Reduction Of Routing Overhead Using Cluster-Fuzzy Algorithm In MANET

D.Nethra Pingala Suthishni Dr.Anna Saro Vijendran

Abstract: A Mobile Adhoc Network (MANET) is a group of devices that are linked wirelessly. Ease of establishment and rapid deployment nature earned popularity for MANET and widely used in numerous applications especially in disaster recovery areas and in the military sector. MANET is with dynamic topology and limited resources that may susceptible to various security attacks. The overall performance of the network may be affected by security attacks. MANETS are exposed to vulnerabilities due to its co-operative algorithms, lack of administration, dynamic topology, and open medium. Intrusion Detection System (IDS) is adopted to observe varied nature of policy violation and malicious activity. IDS is implemented in MANET for monitoring the intrusion of any malicious node. Nodes in MANET are supplied with a minimal amount of energy and recharge or replacing of batteries is tedious. Hence, energy conservation and enrichment of privacy are important in IDS. In this paper, IDS is incorporated with the clustering algorithm and fuzzy rules to obtain better energy utilization. IDS is enhanced to obtain privacy from several security attacks. An extensive experiment is conducted to validate the simulation of the enhanced approach.

Keywords: intrusion detection system, Clustering algorithm, Cluster head, fuzzy rules, energy management.

1 INTRODUCTION

In recent years, the most prominent and exciting technology is MANET and shows the quick proliferation in wireless devices. MANET is greatly exposed to vulnerabilities due to the dynamic changing network topology, open medium, non-existence of centralized monitoring, cooperative algorithms, and management point. Defending networks with encryption software and firewalls are no longer active or sufficient for those features. Intrusion detection (ID) is a safeguarding expertise that spots interlopers who are trying to crack or maltreat the data without the permission of the actual users of the system [1, 2 and 3]. An IDS observes the activity of the system and user to discover the intruders. With the quick propagation of mobile computing applications and wireless networks, several new threats that haven't appeared in the wired networks have appeared in the wireless medium. Deploying wireless medium is exposed to several threats which pose security measures. The massive variance between wireless and wired networks makes traditional IDS inappropriate. Wireless IDSs, is one of the foremost research topics that aim at establishing new mechanisms and architecture to safeguard the wireless networks. In MANETs, detection and prevention of IDS are essential in balancing both to assure a highly protected environment. Intrusion avoidance measures, such as authentication and encryption methods are more suitable in preventing outside attacks. The intruder gathers all its cryptographic key details once the nodes are attacked. Therefore, authentication and encryption cannot secure against a malicious user.

I. INTRUSION DETECTION SYSTEM

MANETs are the most prevalent research area due to the research challenges that are associated with the protocols [4, 6, 7, and 8]. MANET permits users to transmit the data without any physical organization. The production of more powerful, small, and cheaper devices makes MANET a firmest growing network. MANET is a rapidly growing and promising technology that is the foundation of a rapidly deployed network [9, 10, 11]. MANET needs the frequent change of the network's topology. However, various researchers are working to eliminate the core weak points of MANET namely inadequate computational power, bandwidth, security, and battery power [7, 12, 13]. The available security solutions of wired networks are not be implemented directly to MANET that makes susceptible to vulnerabilities. This paper discusses current routing attacks and breaches in MANET and the newly designed IDS. Key management and cryptography are potential solutions for several attacks that are too expensive techniques and resource-constrained methods. The IDS techniques are not ideal among efficiency and effectiveness. Some elucidations [7, 12, and14] work well in the existence of one malicious node and might not be appropriate in the existence of many invaders. Besides, some may need special hardware such as an alteration to the available protocol or GPS. Diverse IDS is used to recognize various types of attacks using diverse ID procedures [8, 15]. Some postulations are made for IDS to work [16, 17]. The program, transmission, and user activities are recognizable. Intrusive activities as well the normal must have separate behaviors, as IDS must analyze and capture system activity to decide if the system is under intrusion or not. IDS is categorized with audit data as either network-based or host-based. A network-based IDS analyzes as well as captures packets from the flow of data traffic and the host-based IDS uses application logs or operating systems in its analysis. Based on detection methods IDS is segregated [5] They are Anomaly, Specification and Knowledge based IDS [18, 19].

2 RELATED WORK

John E. Dickerson et al [20] proposed a Fuzzy Intrusion Recognition Engine (FIRE) and it is designed using a network intrusion detection system (NIDS). Malicious action against the network is assessed by implementing the fuzzy

- *D.Nethra Pingala Suthishni, Department of Computer Science Sri Ramakrishna College of Arts and Science*
- *Dr.Anna Saro Vijendran Dean, School of Computing Sri Ramakrishna College of Arts and Science*

systems. The network system incorporates an agent-based method to distinct monitoring tasks. Every individual agent inside the network system performs their fuzzification with the help of input sources. All agents in the network exchange information with a fuzzy estimation engine and it associates the results of distinct agents. Fuzzy rules to generate signals that are true to a degree of the nodes. Numerous intrusion situations are presented by the author along with the fuzzy systems. The conducted simulation test shows that the fuzzy systems can simply classify DoS attacks and port scanning. FIRE is proficient in identifying some types of Trojan horse and backdoor attacks. NeetiKashyap [21] followed data mining techniques namely classification and clustering in developing an IDS for MANET. The zone routing protocol (ZRP) is used for the hybrid packet flow. Nodes in the network are categorized into three namely selfish, malicious and loyal which are used for identifying the Cluster Heads (CH). Loyal nodes possess sufficient energy to transfer the data in the MANET and assure successful data transmission which acts as one of the CH. MANET topology acts as a CH. Selfish node doesn't pass the data on their self-interest which consumes energy and malicious nodes create a threat to the network which creates security issues. Initially, MANET is created with mobile nodes and that possess normal nodes, malicious nodes, and selfish nodes. Resultant of clustering in IDS is more secure network transmission. Yi-anHuang et al [22] explained the progress in developing ID. Anomaly detection approach is improved to give more details on the source and attack types. Effortless rules employed in finding numerous well-known attacks and attackers. A cluster-based recognition scheme with a run-time resource-limited problem in that cluster head is chosen based on the periodical value. Each node in the network has a unique agent ID. Maintaining the level of effectiveness is enriched with the help of the agent ID generation method. Experiments were conducted extensively to test the efficiency of the research. Yi Ping et al [23] designed timed automata for MANET's DSR protocol that incorporates distributed IDS. Nodes within the cluster were chosen based on the periodical values and the chosen nodes monitor the transmission. Selected nodes supervise the global as well as local IDS. Timed automata are generated manually for abstracting the exact activities of the node in relevance to the DSR. Each node in the architecture owns a unique IDS agent. Finally, the intrusion detection technique is assessed through simulation experiments. The agent-based method shows efficiency and effectiveness. Erfan A. Shams[24]proposed a support vector machine (SVM) based IDS. The performance of MANETs is extensively influenced by the malicious nodes. DoS is one of the general attacks in MANET. The availability and integrity of certain mobile nodes can be achieved with a specific design of the intrusion system. Intruder's activity and the malicious node is removed from the network with the help of effective Intrusion Detection System that improves the network performance by continuous monitoring of network traffic. The major work of this paper is the incorporation of IDS with MANETs as a potent and reliable solution. The proposed IDS can identify the DoS kind of attacks at a high detection rate with a short computing time and simple structure. Experimental observation shows that the proposed IDS improves the reliability of the network considerably by removing and detecting the malicious nodes in the network system. MAJabbar et al [25] deal with a new ensemble classifier (RFAODE). In recent year's information and communication technology (ICT) has become an important part of human life. But ICT brings a lot of cyber risks. New kinds of vulnerabilities and threats are aroused in MANET's and IDS helps in detecting these attacks. Data mining (DM) and Machine Learning (ML) are used by the IDS system. Existing algorithms of IDS have only less accuracy and error rate in categorizing the attacks. RFAODE uses familiar algorithms namely RF and AODE. Average One-Dependence Estimator (AODE) determined the attribute dependency issue in the Naive Bayes classifier. Random Forest (RF) improves reduces the error rate and accuracy. The performance of the proposed RF+AODE is analyzed on the Kyoto data set. RFAODE outperforms the current IDS.

3 FORMULATION OF THE PROBLEM

The main intent of fuzzy logic in IDS is to deal with the fuzzy boundary among anomalous and normal classes. Fuzzy clustering is incorporate to deal varied devices and huge data transmission. On the basis of definite related factors, data are grouped that is the main intent of clustering. The data groups are separated with the assist of data point. Varied membership weights or degrees incorporated with the help of fuzzy and it segregates the data points. In fuzzy clustering algorithm, centres are expressed as fuzzy clusters and concurrently segregated. The count of the cluster (cl) is the input of the membership cluster num×cl is MC={mc_{ij} belongs to the range [0,1]} and num is the data point. Whereas, fuzzy clustering has immense potential in expressing relationship among the data points. Figure 1 illustrates the four partitioned instances.

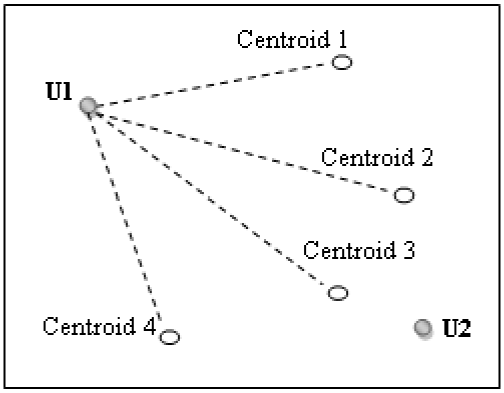

***Figure 1**. Cluster factors of four clusters*

Let the training data set is signified as TD={U,V}, original training set of num data points U={u_i, ...u_{num}} where each point u_i in the D-dimensional gap of vector (u_{il}........ u_{im})and denoted by the tag v_i belongs to V that belongs to the classes c is ω = { ω_1, ω_2,....... ω_n}. Maximum and signified cluster symbols are denoted by

$$D = \{d_i | d_i \max(mc_{ij}, j = 1 \ldots\ldots\ldots k)\}$$
$$holds\ u_i$$
$$Y = \{y_i | y_i argmax_i\ (mc_{ij}, j = 1 \ldots\ldots\ldots k)\}$$
$$signified\ to\ u_i$$

Foremost challenge of network is a cyber attack that is efficiently achieved by the fuzzy clustering algorithms. The key intent of fuzzy clustering is to separate the information in the network into clusters. Maximization is initialized within the cluster and minimization is initiated among cluster that holds similar objects. Prototype of the cluster is employed in measuring the divergence of information in the cluster. Best separation among the data is attained by the minimization function. The Fuzzy clustering incorporates the IDS as two phases that is estimation of midpoint of the cluster and allocating the points to the midpoints which are done using the Euclidian distance. The process is repeated until the termination criterion is attained. Overlapping clusters are estimated with the fuzzy that ranges from 0 to 1. Hence, the algorithm uses fuzzification parameter as f that ranges [1,n] that regulates the degree of fuzzy in the cluster. In the process of fuzzy clustering process, points in one cluster may fit into other clusters that is indicated with the membership grades and it determines the cluster point that denotes another point of other clusters. The points in the cluster are smaller than the degree of center. For every point in the cluster, the coefficient of degree of c^{th} cluster is $u_k(x)$ where x is a mid-point associated with the cluster.

$$\boldsymbol{Coefficient\ of\ x\ is\ termed\ as}\ \forall_x \left(\sum_{c=1}^{n.c} u_{c(x)} = 1 \right)$$

In fuzzy clustering, the centroid of a cluster is weighted by the degree and the relevant cluster:

$$center_c = \frac{\sum_x {u_{c(x)}}^j x}{\sum_x {u_{c(x)}}^j}$$

The degree of the cluster is correlated to the converse of the distance to the midpoint of the cluster

$$u_{c(x)} = \frac{1}{d(center_c, x)}$$

If the coefficients are normalized and incorporated fuzzy with the parameter j is greater than 1. Hence it results in the summation of 1, if it is 2 then linearly equal to 1 and if it is close to 1 that retrieves more weight. The prominent feature of fuzzy clustering is gradual membership of data points to cluster that are measured within the range of 0 and 1 degree values. Each cluster holds data incorporated by the membership function which denotes the fuzzy behaviour. The implementation of algorithm is depicted as follows;

$$OF = \sum_{r=1}^{q} \sum_{s=1}^{CD} M_{rs}^{p} \left\| x_r - CD_s \right\|^2$$

where OF is the objective function, m belongs to 1≤m≥∞ of any real number, degree of membership is M_{rs} in the cluster of s in the X_r, dimension of data is q and the midpoint of cluster is CD_s. The fuzzy and cluster matrix is constructed via objective function and continuous iteration by membership function updation as follows.

$$M_{rs} = \frac{1}{\sum_{L=1}^{CD} \left(\frac{\|X_r - CD_s\|}{\|X_r - CD_L\|} \right)^{\frac{2}{p-1}}}$$

$$CD_s = \frac{\sum_{r=1}^{q} (M_{rs})^p X_r}{\sum_{r=1}^{q} (M_{rs})^p}$$

The process of iteration ends at the condition of $\left\| U^{(L+1)} - U^{L} \right\| <$ € where € ∈ $0 \leq \mathrm{m} \geq 1$ and terminates at the 0 to k step.

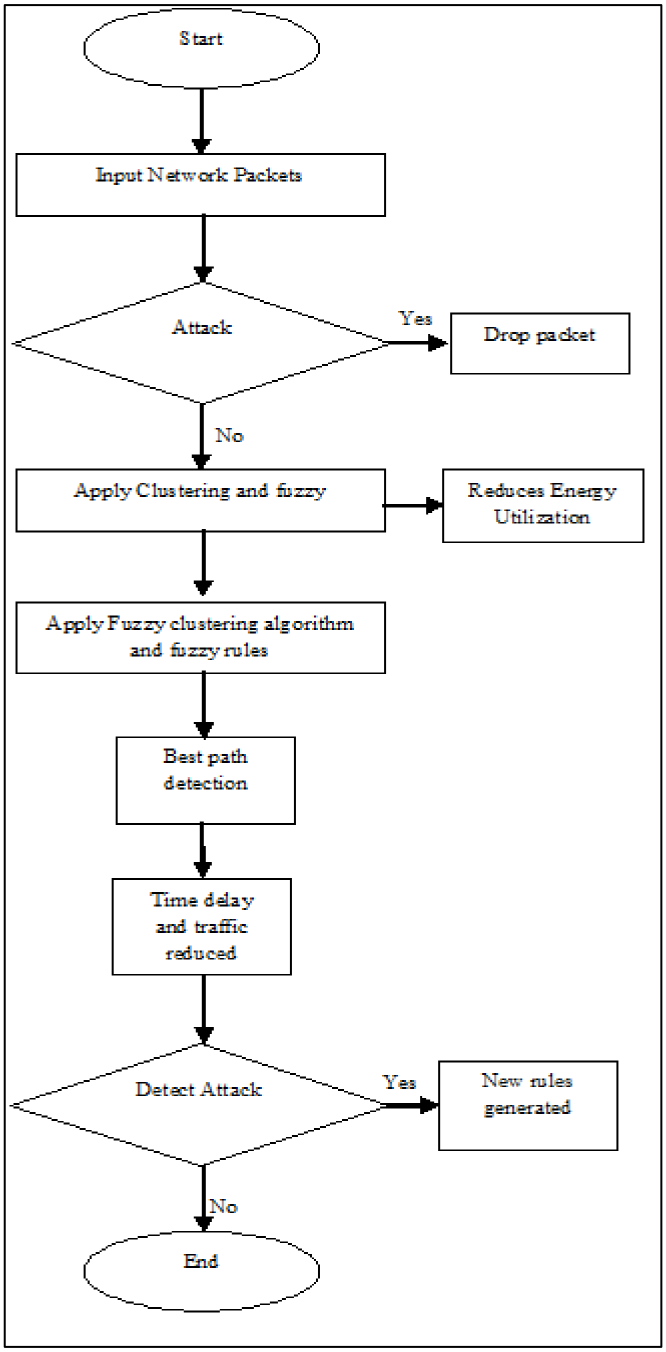
Start
Input Network Packets
Attack
Yes
Drop packet
No
Apply Clustering and fuzzy
Reduces Energy Utilization
Apply Fuzzy clustering algorithm and fuzzy rules
Best path detection
Time delay and traffic reduced
Detect Attack
Yes
New rules generated
No
End

***Figure 1**: Flowchart for IDS with clustering and fuzzy algorithm*

4 PROPOSED ALGORITHM

Routing protocol is enhanced using clustering algorithm in order to balance the energy consumption. A clustering probability model is used to divide the network into various sized heterogeneous clusters based on node residual energy and relative node position in the cluster. A combination of cluster head rotation mechanisms and heterogeneous cluster serves to balance node energy consumption in the network. Fuzzy logic is also classified in this algorithm. Fuzzy logic is used to select the source node and sends the message to the next neighbor node at that time finds the next node for further transmission. Neighbour node identification is accomplished by identifying the membership of the node and energy value is also compared with the other active nodes.

Clustering Algorithm Steps:

Ejres : Current residual energy level of node j

T CH_selec : Maximum required time to select CHs

```
Tj wait ← 1/ Ej res
WHILE  TCH_selec is not expired AND
  (Tj wait is expired OR SjCH_nbr is not empty) DO
    IF received a message THEN
      IF received CH-adv(i,Ei res) THEN
SjCH_nbr←SjCH_nbr U {(i,Ei res)}
      ENDIF
      IF received CH-rel(i) THEN
SjCH_nbr←SjCH_nbr - {(i,Ei res)}
      END IF
    END IF
END WHILE
IF SjCH_nbr is empty THEN
Transmit a CH-adv(i,Ei res) with cluster radius
   Listen for the CH-advs within delay time-period
   IF received CH-adv(i,Ei res) AND i>j THEN
     Transmit a CH-rel(j) with cluster radius
   END IF
END IF
```

Fuzzy Clustering Algorithm:

```
Input: source node s, destination node d
Find source node present the group of cluster then,
IF (s!=d && s==CH &&gd>node present the membership)
THEN
  Cluster message send from source s to CH
   IF (d==CH1 && CH!=CH1) THEN
   Cluster message send from CH to CH1
  CH1 send cluster message to destination d
   END IF
END IF
```

b). Procedure of Improved Intrusion Detection System

Step 1: Initially all nodes are deployed and a matrix as M=[M_{ij}] and $M^{(0)}$

Step 2: Data packet transmission is initiated to all neighbor nodes.

Step 3: Apply the Clustering process and fuzzy to classify the node with reduced energy utilization.

Step 4: Distance between the nodes and energy level is checked for Cluster Head selection.

Step 5: Node with low distance and high energy value elect the Cluster Head(CH) and The co efficient of the clusters midpoint is estimated as $\forall_{x}\left(\sum_{c=1}^{n.c} \boldsymbol{u}_{c(x)} = \boldsymbol{1}\right)$

Step 6: Give source and destination node.

Step 7: Fuzzy clustering algorithm is applied to avoid the traffic problem, and time delay.

Estimation of centre vector is established at the k step and at centroid by

$$\boldsymbol{M_{rs}} = \frac{\boldsymbol{1}}{\sum_{L=1}^{CD}\left(\frac{\|X_r - CD_s\|}{\|X_r - CD_L\|}\right)^{\frac{2}{p-1}}}$$

$$\boldsymbol{u}_{c(x)} = \frac{\boldsymbol{1}}{\boldsymbol{d(center_c, x)}}$$

Step 8: In Fuzzy clustering algorithm, presence of the node is checked to assign the cluster head. Fuzzy rules is applied to the node in the cluster group and the cluster head node. Fuzzy rules used to finds the membership of the nodes. Matrix is updated using the function called,

$$\boldsymbol{CD_s} = \frac{\sum_{r=1}^{q}(\boldsymbol{M_{rs}})^{p}\boldsymbol{X_r}}{\sum_{r=1}^{q}(\boldsymbol{M_{rs}})^{p}}$$

Step 9: Source node transmits the data packets to check whether the source node is present in the cluster group head and then in the membership of the node or not.

Step 10: CH send data to destination node present in the cluster group will receive the data and then send the data to destination node. When the criterion $\left\|U^{(L+1)} - U^{L}\right\| < €$ is reached updation is terminated if not follows step 2.

Step 11: Algorithm incorporation in IDS reduce the energy and improves the privacy.

5 SIMULATION RESULT

a). Simulation setup

In order to create transmission among the network following simulation setup is accomplished.

Table 1. *Simulation setup metrics*

S.NO	*Metrics*	*With IDS*
1	*No of nodes*	*100*
2	*Routing Protocol*	*DSR*
3	*Protocol Queue Type*	*CMUPriQueue*
4	*Initial Energy*	*100(J)*
5	*Packet Size*	*500 bytes*
6	*MAC Type*	*Mac/802_11*
7	*No of Cluster Head*	*10*
8	*CH Propagation*	*10 %*
9	*IDS Propagation*	*11.11%*
10	*No of Sink*	*1*
11	*Simulation Area*	*2150 * 2150 m*
12	*Simulation Ending Time*	*60ms*

b). Performance metric

In Network Simulator-2, the backend of Network Simulator is written in C++ and the front-end of the program is written in TCL (Tool Command Language). A namfile and a tracefile were automatically created, once the tcl program is compiled. These files were used to define keep track of transmission and the movement nodes pattern [26, 27]. In this section, evaluation is conducted in terms performance of network and evaluated using different graph metrics [28]. The performance metrics is classified in to three groups namely,

- Random Packet Dropping Rate,
- Control Packet Dropping Rate
- Block-Based Detection

Performance metrics are used for evaluating the protocols. The performance metrics is classified in to three broad groups and further they are classified as sub groups.

- Random Packet Dropping Rate

Overall Detection Error Probability

Failure of data rate that is due to link error or transmission flaws at that time overall detection error probability is estimated for entire duration of data transmission.

Overall detection error probability = Pgb / Pgb+ Pbg
Where Pgb - Link error rate
Pbg -Packet loss rate

Table 2: *Overall Detection Error Probability*

Time (sec)	*IDS with Clustering Fuzzy rules*
5	*0.2*
10	*0.1802*
20	*0.1801*
30	*0.1788*
40	*0.1793*

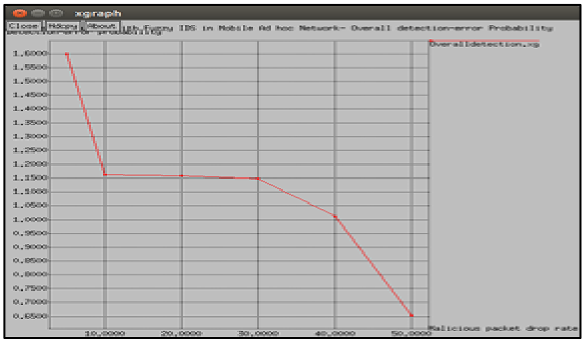

Figure 3: *Simulation Graph - Overall Detection - Error Probability*

Miss-Detection Probability

In miss-detection probability occurrence of malicious node can be perceived with a higher probability. Miss-detection probability is the most desirable context. Miss-Detection probability(Pmd) = Imd / 1000Imd -Attacker is not present time calculate drop.

Table 3: *Miss-Detection Probability*

Time (sec)	*IDS with Fuzzy rules*
5	*1.6*
10	*1.2474*
20	*1.24261*
30	*1.23269*
40	*1.12271*

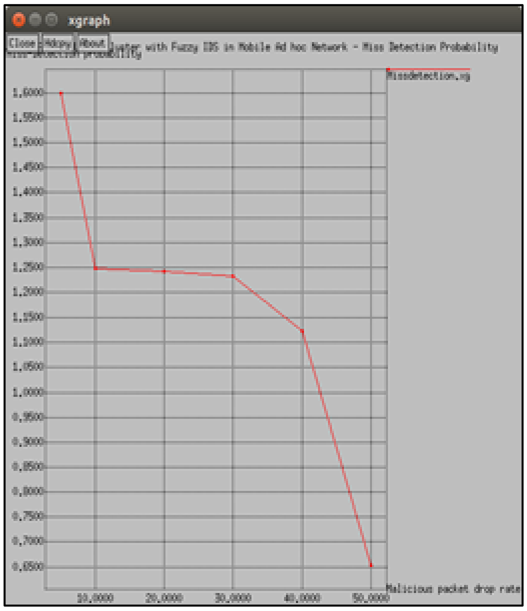

Figure 3: *Simulation Graph - Miss Detection Probability*

False-Alarm Probability

False Alarm Probability is described as the falsely detected data transmission rate when the source node is actually silent in the current transmission medium [29].

False-Alarm probability(Pfa) = Ifa / 1000
Where Ifa is a failure of data in bitmaps.

Table 4: *False Alarm Probability*

Time	*IDS with Fuzzy rules*
5	*1.02*
10	*1.6126*
20	*1.6226*
30	*1.6327*
40	*1.7327*

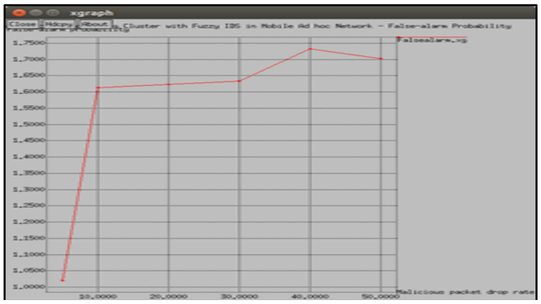

Figure 4*: Simulation Graph - False Alarm Probability*

- **Control Packet Dropping Rate**

Impact of control packet dropping rate

The frequency of synchronization hop is disturbed by the packet drop rate. During frequency synchronization resume the loss of packets transferred over the hop is occurred. Data packet losses and control loss may help to develop the detection accuracy in a considerable rate. Detection accuracy is a function of the control packet dropping rate.

Control Packet Dropping rate = CDL-Mdp

CDL - Control and data packet drop
Mdp - Malicious packet Drops

***Table 5:** Impact of control packet dropping rate*

Time (sec)	*IDS with Fuzzy rules*
5	*1.6*
10	*1.20782*
20	*1.14782*
30	*1.10748*
40	*1.01258*

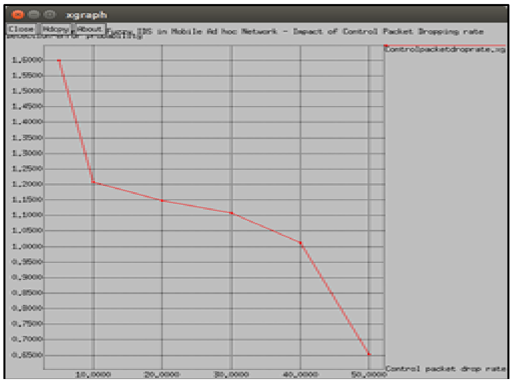

***Figure 5:** Simulation Graph - Impact of control packet dropping rate*

Impact of L data:
Data transferred between two nodes is L data. Average of data transmission failure among two successive nodes is estimated as L-data [30] [31].

L-data = 1 / (1 - PBG)

PBG -Packet loss rate

***Table 6**: Impact of L data*

Time (sec)	*IDS with Fuzzy rules*
5	*1.6*
10	*1.3074*
20	*1.3026*
30	*1.2927*
40	*1.0127*

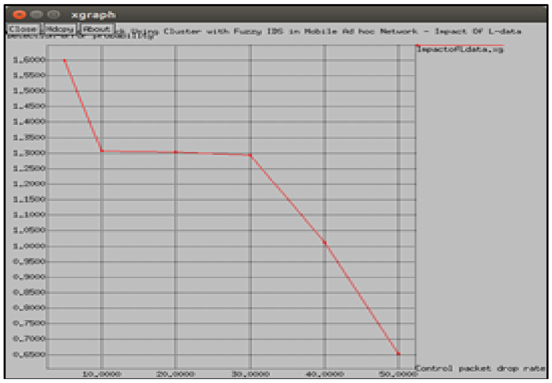

***Figure 6:** Impact of L data*

Impact of PGB :
During the transmission of any packets from source to destination are the transition probabilities from good to bad and from bad to well given by PGB.

PGB = Tpkt - Spkt

zTpkt -Total no of Packet loss
Spkt - Source of Packet loss

***Table 7:** Impact of PGB*

Time (sec)	*IDS with Fuzzy rules*
5	*1.02*
10	*1.5822*
20	*1.5922*
30	*1.6025*
40	*1.6726*

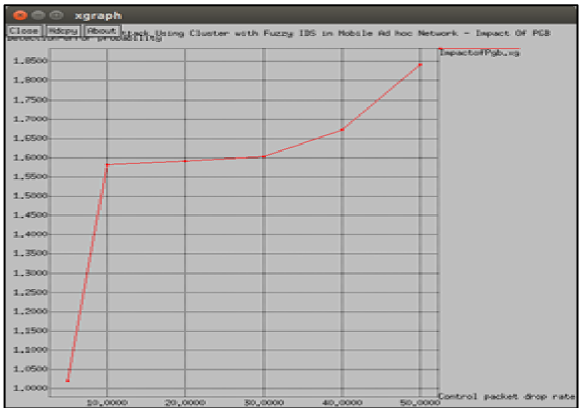

***Figure 7:** Simulation Graph - Impact of PGB*

- **Block-Based Detection**

Random Packet Drop
Random packet drop is losing occurs when one or more packets. The data is transmitting the network fail to reach their destination.

Random Packet Drops = Mpkt * Gpkt

Mpkt -Most recent packet sent
Gpkt - Generates a packet-reception

***Table 8:**Random Packet Drop*

Time	*IDS with Fuzzy rules*
5	*1.02*
10	*1.5722*

20	*1.5822*
30	*1.5925*
40	*1.6026*

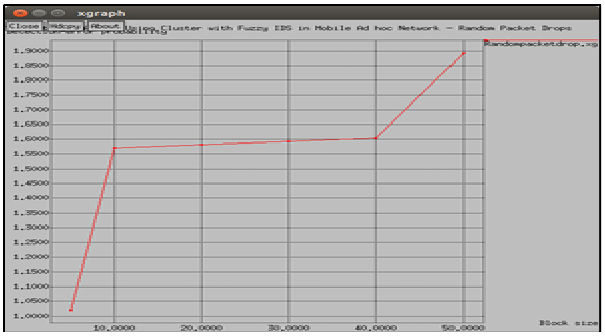

***Figure 8:** Simulation Graph - Random Packet Drop*

Impact of Sample Packets:

In order to attain consistency in detection accuracy two methods are carried namely sample packets are fixed to formulate the sample blocks. The sample blocks are fixed in respect to the block size.

Sample Packet = Bs * Ra

Bs -Decreases with the block size

Ra - Does not reduce the amount of computation

***Table 9:** Impact of Sample Packets*

Time (sec)	*IDS with Fuzzy rules*
5	*1.02*
10	*1.5622*
20	*1.5722*
30	*1.5825*
40	*1.7026*

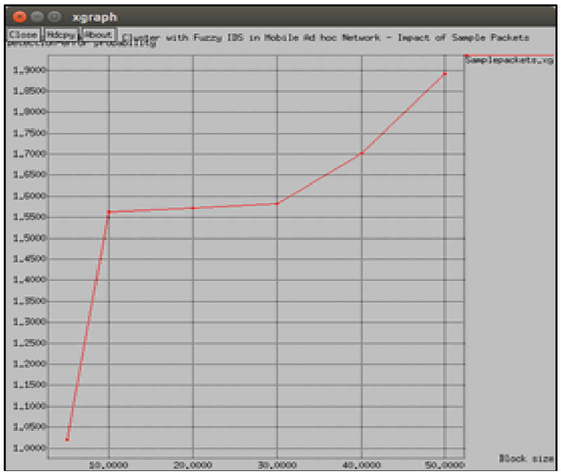

***Figure 9**: Simulation Graph - Sample Packets*

Selective Packet Drops :

Selective packet drop attack is associated with DoS attacks. Malicious nodes in the network trigger the DoS attack. Many techniques have been developed to segregate selective attacks from the network.

SelectivePacket Drops = Hdp + Ldp

Hdp -High packet dropping rate

Ldp - Low packet dropping rate

***Table 10:** Impact of Selective Packet Drop*

Time (sec)	*IDS with Fuzzy rules*
5	*1.02*
10	*1.5522*
20	*1.5622*
30	*1.5725*
40	*1.7026*

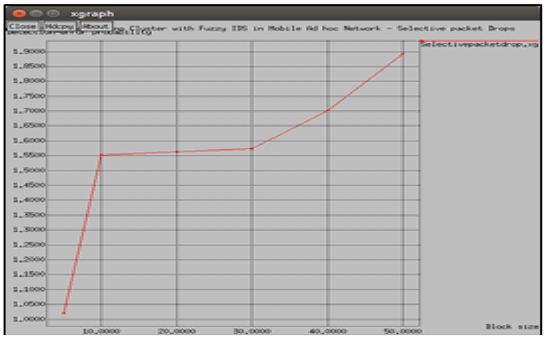

***Figure 10:** Simulation Graph - Selective Packet Drop*

6 CONCLUSION

Security is always a major issue in MANET and every node in the transmission can turn to a selfish or malicious node. Normal data transmission among the network can be influenced by the selfish or malicious node and can destroy the transmission flow in the MANET. In order to prevail over this issue clustering techniques are used to separate intrusive behavior nodes from the normal behavior node. The objective is to execute a smart intrusion detection system using a Data Mining technique and fuzzy rules in MANET. Improved intrusion system has the ability to identify the nodes which can inflict a threat to the network formed and should take remedies in advance so that the attack before its impact should be managed or controlled. Nodes in the network are limited with power hence the proper selection of nodes will decrease the energy utilization. Fuzzy rules help to choose the nodes accordingly and the energy is conserved efficiently. Several algorithms are proposed to face the challenges of IDS though IDS still met with varied challenges. Categorization of attack type is not yet proposed rather data identification, attack identification is more beneficial. Clustering also face challenges when the number of clusters exceeds the preferred limit. Mentioned limitations can be considered for future development of new IDS methodology.

7 REFERENCE

[1] Zhang, Y., & Lee, W. (2000, August). Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking(pp. 275-283). ACM.

[2] Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. IEEE communications surveys & tutorials, 15(4), 2027-2045.

[3] Debar, H., Dacier, M., &Wespi, A. (2000, July). A revised taxonomy for intrusion-detection systems. In Annales des telecommunications (Vol. 55, No. 7-8, pp. 361-378). Springer-Verlag.

[4] Chiang, C. C., Wu, H. K., Liu, W., &Gerla, M. (1997, April). Routing in clustered multihop, mobile wireless networks with fading channel. In proceedings of IEEE SICON (Vol. 97, No. 1997, pp. 197-211).

[5] Clausen, T., &Jacquet, P. (2003). Optimized link state routing protocol (OLSR) (No. RFC 3626).

[6] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., &Jamalipour, A. (2007). A survey of routing attacks in mobile ad hoc networks. IEEE Wireless communications, 14(5), 85-91.

[7] Karakehayov, Z. (2005). Using REWARD to detect team black-hole attacks in wireless sensor networks. Wksp. Real-World Wireless Sensor Networks, 20-21.

[8] Lee, S., Han, B., & Shin, M. (2002). Robust routing in wireless ad hoc networks. In Proceedings. International Conference on Parallel Processing Workshop (pp. 73-78). IEEE.

[9] Desilva, S., &Boppana, R. V. (2005, March). Mitigating malicious control packet floods in ad hoc networks. In IEEE Wireless Communications and Networking Conference, 2005(Vol. 4, pp. 2112-2117). IEEE.

[10] Hu, Y. C., Perrig, A., & Johnson, D. B. (2003, April). Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In Proceedings of INFOCOM (Vol. 2003).

[11] Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference (pp. 96-97). ACM.

[12] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., &Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. IJ Network Security, 5(3), 338-346.

[13] Zapata, M. G., &Asokan, N. (2002, September). Securing ad hoc routing protocols. In Proceedings of the 1st ACM workshop on Wireless security (pp. 1-10). ACM.

[14] Raju, J., & Garcia-Luna-Aceves, J. J. (2000). A comparison of on-demand and table driven routing for ad-hoc wireless networks. In 2000 IEEE International Conference on Communications. ICC 2000. Global Convergence ThroughCommunications. Conference Record (Vol. 3, pp. 1702-1706). IEEE.

[15] Johnson, D. B., &Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In Mobile computing (pp. 153-181). Springer, Boston, MA.

[16] Zhang, Y., Lee, W., & Huang, Y. A. (2003). Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9(5), 545-556.

[17] Mishra, A., Nadkarni, K., &Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. IEEE wireless communications, 11(1), 48-60.

[18] Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-Fernández, G., &Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. computers& security, 28(1-2), 18-28.

[19] Lunt, T. F., Jagannathan, R., Lee, R., Whitehurst, A., &Listgarten, S. (1989, March). Knowledge-based intrusion detection. In [1989] Proceedings. The Annual AI Systems in Government Conference (pp. 102-107). IEEE.

[20] Dickerson, J. E., Juslin, J., Koukousoula, O., & Dickerson, J. A. (2001, July). Fuzzy intrusion detection. In Proceedings Joint 9th IFSA World Congress and 20th NAFIPS International Conference (Cat. No. 01TH8569) (Vol. 3, pp. 1506-1510). IEEE.

[21] Kashyap, N. (2015, March). Smart intrusion detection system for MANET. In 2015 International Conference on Advances in Computer Engineering and Applications (pp. 252-177). IEEE.

[22] Huang, Y. A., & Lee, W. (2003, October). A cooperative intrusion detection system for ad hoc networks. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (pp. 135-147). ACM.

[23] Ping, Y., Xinghao, J., Yue, W., &Ning, L. (2008). Distributed intrusion detection for mobile ad hoc networks. Journal of systems engineering and electronics, 19(4), 851-859.

[24] Shams, E. A., &Rizaner, A. (2018). A novel support vector machine based intrusion detection system for mobile ad hoc networks. Wireless Networks, 24(5), 1821-1829.

[25] Jabbar, M. A., &Aluvalu, R. (2017). RFAODE: A novel ensemble intrusion detection system. Procedia computer science, 115, 226-234.

[26] Received from www.isi.ed

[27] u/nsnam/ns/tutorial Marc Greis tutorial on ns2

[28] Received from Matthias Transier " Ns2 tutorial running simulations "

[29] Butun, I., Ra, I. H., &Sankar, R. (2015). An intrusion detection system based on multi-level clustering for hierarchical wireless sensor networks. Sensors, 15(11), 28960-28978.

[30] Received from https://www.igi-global.com/ dictionary/ miss-detection-probability/46227

[31] Received fromhttps:// www.sciencedirect.com/ topics/ engineering/packet-loss