International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

An Efficient Multi Level Intrusion Detection System for Mobile Ad-Hoc Network Using Clustering Technique

K. Bala, A.Chandra Sekar, M. Baskar, J. Paramesh

Abstract: ***Mobile Ad-Hoc Network (MANET) is constructed using autonomous self-disciplinary nodes that communicate and exchange information through wireless medium. VM based IDS identify the attacks in the Virtual Machine Level with isolated properties of data center at the cloud. This is efficient only at the data center level i.e. infrastructure level. These problems are addressed by the proposed multi – level IDS for MANET using clustering technique. It identifies the black-hole attack from the external level to internal level. The pattern of the internal as well as external attacks are extracted and stored into the knowledge base for further analysis. The nodes are clustered and select an arbitrary node as a cluster head. The topology also monitored for maintaining consistency over the detection. The MANET packets are compared with the knowledge base to detect the malicious packets. The malicious node can also be eliminated from the network. Various modern IDS tools are analyzed with large set of attacks in multiple levels in order to maintain high reliability. Different algorithms are compared with proposed IDS in performance evaluation metrics such as IDS rate, Positive Rate and alarm rate and so on. The proposed IDS provides high accuracy when compared to existing algorithms in all levels.***

Index Terms : Mobile Ad-hoc Network (MANET), Intrusion Detection System (IDS), Route Request (RREQ) and Route Reply (RREP), Security Event Manager (SEM).

I. INTRODUCTION

This article deals with Intrusion Detection System (IDS) with MANET. This type of IDS uses various levels of attacks detection, both network based as well as host based. Related work provides complete overview of the IDS. Conceptual diagram indicates the various forms of IDS and advantageous of the proposed IDS. Various attacks and relevant features are used for pattern identification during attack detection. Algorithm provides the properties like attack classification, cluster formation and malicious packets identification and isolation. Recent tools related to IDS are analyzed with various performance parameters. Various algorithms with attack types are assessed for better efficiency. Accuracy of the proposed algorithm is compared with different algorithms.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Mrs.K.Bala*, Research Scholar, Faculty of ICE (Department of CSE), Anna University, Chennai, Tamilnadu, India.

Dr. A.Chandra Sekar, Professor and Head, Department of CSE, St. Joseph's College of Engineering, Tamilnadu, India.

Dr. M. Baskar, Department of CSE, SRM Institute of Science and Technology, Kattankulathur, Kancheepuram, Tamilnadu, India.

Mr. J. Paramesh, Associate Professor, Department of Information Technology at Misrimal Navajee Munoth Jain Engineering College, Chennai, Tamil Nadu.

II. RELATED WORKS

Two types of security attacks are raised by intruder. They are active attacks and passive attacks. Active attacks affect the integrity and availability of information. Passive attacks affect the confidentiality of the data without any modification. These attacks are generated by internal intruder and external intruder. Intrusion is a malicious activity done over the network for disturbing its operation. This is detected by implementing IDS (Intrusion Detection System) algorithm in order to improve the network performance. There are two types of IDS (Intrusion Detection System) namely internal and external. Internal IDS detect the unwanted activity within the network called host based where as external IDS detects the activity over the entire network.

Knowledge base is a database which stores the behavior of intruder. IDS extracts the behavior of the intruder and stores it in the knowledge base. Then it collects the intruder's behavior from the knowledge base and compares it with incoming packet's behavior for identifying the malicious activity. The knowledge is represented as patterns or rules with related attributes. Various expert systems are available for IDS which are restricted to specific pattern. It can be addressed by using efficient algorithm with real time attack detection. The undetected classified malwares are detected by using Intrusion prevention technique. The proposed algorithm uses both internal and external attack characteristics which are used to detect both host level and network level intrusions. Proposed MANET based IDS uses the better accuracy with high reliability over the internet. Topology is considered as a main element for detecting maximum attacks in order to achieve high performance when compared to other IDS algorithms.

Normally the intruder uses the shortest path to the desired source node for collecting the packet. It generates the malicious packets without any route exit in the corresponding destination. All packets use the malicious node as route to any other node. The malicious node is called black hole node. These types of nodes are collecting the packets from source node. This type of attack is called black hole attack. Block hole node always replies the response quickly with shortest path to the initiator. MANET always isolates such kind of malicious nodes with better performance and security. The proposed IDS detects the black hole attack and also isolates the unwanted malicious node from the current list.

III. CONCEPTUAL DIAGRAM

Intrusion Detection System is classified into external and internal. IDS is used to identify the intruder in the network and alert the administrator to perform corrective action against the network malfunctioning. The firewall filters the unwanted packets which are coming from the internet. The attackers are doing various attacking activities to intrude the network resources. IDS is an efficient mechanism for maintaining networks in the trusted manner. Internal IDS is deployed in the host level which always monitor the malicious packets and malicious nodes. The integrated version of IDS can be implemented for better security. The proposed IDS provide efficient and high performance security over the MANET with reliability. Figure 1.1 presents the basic conceptual diagram of the network based Intrusion Detection System. Figure 1.2 represents the host based Intrusion Detection System. Figure 1.3 shows the integrated Intrusion Detection System. The proposed Intrusion Detection System is depicted in Figure 1.4.

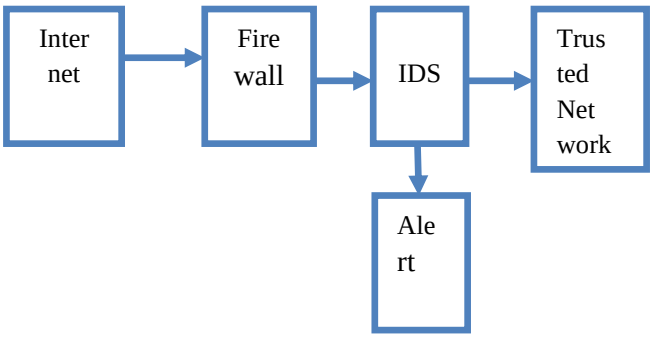

Figure 1.1 Network Based Intrusion Detection System

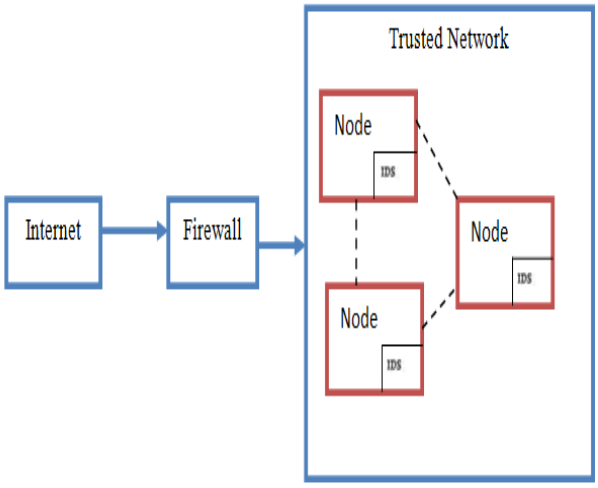

Figure 1.2 Host Based Intrusion Detection System

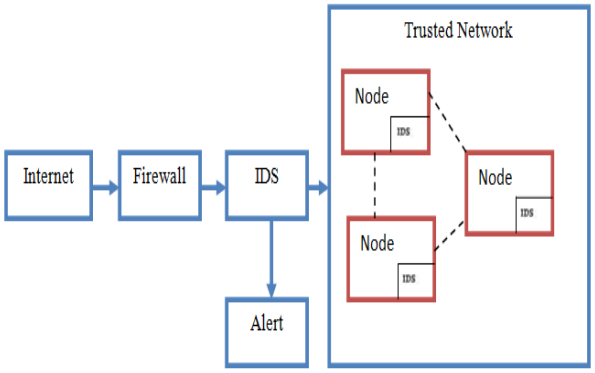

Figure 1.3 Integrated Intrusion Detection System

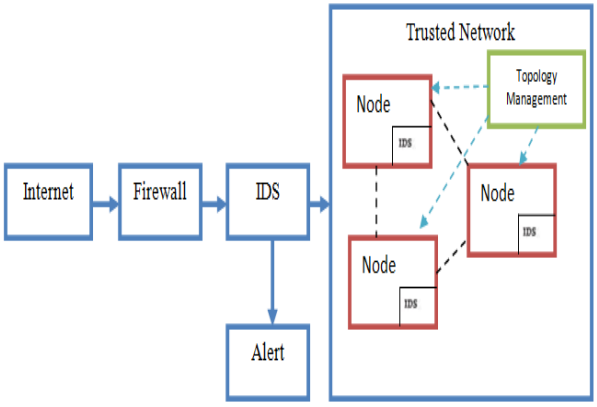

Figure 1.4 Proposed Intrusion Detection System

IV. PROPOSED METHODOLOGY FOR INTRUSION DETECTION SYSTEM

Initially the known attacks are identified from various sources of MANET for identifying the patterns in the form of rules and its characteristics of the attacks. These rules are stored in the database called knowledge base with standard specification. The pattern is in any form of attributes which is suitable for attack detection during the interaction. Normally the nodes in the MANET are considered as independent nodes i.e. no interaction between them. These nodes are clustered to form a network which is suitable for the packet exchange. The topology gives the complete layout of the nodes in the network. If there is any change in the topology then the nodes are clustered which are suitable for the network from the node list. New cluster head is selected for further process. The network is formed from the new node list and the process is repeated until no change comes in the topology. Source node sends the packet to the destination node though pre-specified route by sending RREQ packets to its entire neighboring nodes. All nodes send RREQ packet to other neighboring nodes and so on. Once the flooding process gets completed then all nodes send RREP packet to the source node. The source node selects the path from the received list then starts the data transmission process. Source node has no ability to find the malicious node before sending the packet to the destination. Source node always use packets with fields like source

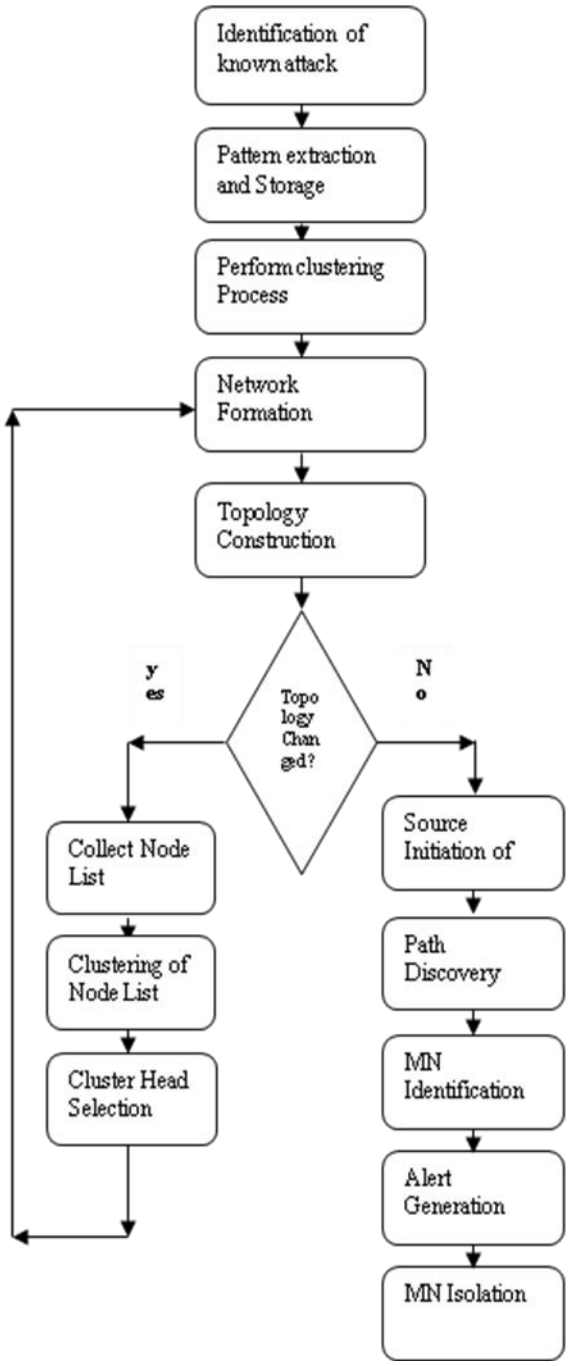

Figure 1.5 Flow Diagram For The Proposed Intrusion Detection System

address, destination address, sequence number and hop count to other node. The problem of identifying the malicious packet from malicious node is addressed using IDS method. The proposed IDS algorithm use packets and its patterns with attributes for route discovery. If any of the node sends the RREP to the source node with minimum number of hop count with quick reply considered as a malicious node. Suppose more than one node are having same hop count and sequence number with RREP then the node which is having least sequence number is marked as a malicious node. This node will be isolated from the network. Figure 1.5 shows the flow diagram for the proposed IDS algorithm in the MANET. Table 1.1 shows the features list which is extracted from network packets using CICFlowMeter-V3. Table 1.2 represents various attack types of the MANET.

Table 1.1 CICFlowMeter-V3 features List

Attack name	Attack Description
buffer_overflow	User to Root
ftp_write	Remote-to-Local
guess_passwd	Remote-to-Local
Imap	Remote-to-Local
Multihop	Remote-to-Local
Neptune	Denial of Service
Perl	User to Root
Phf	Remote-to-Local
Pod	Denial of Service
Portsweep	Probe
Rootkit	User to Root
Smurf	Denial of Service
Spy	Remote-to-Local
Teardrop	Denial of Service
Warezclient	Remote-to-Local
Warezmaster	Remote-to-Local

Table 1.2 Attack types

Feature List	Description
fl_dur	Duration of the flow
tot_fw_pk	Total packets in outgoing flow
tot_bw_pk	Total packets in incoming flow
fl_byt_s	byte transferred rate per second
fl_pkt_s	packets transferred per second
fl_iat_avg	Average flow time
fl_iat_max	Maximum flow time
fl_iat_min	Minimum flow time
fw_pkt_s	Request packets per second
bw_pkt_s	Response packets per second
pkt_len_min	Minimum flow length
pkt_len_max	Maximum flow length

V. ALGORITHMS FOR PROPOSED IDS

Algorithm attack_classification()
Begin
Let known attack list as KA;
Collect the KA from different networks and sources;
For each attach ε KA do
Begin
Identify the attributes of the attack;
Select the pattern of the identified attributes;
Classify the attributes as ATTLIST using K-Means Clustering
If ATTLIST == Network based then
For each attribute ε ATTLIST do
Begin

```
        Identify network attribute list  NAT;
                Generate the pattern as NPAT;
                Store the pattern in the storage;
        End
End
        Else if ATTLIST == Host based then
            For each attribute ε ATTLIST do
            Begin
              Identify host attribute list HAT;
              Generate the pattern as HPAT;
              Store the pattern in the storage;
            End
                End
        Return NPAT and HPAT;
End.

Algorithm Cluster_Formation()
Begin
Let N1, N2,…,Nn be  Node_List in MANET
AC= attack_classification()
For each node ε Node_List do
Begin
    Select node as cluster head of  MANET i.e. MN;
    L1: If node== MN then
    Begin
      Choose the next node in the Node_List except MN;
       Form the cluster as C;
       Construct the topology as TP;
        Set Status= true
    End
For each node ε TP do
Begin
Check the topology status
If Status== True then
Begin
   Topology is same i.e. not changed
    IDS (TP, AC);
End
Else
Begin
  Topology gets changed;
  Collect the node from the Node_List;
   Perform the clustering process;
  Choose the new cluster head for current topology;
  Goto L1;
          End
      End
   End
End

Algorithm IDS (topology TP, Attack ATTLIST)
Begin
Let packet with attributes as P;
Let sequence number as SN;
Let source address as SA;
Let Destination address as DA;
Let Hop count as HC;
For each node ε TP do
Begin
   L2:Maintain flow pattern for TP;
   Identify the packet pattern p;
   Choose the destination;
   Send the packet <SA, DA, HC, SN> to the destination
   along the path;
Compare the packet pattern with database;
If match == found then
   Set the packet as malicious;
   Alert the network administrator for attack;
   M_Node=Malicious_Node_Detection ();
   Isolate M_Node from the cluster and TP;
   Reform the cluster with new cluster head;
   Else
       Packet is not malicious
    End
  Goto L2;
  End
End
Algorithm Malicious_Node_Detection ()
Begin
Let  S is a Source Node;
Let D is a Destination Node;
Let Seq is a Sequence Number;
Let N is a Node List;
For each node ε S do
Begin
  Send the RREQ message to all neighboring nodes;
   Initiate the route discovery process;
   Wait for RREP message from other nodes;
    If RREP.count > 1 then
  If  N and Seq are equal then
  Select the node with minimum hop count as MN;
   Mark MN as malicious node;
            End
        End
     End
  Return MN;
End
```

VI. COMPARISON OF VARIOUS IDS TOOLS

Security Event Manager (SEM) uses integrated IDS of both host based as well as network based which provides complete information for network security. It has the features like generic report generation, security event correlation, threat prevention, monitoring of integrity and forensic analysis. It maintains the intelligent security center which provides the monitoring as well as the attacks are detected quickly. Snort is an IDS which follows network based detection and prevention model. It has features like real time packet analysis and log maintenance over internet.

It performs the task like analysis of networking protocol, searching of data and so on. It also detects the attacks such as scanning of port, attack in CGI scripts and operating system malfunctioning etc. Three types of rules can be used by snort namely alert, log and pass rule. Alert rule generates the alert whenever attack is happened. Log rule maintains the packet and its characteristics. Pass rule identifies the malicious packet and drop the packet from network. OSSEC is a host based intrusion detection system with high level of configuration for maintaining suitable rule management process. It allows the user to change the rules whenever the attacks are raised. This is controlled by writing the related script with rules in order to take corrective action against alert. It supports multiplatform IDS which handle generic attacks from various sources. Non compliant malicious action

and file system modification are detected by this system. Suricata is a network IDS which is used to detect the threat occur in the network level. It performs the activity like real time IDS, intrusion prevention method, network monitoring and offline packet processing etc. It is a rule and signature based IDS which is used to detect complex attacks using the custom scripting support. It uses different IO packet formats with high efficiency and security. Bro is network based prevention system with monitoring capability. It is used to detect the network anomalies occurred related to behavioral pattern in cyber security domain. It also performs the operations like immediate alert response, forensics, record mining and hashing. These IDS systems are based on the application oriented intrusion detection. So the effective hardware and software based IDS can be implemented for efficient operation. This is overcome by using proposed IDS model with dynamic topology with clustering technique.

VII. ANALYSIS OF VARIOUS IDS ALGORITHMS

Negative Selection Algorithm (NSA) is suitable for flexibility and scalability problem by implementing the model such as self and non self category. It gives better intrusion detection rate over the network with intruder elements like internal and external. It also checks the network whether the intruder present or not. It is not suitable for MANET attacks like RCA attack, flooding attack, black hole and warmhole attack. Detection rate of read, write, lock and kill operation is 1.115ms, 0.218ms, 0.325ms and 0.310ms respectively (Anass Khannous et al, 2014). Multi-agent intrusion detection algorithm (MIDA) controls the illegal packets and also detects the attacks on the Internet. It extracts and selects the features which are used to perform intrusion detection operation in scalable and reliable manner. It also compares with various feature selection methods for increasing the true detection rate and reducing false detection rate. The detection rate of MIDA algorithm related to attacks such as probe, UR2 and R2L is 0.46%, 0.41 and 0.79 respectively (Yi Gong et al, 2014). It can be applied to real time industrial attack detection and management. Intelligent intrusion detection system is used to detect the anomaly and misuse of network elements in an optimized manner. Optimization techniques are derived from Genetic Algorithm (GA) based approach. The feature space is reduced by considering the neural network based analysis with high dimensional perspective. Fuzzy rules are also applied with the rules for clustering the preprocessed information. It achieves better detection rate and minimum false alarm rate with high reliability (Yu-Ping Zhou et al, 2010). MANET is a self organized network which is used to initiate the data transfer among other nodes. So it suffers from various attacks while transmitting the data. IDS with Fuzzy systems provide efficient identification mechanism for secure communication among the various nodes. The identified threats are categorized in to various levels for prevention of successive attacks. The performance parameters like packet delivery ratio, drop count of the packet and jitter of the MANET based IDS with fuzzy systems are 1, 0 and 11.21 respectively (Vishnu Balan et al, 2015). Support confidence based IDS framework uses IDS with suitable patterns with flexible GA operations. These patterns are used to detect the intrusion over the network with related weights. The accuracy of the IDS is less because of the train and error practice applied over the MANET. False positive rate is almost equal in all cases when compared to False negative rate which leads into the performance problem (Dheeraj Pal et al, 2014). Baskar et.al.,(2017) Implemented a low rate DDoS attack detection algorithm which combines four different models. Each model works based on the traces of previous access. This needs huge amount of data to be transferred between the controlling devices to the source which manipulate the data to identify the low rate attack. Similarly in [31], the presence of network threat is detected in a region based approach, which uses the traces generated at specific region towards mitigation. Holland's classifier is a classifier which is used to detect the attacks using immune system. It is applied over entire network with external intruder detection. It achieves maximum detection rate 90 % and false rate is 10% over network nodes and intruders. This system has various phases such as Detection phase, Negative Selection phase, Tolerization phase, Memorization phase and Co-Stimulation phase. These phases detect the attacks with detection percentage, false rate and negative percentage is 90.57%, 17.21 and 9.425 % respectively (Arisoa S. Randrianasolo and Larry D. Pyeatt, 2016). IP spoofing detection IDS method is used to detect the anomaly packets in IP level. It considered the parameters like source address of the packet, dynamic configuration; flow management for high efficient detection of IP based attack detection. Flow of the packets is organized using fuzzy based scheme with auto selection of flow path against flooding attack. Packets related flow control comprises of various fields such as IP of source and destination, port of source and destination with suitable protocol field. Initially alarm rate is low which grows high whenever true detection reaches maximum threshold level (Sui Song, C. N. Manikopoulos, 2006).Experimental evaluation uses 20 nodes in the MANET then maintain 18 nodes are of normal nodes and 2 nodes are of malicious nodes. Movement of the nodes is selected in random model. Number of flow is 6 and traffic type is CBR (Constant bit Rate) and FTP (File Transfer Protocol). The packet rate is 2 packets per byte. Data Payload is set to 1024 bytes and transmission range is 300 meter. Figure 1.6 and Figure 1.7 represents the comparison of packet delivery ratio over various attacks and its categories. Packet drop of various attacks and its comparison is shown in Figure 1.8 and Figure 1.9. Jitter comparison is shown in Figure 1.10 and Figure 1.11.

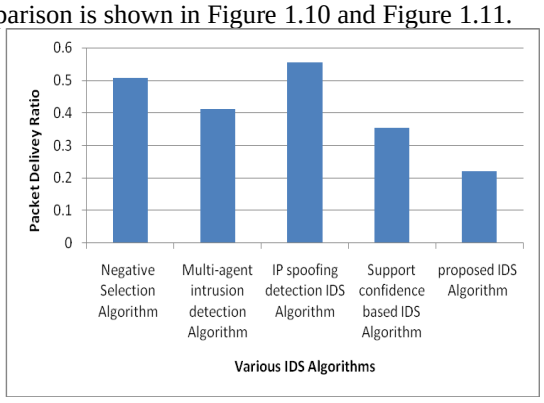

Figure 1.6 Comparison for packet delivery ratio with attack

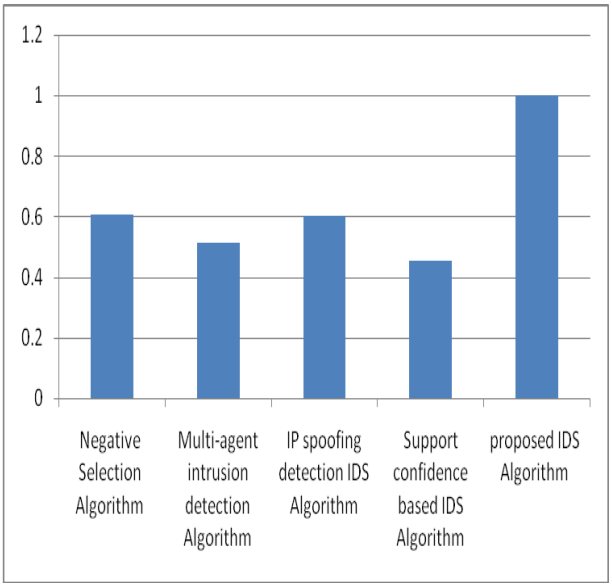

Figure 1.7 Comparison for packet delivery ratio without attack

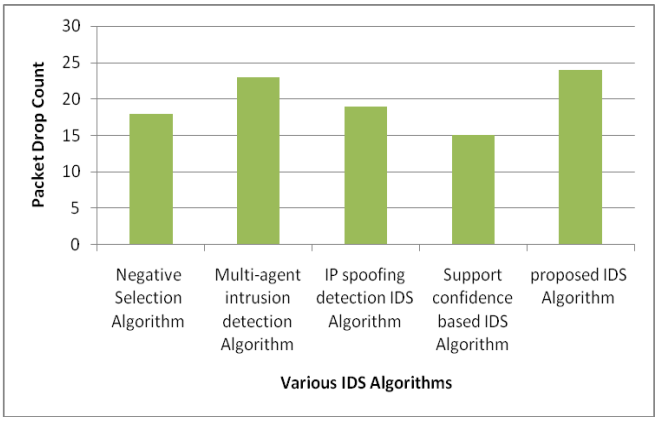

Figure 1.8 Comparison of packet drop with attack

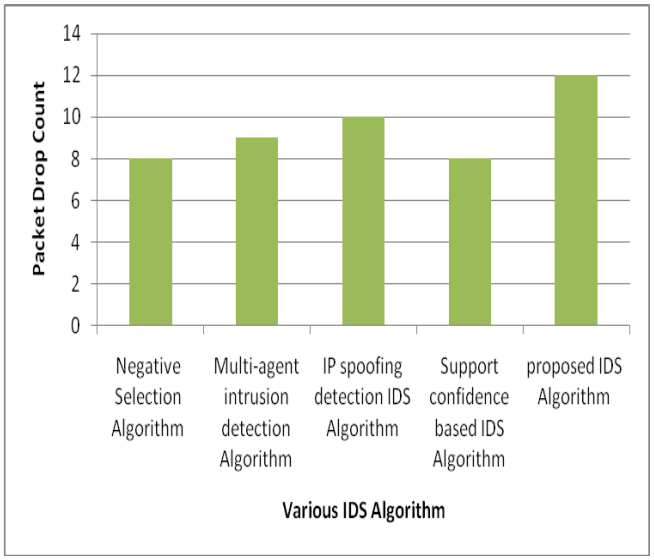

Figure 1.9 Comparison of packet drop without attack

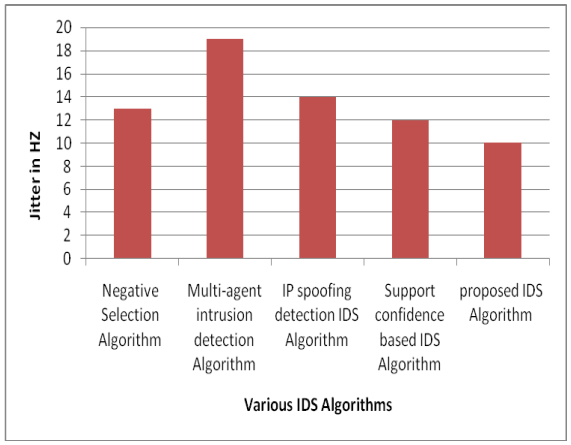

Figure 1.10 Comparison for Jitter with attack

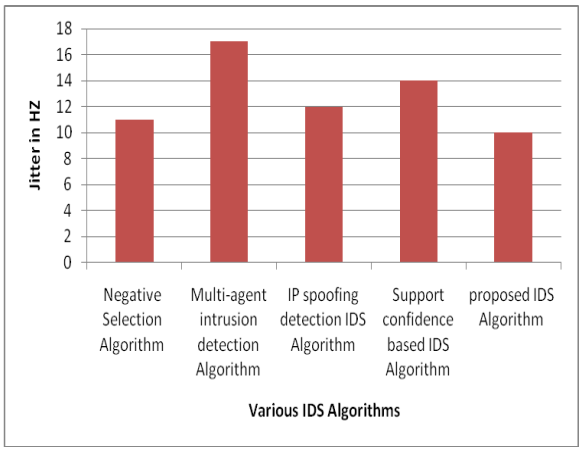

Figure 1.11 Comparison of Jitter without attack

VIII. RESULTS AND DISCUSSIONS

Performance evaluation of the IDS categorized into three types namely threshold based, Ranking Based and Probability based (Gulshan Kumar, 2004). Threshold based IDS predict the attack which is very close to the predefined value. It includes the types like F-measure, classification rate and recall etc. The order of the attack detection is done by rank based approach which includes the parameters such as False Positive Rate, False Negative Rate, Detection Rate and precision etc. The attack detection is related to the probability of occurrence with False negative condition is called probability based approach with mean square error, root mean square error and so on. True Positive (TP) is a successful condition of attack detection. True Negative (TN) is a condition when no attack has taken place and no detection has taken place. False Positive (FP) is a condition that produces an alarm when no attack has taken place. False Negative (FN) is correct labeling of authorized user and False Negative is a rate at which the intrusion is not detected properly. Proposed IDS algorithm is analyzed and experimented using the MANET and IDS concepts with clustering and reliable topology. The analysis is carried out based on different evaluation metrics with multi level perspectives. True Positive Rate (TPR) metric is calculated ratio between True Positive and combination of False Negative. False Negative Rate is calculated with FN and combination of FN and TP.

IDS rate is measured over the total number of attacks and detected attacks. False alarm also reduced by assessing the rate using False Alarm Rate (FAR). Genetic Algorithm (GA) based IDS algorithm achieves maximum success rate with minimum false rate. Fuzzy based IDS uses various association rules with minimum support and confidence level when compared to GA based IDS algorithm. Hybrid IDS performs detection operation over both internal network and external network by handling any kind of intruders with maximum accuracy. Multi-agent IDS improves the performance by minimizing the traffic analysis and data processing time while performing detection operation. It uses reduced running time when compared to existing algorithms.Proposed IDS achieves high accuracy when compared to existing algorithms by considering parameters like reliability, distance, memory, processing, power, precision and so on. Figure 1.12 represents the comparison of various algorithms and its detection rate. Figure 1.13 and Figure 1.14 presents the true positive and false positive rate comparison respectively. True alarm rate and false alarm rate comparison is shown in Figure 1.15 and Figure 1.16. Accuracy of various algorithms over different set of attributes which are related to detection of the attack is shown in Figure 1.17.

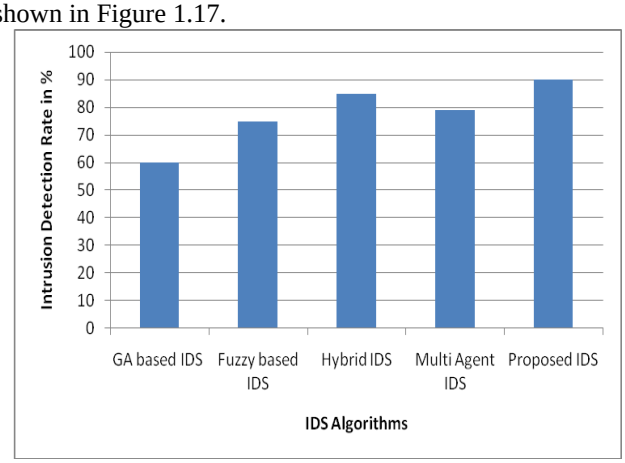

Figure 1.12 Intrusion Detection Rate comparison

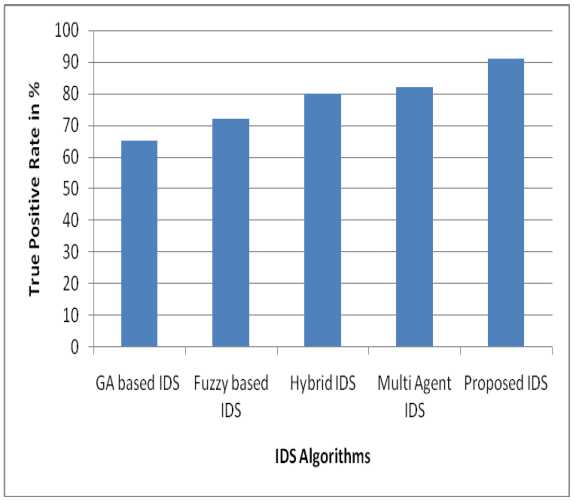

Figure 1.13 True Positive Rate comparison

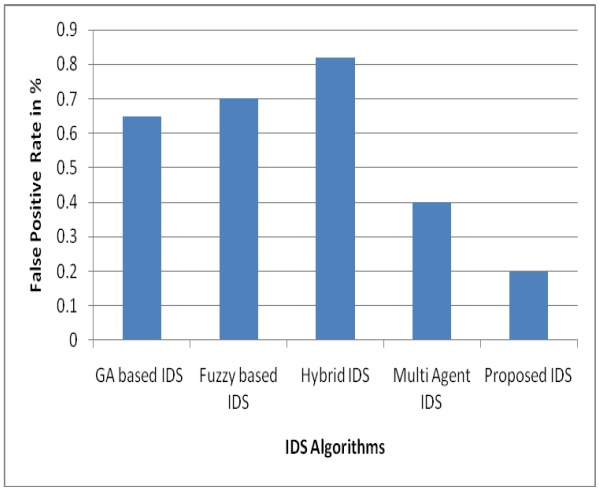

Figure 1.14 False Positive Rate comparison

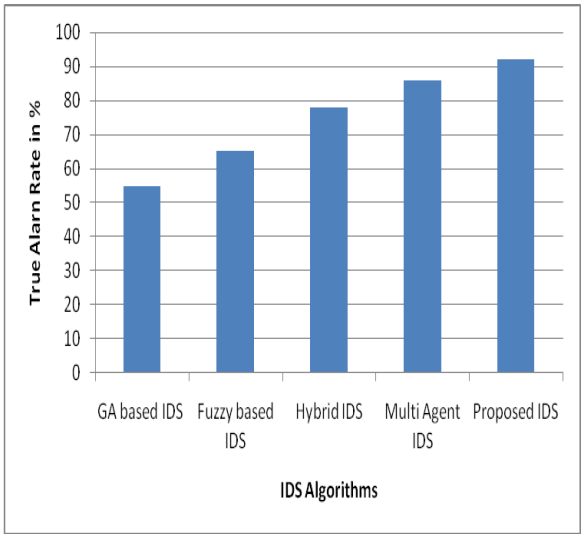

Figure 1.15 True Alarm Rate comparison

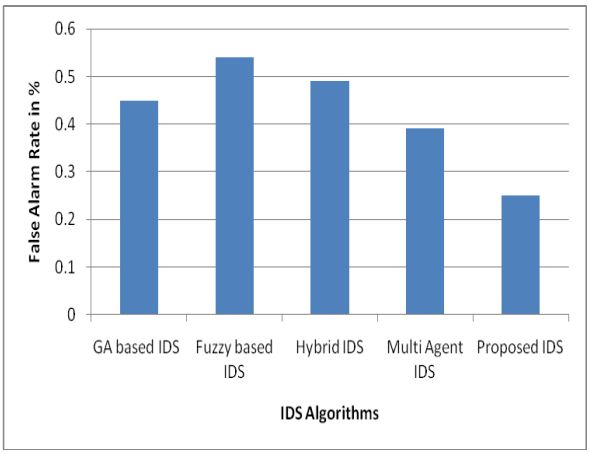

Figure 1.16 False Alarm Rate comparison

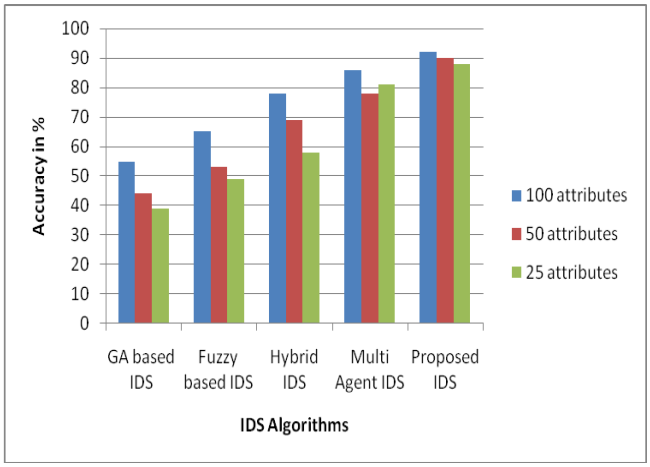

Figure 1.17 Accuacy Vs Attributes

IX. CONCLUSION

The proposed multi level IDS for MANET using clustering technique identifies the black-hole attacks of MANET and also analyzed the pattern related to internal and external intruder. Attacks are classified using K-Means clustering and selected the suitable list of nodes with cluster head. Topology maintenance is carried out in order to detect the attack consistently. IDS tools are analyzed and made a comparison over various systems with properties and its attributes. IDS algorithms are compared and identified the issues related to the MANET. The accuracy of the various algorithms are calculated and compared with the proposed IDS method with high reliability.

REFERENCES

1. PreetiSachan, and Pabitra Mohan Khilar, "Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism", International Journal of Network Security & Its Applications (IJNSA), vol. 3, no. 5, 2011.
2. Ramanathan Ram and Jason Redi, "A Brief Overview Of Ad Hoc Networks: Challenges and Directions", IEEE communications Magazine, vol. 40(5), pp. 20-22, 2002.
3. Sankaranarayanan, S, Murugaboopathi, G, "Secure Intrusion Detection System in Mobile Ad Hoc Networks using RSA Algorithm", Proceedings of the Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), pp. 354–357, 2017.
4. Sandeep Rai *et al*, "Cluster Based Energy Efficient Authentication Scheme for Secure IDS over MANET", 7th International Conference on Communication Systems and Network Technologies (CSNT), DOI: 10.1109/CSNT.2017.8418537, IEEE, pp. 1-7, 2017.
5. Shimbre., Nivedita, and Priya Deshpande, "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm", Computing Communication Control and Automation (ICCUBEA), International Conference on IEEE, 2015.
6. Shubham, B, "Advanced Channel Aware AODV Routing Protocol in Mobile Ad Hoc Network", International Journal of Engineering Technology and Management, vol. 1(1), pp. 61–66, 2013.
7. Swapnil Shinde, Ashwini Bangar, Manali Tawde, "Comparative Study and Analysis of IDS Implementation in Cloud Computing Environment", IOSR Journal of Computer Science, pp. 33-39, 2014.
8. Silva, E, Da Silva, and Albini, LCP, "Resisting Impersonation Attacks in Chaining-Based Public-Key Management on MANETS: The Virtual Public Key Management", Proceedings of the International Conference on Security and Cryptography (SECRYPT 2009), INSTICC, pp. 155–158, Jul 2009.
9. Singla, ER, and Singh, EJ, "Node-Disjoint Multipath Routing Based on AOMDV Protocol for MANETS", International Journal of Computer Science and Information Technology, vol. 5(4), pp. 5491–5496, 2014.
10. Sobh, TS, Mostafa, WM, "A Cooperative Immunological Approach for Detecting Network Anomaly", International Journal of Applied Soft Computing, vol. 11(1), pp. 1275–1283, 2011.
11. Sui Song, CN, Manikopoulos, "IP Spoofing Detection Approach (ISDA) for Network Intrusion Detection System", IEEE Sarnoff Symposium,DOI:10.1109/SARNOF.2006.4534792, IEEE, pp. 1-6, 2006.
12. Ashish Kumbhare, Manoj Chaudhari, "IDS: Survey on Intrusion Detection System in Cloud Computing", International Journal of Computer Science and Mobile Computing, vol. 3, issue. 4, pp. 497-502, April 2014.
13. Suresh, A, Reyana, A, Varatharajan, R, "Multi-Core Architecture for Optimization of Energy over Heterogeneous Environment with High Performance Smart Sensor Devices", International Journal of Wireless Personal Communications, 2018.
14. Suresh, A, Varatharajan, R., "Competent Resource Provisioning and Distribution Techniques for Cloud Computing Environment", International Journal of Cluster Computing, 2017.
15. Vijayarani, S, Maria Sylviaa, S, "Intrusion Detection System – A Study", International Journal of Security, Privacy and Trust Management, vol. 4, no. 1, 2015.
16. Vinay Rishiwal, Sandeep Kumar Agarwal, Mano Yadav, "Performance of AODV Protocol for H-MANETs", International Conference on Advances in Computing, Communication & Automation (ICACCA) (Springer), DOI: 10.1109/ICACCA.2016.7578898, IEEE, pp. 1-6, 2016.
17. Vincent, SSM, and Thamba MW, "Improving CA-AOMDV Protocol against Black-hole Attacks", International Journal of Computer Applications, vol. 5(4), 2012.
18. Waleed Bulajoul, Anne James, Mandeep Pannu, "Network Intrusion Detection Systems in High Speed Traffic in Computer Networks", IEEE, 2013.
19. WaliaHimanshu, Mandeep Singh, and Rahul Malhotra, "A Review: Mobile Ad Hoc Routing Protocols", International Journal of Future Generation Communication and Networking, vol. 9(2), pp. 193-198, 2016.
20. Abhishek Sawant, Jyoti Yadav, Avneet Kaur Arora, Janhavi Deo, Nutan Dhange, "Intrusion Detection System using Data Mining", International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, issue. 2, 2015.
21. Xu Wei-Qiang and Tie-Jun Wu, "TCP Issues in Mobile Ad Hoc Networks: Challenges and Solutions", Journal of Computer Science and Technology, vol. 21(1), pp. 72-81, 2006.
22. Yi Gong, Yong Fang and Liang Liu, "Multi-Agent Intrusion Detection System Using Feature Selection Approach", Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, DOI 10.1109/IIH-MSP.2014.137, IEEE, pp. 528-531, 2014.
23. Kiran Dhangar, Deepak Kulhare, Arif Khan, "A Proposed Intrusion Detection System", International Journal of Computer Applications, vol. 65, no. 23, pp. 0975-8887, March 2013.
24. Arisoa S Randrianasolo and Larry D Pyeatt, "An Artificial Immune System Based on Holland's Classifier as Network Intrusion Detection", 11th International Conference on Machine Learning and Applications, DOI: 10.1109/ICMLA.2012.92, IEEE, pp. 1-8, 2012.
25. BlazevicLjubica, LeventeButtyan, SrdjanCapkun, Silvia Giordano, JP, Hubaux, and JY, Le Boudec, "Self-Organization in Mobile Ad Hoc Networks: The Approach of Terminodes", IEEE Communications Magazine, vol. 39(6), pp. 166-174, 2001.
26. Carvalho, JMA, Costa, PCG, "Collaborative Approach for a MANET Intrusion Detection System using Multi Lateration", International Journal of Electrical and Computer Engineering Systems, pp. 59–65, 2016.
27. Baskar.M, Gnansekaran.T "Multi Model Network Analysis for Improved Intrusion Tracing towards Mitigating DDoS Attack", Asian Journal of Research in Social Sciences and Humanities, ISSN 2249-7315(Print): ISSN (Online) 2250-1665, Vol.7, No.3, pp.1343-1353, March 2017
28. Baskar.M, Gnansekaran.T "Developing Efficient Intrusion Tracking System using Region Based Traffic Impact Measure Towards the Denial of Service Attack Mitigation", Journal of Computational and Theoretical Nanoscience, Volume No.14, Issue No.7, pp: 3576-3582, ISSN: 1546-1955 (Print): EISSN: 1546-1963 (Online) , July 2017.

AUTHORS PROFILE

Mrs. K. Bala, Research Scholar of the Faculty of Information and Communication Engineering (Department of CSE) in Anna University, Chennai, Tamil Nadu. She has completed her Bachelor of Engineering Degree in Computer Science and Engineering from University of Madras, Chennai. She has completed her Master of Engineering in Computer Science and Engineering from Vinayaka Missions University, Salem. Her research interests include Network security, Mobile Ad-hoc Networks and Wireless Sensor Networks.

Dr. A. Chandra Sekar, Professor and Head of the Department of CSE at St. Joseph's College of Engineering, Chennai, Tamil Nadu. He has overall teaching experience of over 20 years in Engineering colleges. He has guided more than 12 Research Scholars and more than 50 M.E Students. He has published over 100 research articles in refereed International and National journals and he is guiding research scholars and M.E. students in the areas of Network Security, Cloud Security, Data mining, Artificial Intelligence and Big Data Analysis.

Dr. M. Baskar received B.E. Computer Science and Engineering from Anna University, Chennai, M.Tech. Information Technology from Sathyabama University, Chennai and Ph.D.,(Information and Communication Engineering) from Anna University, Chennai. His Area of research interest includes Computer Networks and Security, Parallel and Distributed Systems, Image Processing, Big Data, Machine Learning and IoT. He is published 20 Research Article in reputed International Journals and 10 Article in International Conferences. He is acting as a reviewer in Cluster Computing, Journal of Web Engineering, Multimedia Tools and Applications, Neural Processing Letters and Concurrency and Computation: Practice and Experience. He is a Life time Professional body member of CSI, ISTE, IET, ISRD, IRED, IACSET, IAENG, SDIWC and UACEE.

Mr. J. Paramesh, Associate Professor in the Department of Information Technology at Misrimal Navajee Munoth Jain Engineering College, Chennai, Tamil Nadu. He has overall teaching experience of over 21 years in Engineering Colleges. He has guided more than 150 UG and PG Students in the areas of Computer Networks, Information Security, Cloud Security, Data mining, Artificial Intelligence and Big Data Analysis. He has published over four research articles in refereed International and National journals.