward, a total number of packet received, a total number of packet drop, a total number of packets in the communication, mean received signal strength and standard deviationinformation of each node are collected from the static agents. This information issent to the selected cluster head which create rules by using RNTreeto detect the attacks in the network. Thus the data collection by thestaticagents creates dynamic rules for detection of malicious nodes in the network.

2. LITERATURE SURVEY

2.1 Knowledge-based IDS

A mechanism [4] was proposed for detection of gray hole attacks in the network. Initially, all the nodes in the network were initialized with integer credit values. The credit values of each node were calculated based on the forwarding RREQ message. The count of credit value of a node was increased when it received an RREQ from intermediate node or else the count of credit value was decreased. After that, check the source sequence number and destination sequence number. If the destination sequence number was greater than the source sequence number, then the node was identified as a gray hole. However, this mechanism consumed more energy and time for gray hole detection in the network.

An algorithm [5] was presented for SYN flooding attack detection. This algorithm introduced unnecessary delays to determine the nodes which delay the communication and affected the multimedia communication in MANET. A game theory was also used in this algorithm that created a game between the multimedia server node and the malicious node. A block list maintained the detected attacks and it was used for further consideration. Hence this algorithm gave full assurance that the node selected for the transfer of data. But the game theory in this algorithm is not reaching the maximum throughput.

2.2 Behavior-based IDS

A lightweight scheme [6] was proposed to detect Sybil attack in MANET. The lightweight scheme used Received Signal Strength (RSS) to differentiate Sybil and legitimate identities. Initially, the entry and exit behavior of legitimate node was demonstrated using simulation and testbed experimentation. Then, a threshold was defined which distinguished between Sybil and legitimate identities based on nodes' entry and exit behavior. Finally, fine tuned the detection threshold by combining the RSS data fluctuation taken from the testbed experimentation. The major drawback of lightweight scheme is sometimes the false positive rate is high.

The protection of navigational protocol [7] was presented in occasional portable networks against black holes, silver holes and wormhole attack. This protocol was comprised of two phases. In the first phase of the navigational protocol, the distance between the inception and destination with Round Trip Time (RTT) was calculated and based on it wormhole, silver hole and black hole attacks in the network were detected. In the second phase of navigational protocol, packet forwarding table was used to prevent the black holes, silver holes and wormholes incidence between the inception and destination nodes. However, at some points the end-to-end delay is high.

A Detecting and Eliminating Black Holes (DEBH) approach [8] was proposed for black hole detection in MANET network. It used an additional Black hole Check and data control packet to detect and eliminate the malicious nodes in the network. The freshest path in the network was found by using Ad hoc On-demand Distance Vector (AODV) routing protocol in DEBH. After that, the safety of the selected path was checked. When a node was detected as malicious node then that node was isolated from the entire network by broadcasting a packet that contained the ID of malicious nodes. However, it is more suitable only for black hole attack detection.

An algorithm [9] was proposed for detection of black hole and gray hole attack in MANET. This algorithm was composed of two phases are route discovery and monitoring phase. In the route discovery phase, sender first sent the trap route request (RREQ). It contained the destination address which does not exist in the network so when blackhole node received RREQ, then it immediately sent reply to source node. After receiving the fake RREQ response sender node record the source of RREP and added it to their malicious list. In the monitoring phase, all nodes monitoring their neighbor nodes activity when it found any malicious nodes in the network it does not forward data to next node so their forwarding ratio is decreased. If this ratio is less thanthreshold value, the monitoring node immediately sent alert message to source node. However, the selection of threshold value influences the performance of algorithm.

2.3 Machine learning-based IDS

A novel technique called Accurate Prevention and Detection of Jelly Fish Attack Detection (APD-JFAD) [10] was proposed to combat Jellyfish attack in MANET. The APD-JFAD technique was a fusion of an authenticated routing-based framework for detecting attacks and Support Vector Machine (SVM). SVM was used to learn packet forwarding behavior. A node was assumed to launch Jellyfish attack which was hard to detect. Node property based hierarchical trust evaluation was carried out in the APD-JFAD technique. Accordingly to large extent, Jelly Fish attack was defended in MANETs by selecting trusted paths for routing packets from source to destination. The accuracy of APD-JFAD technique could be improved by integrating deep learning method.

3. PROPOSED METHODOLOGY

In this section, the cluster head selection and agent based data collection for Online Collaborated Malicious Node Detection (OCMND)is described in detail. Initially, static agentsare deployed in all nodes which take the tasks of collecting information in all nodes. During cluster formation, clusters are formed with the nodes based on the distance between the nodes. Then, cluster head selection process is started with cluster formation based on the connectivity degree and residual energy of a node in the clusters. Each node processed the CMND and the information about the attack detection in each node is collected by static agent. It is sent to the cluster head where the RNTree is processed to create dynamic fuzzy rules. Based on the dynamic fuzzy rules the attacks in the MANET are detected. The overall process of OCMND is given in following figure 1.

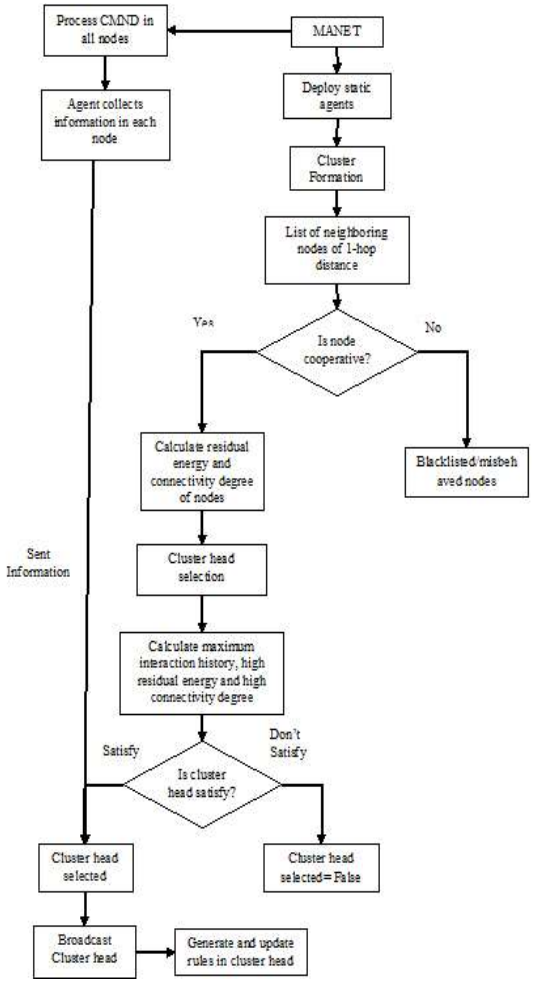

Figure 1. Overall Flow of OCMND

3.1 Formation of clusters

In MANET, the set of all nodes are denoted as $N = n_1, n_2, \ldots n_i$, where $i \geq 2$. Static agents are deployed in each node and the static agent communicates by using remote procedure calling or messaging. After deployment,a pair of nodes $n_i, n_j \subseteq N$may interact with each other. If $n_i$and n_j are cooperate, then the interaction between n_i and n_j is observed as successful. If either n_i or n_j does not cooperate, then it is observed as unsuccessful. The interaction history [11] of observed outcome between n_i and n_j from the perspective of n_i is recorded at any given time t which is given as follows:

$$Int\_His^{t}_{n_{ij}} = \left(S^{t}_{n_{ij}} + US^{t}_{n_{ij}}\right) \quad (1)$$

In equation (1), $Int\_His^{t}_{n_{ij}}$ is the interaction history of observed outcome between n_i and n_j, $S^{t}_{n_{ij}}$ is the number of successful interaction between n_i and n_j and $US^{t}_{n_{ij}}$ is the number of unsuccessful interaction between n_i and n_j. Followed by the deployment, the node discovery process discovers neighbor nodes of each node by broadcasting one-hop hello packets. On the reception of a hello message from node n_i, node n_j replies with an authenticated message using the pairwise key. The reply consisted of n_j's node ID, time stamp and location information of node n_j. The node n_j is recorded in the n neighbors list when that node is verified to be authentic.

After deployment, the nodes broadcast their ID(n_i), residual energy and connectivity degree along with the request or reply (REQ/REPLY) flag. The residual energy [12] of a node $n_i$is defined as the energy present at the node n_i at a particular time. The node spends energy while transmitting and receiving data packets from n_i to n_j. It can be calculated as,

$$RE(n_i, n_j) = I(n_i) - \left(E_t(n_i) + E_r(n_i)\right) \quad (2)$$

In equation (2), $RE(n_i, n_j)$ denotes the residual energy of a node n_i while transmitting and receiving data packets from n_i to n_j, $I(n_i)$ denotes the initial energy of a node n_i, $E_t(n_i)$ denotes the transmitting energy of a node n_i, and $E_r(n_i)$ denotes the receiving energy of a node n_i.

The connectivity degree [13] is the measure of the in links and out links from node n_i to another noden_j. It can be calculated as,

$$CD(n_i, n_j) = d\left(in_{n_i n_j}\right) + d\left(out_{n_i, n_j}\right) \quad (3)$$

In equation (3),$CD(n_i)$ denotes the connectivity degree from node n_i to n_j, $d(n_{in})$ denotes the number of in-links

of node n_i and $d(n_{out})$ denotes the number of out-links from node n_i to n_j.

The node which has maximum one hop neighbors, high residual energy and high connectivity degree is selected as cluster head. Other nodes become members of the cluster or local nodes. A circle is formed with a fixed radius by selecting (i.e., either randomly or with highest cooperating neighbor density within 1 hop distance) a node as center and arbitrary small length as radius. Center of the new circle is calculated as the mean of the points within the circle while the radius is increased by the distance of two successive centers. The nodes reply back and in this way clusters are formed in the network. The cluster formation algorithm is given as follows:

Cluster Formation Algorithm

Input: $N = n_1, n_2, \ldots n_i$, small length $d1$

Output: Set of clusters C1, C2,C3….Cn

Begin cluster=1

Repeat

Choose a node n_i which is 1 hop distance apart from other participating nodes with a small length $d1$ randomly

Do

Initialize $N = n_i, d = d1$

Draw a circle with n_i as center and d as radius

Calculate new radius $(d1) = d + |n_i - n_j|$

While $n_i \neq n_j$

Cluster-1 is formed with cooperating nodes lying within the circle

End

3.2 Selection of cluster head

Here the selection of cluster heads in a MANET is considered for n nodes such that every node in this network is within distance h hops of a cluster head. The cluster lifetime represents the time from the point a node is elected as cluster head until the point a node changes its status to normal node. A clustering message is sent to every three seconds. Thus, a neighbor node is kept in the neighbor table for $3 \times COUNTR$ seconds and removed if there is no further clustering message received. Initially, for all nodes in the network the interaction history (Int_His) has been considered as 0 or $\geq$ 1. From equation (2) and (3), residual energy and connectivity degree can be evaluated by

$$RE(n_i, n_j) = \frac{\sum_{i,j=1, i \neq j}^{n} I(n_i) - \left(E_t(n_i) + E_p(n_i)\right)}{Int\_His_{n_{ij}}^{t}} \quad (4)$$

$$CD(n_i, n_j) = \frac{\sum_{i,j=1, i \neq j}^{n} d\left(in_{n_i,n_j}\right) + d\left(out_{n_i,n_j}\right)}{Int\_His_{n_{ij}}^{t}}$$

$$V = RE(n_i, n_j) + CD(n_i, n_j)$$

In equation (4) and (5), $i, j \in nodes$, $RE(n_i, n_j)$ is the i's residual energy while transmitting and receiving data packets from i to j, $CD(n_i, n_j)$ is the connectivity degree between node i and j and n is the number of nodes in cluster.Due to the dynamic changes in the topology of network, cluster structure is updated time to time. Based on the residual energy and connectivity degree of a node, cluster head is selected. The cluster head selection algorithm is given as follows:

Cluster Head Selection Algorithm

Input: Set of nodes

Output: Cluster head

Initialize $CH_{cur} = 0$, $CH_{prev} = 0$, $Time_{prev} = 0$, $now = 0$, $Time - OUT_{loop} = 3 \times COUNTR$.

Evaluate residual energy and connectivity degree of each node by using equations (4) and (5).

if $Int\_His_{n_{ij}}^{t} \geq 0$

while $Time_{prev} \leq now$ or $(V == low)$ do

CH_{prev} remains as cluster head

end while

if $V(CH_{prev}) = V(CH_{cur})$ and $Int\_His(CH_{prev}) = Int\_His(CH_{cur})$ then

Both CH_{prev} and CH_{cur} remains as cluster heads

else

Select new cluster head(s)

end if

Initially in the cluster head selection algorithm, the current cluster head CH_{cur}, previous cluster head CH_{prev}, time at a point before a cluster head is elected $Time_{prev}$ and the current time now are initialized as 0. The interaction history of all nodes in the cluster is considered as 0 or 1. The residual energy and connectivity degree of each node in the cluster is calculated. The CH_{prev} remains as cluster head until $Time_{prev}$ is less than now and V is equal to low. Check the current and previous cluster head node's residual energy and connectivity degree. If both nodes have the same residual energy and connectivity degree and the interaction history of both nodes are same, then both nodes remains as previous

cluster head and cluster head. Otherwise, new cluster head is selected.

After the selection of cluster head, each cluster head starts to broadcast cluster beacon. As the node n_k gets the cluster head beacon, it sends request beacon to join the network with its public key. The cluster head checks whether it is a duplicate message or not. If it is not a duplicate, the cluster head stores the public key of $n_k$as its id and generates a pairwise shared key to communicate between cluster head and n_k. Also sends a secret key for secure intra cluster communication.

After the cluster head selection process, the CMND is processed in all the nodes. The deployed static agent collects the information such as node id, hop-length, total number of packet forwarded and received, total number of packet drop, total number of packets in communication, mean received signal strength and standard deviationwhich are obtained from each mechanism in CMND. Theinformation are sent to the cluster head where RNTree is trained with these information and create rules to detect black hole, grey hole, wormhole and flooding attacks.

4. RESULT AND DISCUSSIONS

A Network Simulator-2 (NS-2) is used as a simulation tool to analyze the performance of CMND and OCMND in terms of accuracy, precision, throughput and Packet Delivery Ratio (PDR). NS-2 is a sequential simulator which uses the standard discrete event simulator algorithm. Its input is a description of a network model and its output is an imaginary history of this network. It works at packet level and provides substantial support to simulate bunch of protocols. The simulation parameters are given in the following Table 1.

Table 1. Simulation Parameters

Simulator	NS-2.34
DoS attack	Black/Gray/worm-hole/ flooding attack
Channel Type	Channel/Wireless Channel
Antenna Type	Antenna/Omni Antenna
Radio Propagation model	Propagation/Two Ray Ground
Link Layer type	LL
Interface queue type	Queue/ Drop Tail / PriQueue
MAC type	MAC/802_11
Protocol studied	DSR
Simulation area	1000*1000
Trace format	New wireless format
Node movement model	Random waypoint
Traffic type	CBR (UDP)
CBR rate	50 Kbps
Data Payload	512 bytes/packet
Number of nodes	100
Malicious nodes	14

4.1 Accuracy

Accuracy is calculated by dividing the number of correctly predicted instances (in this case malicious nodes) by the total number of nodes in the network. It is given as follows:

$$Accuracy = \frac{True\ Positive\ (TP) + True\ Negative(TN)}{TP + TN + False\ Positive\ (FP) + False\ Negative(FP)}$$

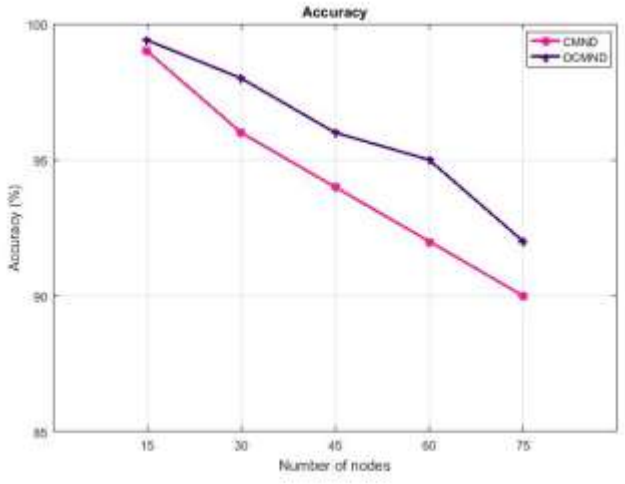

Figure 2. Comparison of Accuracy

Figure 2, shows the comparison between CMND and OCMND in terms of accuracy. The number of nodes is taken in x-axis and the accuracy is taken in y-axis. When the number of node is 45, the accuracy of OCMND is 2.13% greater than CMND. From this analysis it is proved that the proposed OCMND has high accuracy than the CMND method. The OCMND method analysis the network information over a time period using the static agent which generates the dynamic rules that leads to high accuracy.

4.2 Precision

Precision is the ratio of number of correctly predicted malicious nodes to the total number of correctly predicted malicious nodes and wrongly predicted non-malicious nodes in the network.

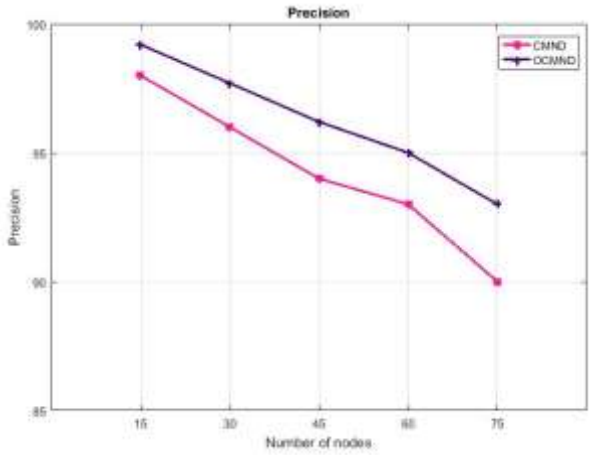

Figure 3. Comparison of Precision

Figure 3, shows the comparison between CMND and OCMND in terms of precision. The number of nodes is taken in x-axis and the precision is taken in y-axis. When the number of node is 45, the precision of OCMND is 2.34% greater than CMND. From this analysis, it is proved that the proposed OCMND has high precision than CMND. The

OCMND collects the network information instantaneouslythrough the static agent which helps to generate dynamic rules. As a result, the OCMND has high precision.

4.3 Throughput

The amount of forwarded data packets over a time period is known as throughput and its unit is Kilobits per second (Kbps). It can be calculated as,

$$Throughput = \frac{Number\ of\ transmitted\ packets}{Time\ taken}$$

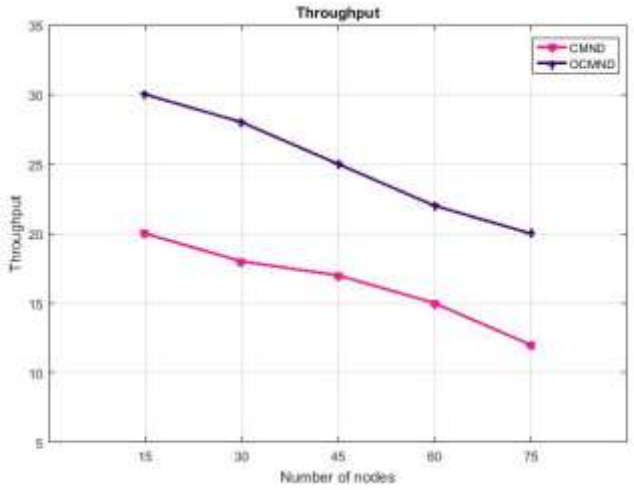

Figure 4. Comparison of Throughput

Figure 4, shows the comparison between CMND and OCMND in terms of throughput. The number of nodes is taken in x-axis and the accuracy is taken in y-axis. When the number of node is 45, the accuracy of OCMND is 47.05% greater than CMND. From this analysis it is proved that the proposed OCMND has high throughput than the CMND method. The OCMND detects various types of attacks through the dynamic rule creation based on the network information collected by the static agents. Thus, by detecting various types of attacks using dynamic rules the amount of forwarded packets in the network is increased.

4.4 Packet Delivery Ratio

The fraction of the total amount of data packets received at the destination to the total amount of forwarded packets from the source is called Packet Delivery Ratio (PDR).

$$PDR = \frac{Totalnumberofpacketsreceivedbydestination}{Totalnumberofpacketssentbysource}$$

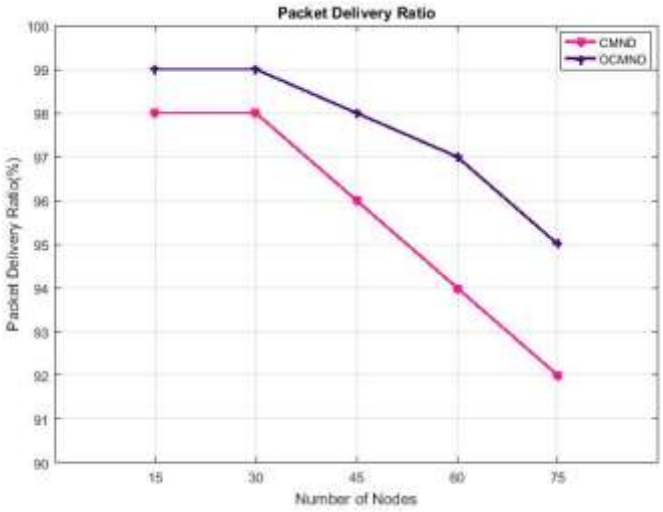

Figure 5. Comparison of Packet Delivery Ratio

Figure 5, shows the comparison between CMND and OCMND in terms of PDR. The number of nodes is taken in x-axis and the accuracy is taken in y-axis. When the number of node is 45, the accuracy of OCMND is 2.08% greater than CMND. The dynamic rules of OCMND effectively detect the attacks it is because of analyzing the network behavior using static agent. As a result, the PDR of OCMND is high than CMND method.

5. CONCLUSION

In this paper, static agents are used for data collection in CMND based attack detection in MANET. A MANET is created with a set of nodes and static agents are deployed in each node. Then clusters are formed with nodes which are closer with centric node. After the cluster formation, a cluster head is selected based on the residual energy and connectivity degree of a node. The CMND results of each node are collected by the static agent and it is sent to the cluster head. The RNTree is trained by the information sent by the static agent and detect the attacks in the MANET. The experimental results show that the proposed Online CMND has better accuracy, precision, throughput and PDR than CMND method.

References

[1] More, S., Matthews, M., Joshi, A., &Finin, T. (2012, May). A knowledge-based approach to intrusion detection modeling. In *2012 IEEE Symposium on Security and Privacy Workshops*(pp. 75-81). IEEE.

[2] Shah, S. A. R., &Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems*, *80*, 157-170.

[3] Shona, D., & Kumar, M. S. (2019). A collaborated rule-based classifier for malicious node detection in MANET. *Journal of Advanced Research in Dynamical and Control Systems*, *11*(6), 32-48.

[4] Makwana, S., &Vaghela, K. (2015). Detection and Elimination of Gray Hole Attack using Dynamic Credit based Technique in MANET. *International Journal of Computer Applications*, *125*(4).

[5] Geetha, K., &Sreenath, N. (2016). Detection of SYN Flooding Attack in Mobile Ad hoc Networks with AODV Protocol. *Arabian Journal for Science and Engineering*, *41*(3), 1161-1172.

[6] Abbas, S., Merabti, M., Llewellyn-Jones, D., &Kifayat, K. (2012). Lightweight sybil attack detection in manets. *IEEE systems journal*, *7*(2), 236-248.

[7] Behzad, S., Fotohi, R., &Dadgar, F. (2015). Defense Against the Attacks of the Black Hole, Gray Hole and Wormhole in MANETs Based on RTT and PFT. *International Journal of Computer Science and Network Solutions (IJCSNS)*, *3*, 89-103.

[8] Dorri, A., Vaseghi, S., &Gharib, O. (2016). DEBH: detecting and eliminating black holes in mobile ad hoc network. *Wireless Networks*, 1-13.

[9] Sharma, N., &Bisen, A. S. (2016, March). Detection as well as removal of black hole and gray hole attack in MANET. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 3736-3739). IEEE.

[10] Doss, S., Nayyar, A., Suseendran, G., Tanwar, S., Khanna, A., & Thong, P. H. (2018). APD-JFAD: Accurate prevention and detection of Jelly Fish attack in MANET. *Ieee Access*, *6*, 56954-56965.

[11] Ferdous, R., Muthukkumarasamy, V., &Sithirasenan, E. (2011, November). Trust-based cluster head selection algorithm for mobile ad hoc networks. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 589-596). IEEE.

[12] Subashree, C. P., &Thangalakshmi, S. (2016). Energy efficient aggregation in wireless sensor networks using artificial intelligence based aggregator election. *International Refereed Journal of Engineering and Science (IRJES)*, *5*(3), 8-16.

[13] https://systemsinnovation.io/network-connections.