INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET)

ISSN 0976 – 6367(Print)
ISSN 0976 – 6375(Online)
Volume 5, Issue 6, June (2014), pp. 01-10
© IAEME: www.iaeme.com/ijcet.asp
Journal Impact Factor (2014): 8.5328 (Calculated by GISI)
www.jifactor.com

IJCET

©IAEME

ANOMALY BASED DETECTION AND PREVENTION TO PROVIDE SECURE MANET USING DUAL HEAD CLUSTER IN HIERARCHICAL COOPERATIVE IDS

Ms. Maheshwari Sonawane[1], Prof. Saniya Ansari[2]

[1, 2]Department of Electronics & Telecommunications, DYPSOE, PUNE, INDIA

ABSTRACT

A purely wireless network wherein each device itself acts as a node and also performs the task of router is called as Mobile Ad-hoc network. A MANET has become a need of today's fastest developing era.

A measure issue in MANET is security as it is an autonomous system of nodes which has no fixed infrastructure and also, due to continuous movement of mobile nodes it has dynamic topology so it is difficult to maintain security. In our proposed system a cluster with dual head will be used in cooperative IDS for anomaly detection system .Two head nodes will be protecting each other from intrusion along with detecting intrusion for cluster member. This intrusion can be detected by signature analysis or anomaly based detection. Anomaly based detection will detect intrusion by monitoring the whole system activities. Our proposed system will also find attacks which are new and which were not possible to detect by using signature analysis. Proposed system will be able to detect the anomaly behaviour of the attacks like black hole, Dos and flood anomaly. As a result of our research work a stable, secure network will get formed.

Keywords: IDS, MANET, Cluster, Anomaly Detection system, Dos, Black –Hole Attack, Secure Network.

1. INTRODUCTION

Due to the need of fastest developing era users of network are now increasing day by day. Wireless network is becoming one of the fastest growing and demanding networks now a day. Mobile Ad-hoc Network is one of them. The applications of MANET range from a one-off meeting network, emergency operations such as disaster recovery to military applications due to their easy deployment [8]. MANET is an autonomous system which does not have any centralized administrative system. Each node of a network also serves as a router while itself being a part of a

network. MANET being a network of highly mobile nodes it has dynamically changing topology. Security is one of the measure issues in MANET because of the absence of centralized infrastructure, physically unsecure nodes, low power supply and its dynamic changing topology [1].

In order to provide security to MANET many protocols have been developed, lots of research work is still going on to provide the security to MANET. Other techniques such as Intrusion Detection Systems and clustering approach has also been adopted by researchers for strong security measure and also to improve the performance by considering limitations of the mobile nodes in the MANET and its dynamically changing topology. Various intrusion detection techniques which have been developed for wired network cannot get applied as it is on MANET as MANET is purely wireless network [1].

Co-operative IDS is type of architecture based IDS for MANET. To find the intrusion locally or globally task of detection is divided among several nodes in cooperative IDS system. So, the intrusion is detected by IDS agent i.e. node in that cluster and which is managed by the head in that cluster, such architecture is called as hierarchal cooperative IDS system. But if head node in that cluster get fail then whole cluster may get damage so, in our proposed system we are using two heads per cluster. Advantage of using two head per cluster is if any of the head stop working or if it gets down the system will not depend on that as we have secondary node to manage [1]. Energy of the nodes of MANET is a measure issue so, by having two head per cluster power will get saved also these two nodes will be protecting to each other from intrusion [1].

The anomaly-based IDS detect activities that are different from the normal expected system behaviour. Anomaly detection has some techniques to detect anomaly in network like statistical anomaly detection, anomaly detection using neural networks, immunology based system, data mining, and Chi-square test utilization. This system is also known as behaviour-based IDS, in which the normal behaviour of the network is captured, and then it is compared with the current behaviour of the network to detect anomaly in the network. Anomaly detection systems typically consist of two phases of operation training and testing.

Training is the process of modelling the normal behaviour of the network. This model generated by the training is then used as profile for the network and users. Stable profile is needed for anomaly based IDS to be effective. A profile consists of information about the list of parameters which are specifically geared to the target being monitored. Constructing an effective profile involves gathering information on behaviour and activity that is considered acceptable for the network.

Testing is the process of comparing the model generated by training process and the current network activities. The detection techniques usually involve statistical or mathematical approaches to flag any deviation between two models. For anomaly detection techniques to be effective, they must have mechanisms that keep the false alarm rate low.

ABID systems extensively use statistical methods [8] [9] to estimate the deviation between the expected and the current behaviour to detect an intrusion in the network. Statistical probabilistic techniques including the chi-square test, Hotelling's T2 test, decision trees and Markov chains are employed in ABID systems.

Neural network algorithms [10] have also been used to learn and model the behaviour of the users in the network. The key advantage of ABID systems is that they can detect new attacks. ABID systems can also provide early warnings of potential intrusions in the network. However, they are prone to generate false alarms.

Whereas in signature analysis, all available attacks are used as a database so, only repeated attacks are detected. But anomaly detection is based on the behaviour so, it can help in the formation of more secure and stable network. Here we use NS2 simulator to calculate result.

2. RELATED WORK

In order to provide security to MANET many researchers has performed it on hardware and software. MANET has tremendous range of applications in variety of fields.

Lee, Zhang and Huang (Zhang et al., 2003; Zhang & Lee, 2000) proposed an anomaly-based detection system that is cooperative and distributed. In this system, each node independently detects local intrusions and gathers information by using an IDS agent. And if needed, it cooperates with other neighboring IDS agents to increase the accuracy of detection. In this system, each operation is done by a given module in the agent. The key advantage of the system is that it is distributive and cooperative, and consequently it increases the accuracy. Its main disadvantage is that the responding time and the rate of false positive are high.

Kachirski and Guha (2003) proposed a multi sensor anomaly-based detection system that is based on the mobile agent technology. This system uses three main agent, monitoring, decision and action to detect the intrusion. The monitoring agent supervises the network and the nodes, the action agent is responsible for producing suitable response against the intrusion and the decision agent analyzes the gathered data for detection of intrusion.

This system is based on hierarchical structure and the agents. These agents are placed on nodes based on their function. Therefore, the action agent is placed on all nodes of the network and the decision agent is placed on some of nodes. The most important advantage of the system is applying the distributed mobile agents. Moreover, its most important disadvantage is that finding suitable nodes to appoint to main tasks is time-consuming and is more complex.

Sun et al. (2003) introduces a zone-based anomaly detection system. In this system, MANET is divided to several non-overlapping zones. In this system, the nodes are organized in two layers, intra-zone and inter-zone (or gateway nodes). Each node has an IDS agent that is executed on it. Other components of this system are data collection module, detection engine, local aggregation and correlation engine (LACE) and global aggregation and correlation engine (GACE). The data collection module and the detection engine are responsible for gathering the audit data and analysing every instant of intrusion respectively. The LACE module is responsible for correlation and aggregation of the local reported alerts. These alerts are broadcast for all nodes in the same zone. The function of GACE in this system is depends on the type of the node. If node is an intra-zone one, it just sends the reports to the inter-zone nodes. And if the node is an inter-zone one, it receives the reports from other intra-zone nodes, aggregates and correlates them and compares with its own reports and if needed it creates some alerts. The intrusion response module is responsible to produce suitable respond against the detected intrusion. In addition, this module is responsible to managing alerts received from GACE.

The key advantage of the system is dividing the network into non-overlapping zones and its main disadvantage is that the responding time is long.

Nakayama et al. (2009) proposed an anomaly-based detection system to detect malicious activities that target at the AODV routing protocol (Perkins et al., 2011). The proposed system uses the machine learning technique to detect the intrusion. So, after gathering the data step, then an approximate distribution of the normal behaviour is extracted. Then by analysing the gathered data and compare it with approximate distribution, system can find any deviation from normal behaviour. If the deviation exceeds the threshold, the system realizes that an attack was occurred. The main advantage of this system is the low rate of the false positive and the key disadvantage is that it cannot be used for detection of all possible attacks.

Joseph et al. (2011) proposed an anomaly-based detection system in the MANET to detect sinkhole attack (like those nodes that do not cooperate with the network in routing and forwarding operation). This system by a classifier can detect malicious behaviours. This system can gathered data from the network, MAC and physical layers. Then by processing the gathered data by the

classifier, a function created to make the decision. This function will distinguish whether the current event is legal or it is a result of sinkhole attack. The main advantage of this system is using the features of several layers and its main disadvantage is that it is used just to detect one type of sinkhole attack.

Lauf et al. (2010) proposed a two-stage anomaly-based detection system. Its goal is to act in environments with limited resources, like the MANETs. This detection system can be divided into two stages. The first stage for fast detection of the threat and, then compute a threshold for the second stage. While the second stage aims at exactly detecting the resources of the threat and also for detecting repeated attacks simultaneously. At the first stage in this system, an analysis is done on the gathered data, if any deviation was detected, then second stage is called. The main advantage of this system is that needed minimum amount of the resource. Because it is called the second stage only if it needed. The main disadvantage of the system is the high rate of the false positive.

Kabiri and Aghaeiin (2011) present an anomaly-based technique that focuses on denial of service (dos) attacks. The proposed system gets benefit from its neighbours' normal behaviours and analysis them based on the optimal features. Its main advantage is that it reduce the computational and data processing overhead by using a set of the optimal features. The key disadvantage of the system is that the system is exposed to high rate of false positive.

Nadeem and Howarth (2009) proposed an anomaly-based detection system for MANET to detect dos attacks. The proposed system detects the malicious behaviours based on statistical analyses. In this system, after gathering data, its probability distribution is estimated and it is compared with normal behaviour by using chi-square test (Lancaster, 1969). If the distribution of the gathered data does not fit the normal behaviour, then the observed behaviour is considered as a suspicious, for every suspicious behaviour, the counter increased a unit. Besides, in the case of exceeding the threshold, the node will be labelled as malicious.

The main advantage of this system is the low rate of false positive and its main disadvantage is that it is just able to detect dos attacks.

Albers et. al. [3] proposed a distributed and collaborative architecture of IDS by using mobile agents. A local intrusion detection system (LIDS) with every node can be extended for global concern to find the intrusion more effectively.

Security policy adaptation reinforced through agents (SPARTA), IDS based on mobile agent suggested by Krugel et. al. [6] and uses an event definition language (EDL) for the description of attacks.

Zeba Ishaq [1] proposed a system of Secure MANET using dual head cluster in Hierarchal Cooperative IDS he also has suggested that signature analysis will get replaced by anomaly detection to find the new attacks; this is the key guidance for our proposed system.

3. PROPOSED WORK AND METHODOLOGY

In our proposed system we are using Hierarchical Cooperative IDS. A MANET node typically has limited battery power and is not always efficient to make each MANET node the monitoring node for itself, especially when the threat level is low. We describe a cluster-based detection scheme where a cluster of neighbouring MANET nodes can periodically, randomly and fairly elect two monitoring node for the entire neighbourhood.

The normal traffic i.e. normal behaviour will be captured by the head node and if intrusion occurs or if any deviation in normal behaviour occurs the intrusion will get detected. By using this method we can detect new attacks.

To implement the anomaly detection technique NS2 is used in our proposed system, we have designed the MANET topology of 30 nodes using AODV protocol .The steps start with examining of

the simulated data by using (NS2) and ends with a graph representing the abnormal traffic and normal traffic in a time interval.

3.1 Simulation Environment

For simulation, of our research work we have set the parameter as shown in table I.

Table 1: Details of simulation parameters

Simulator	NS2 –(ver 2.34)
Simulation area	1000(m)x1000(m)
No of nodes	30
No of clusters	6
No of malicious nodes	1
Maximum bandwidth	2 Mbps
Simulation Time	1000 sec
Transmission range	250m
Traffic type	CBR
Routing protocol	AODV

The nodes are numbered from 0 to 29

3.2 Algorithm for Statistical Anomaly Detection

Advantage is our proposed system can detect the new attacks as well, it initially captures the normal behaviour of the system then it's easy to detect the deviation from normal to abnormal behaviour. So, to detect the new attack one should go for anomaly detection. Algorithmic explanation of anomaly detection is here [7]

1st step: Initialize Node
I =0 to 29
Initialize Threshold =value
2nd step: Transfer Packets in Sequential Node
For I=0 to 29
Transmit (node [i], node (i+1))
3rd step: If (Transmit (node (i), node (i+1)!)
Display "Anomaly Detected"
Then, If (Threshold==n)
Count status of each node (no of packets) = Counter
Threshold ≥ Counter
DDoS attack Detected i.e. Flood anomaly detected Else, Display "No anomaly found"
Packet Received (node (i), node (i+1)
Display Counter on Node [i] If (i==29) Xmt (node [i-(i-1)], node [i]) Display "Flash Anomaly Detected", go to call (III)
Above algorithm is for anomaly detection. Likewise we can add no. of detection techniques for known attacks and unknown attacks will be get detected by the deviation of the networks regular activities.

4. SIMULATION RESULTS

We have selected NS2, network simulator for this research work as it is open source tool and implements standard protocol as per RFC.

4.1 Design of Network

For implementation of our proposed system we have set up a MANET topology of 30 nodes.

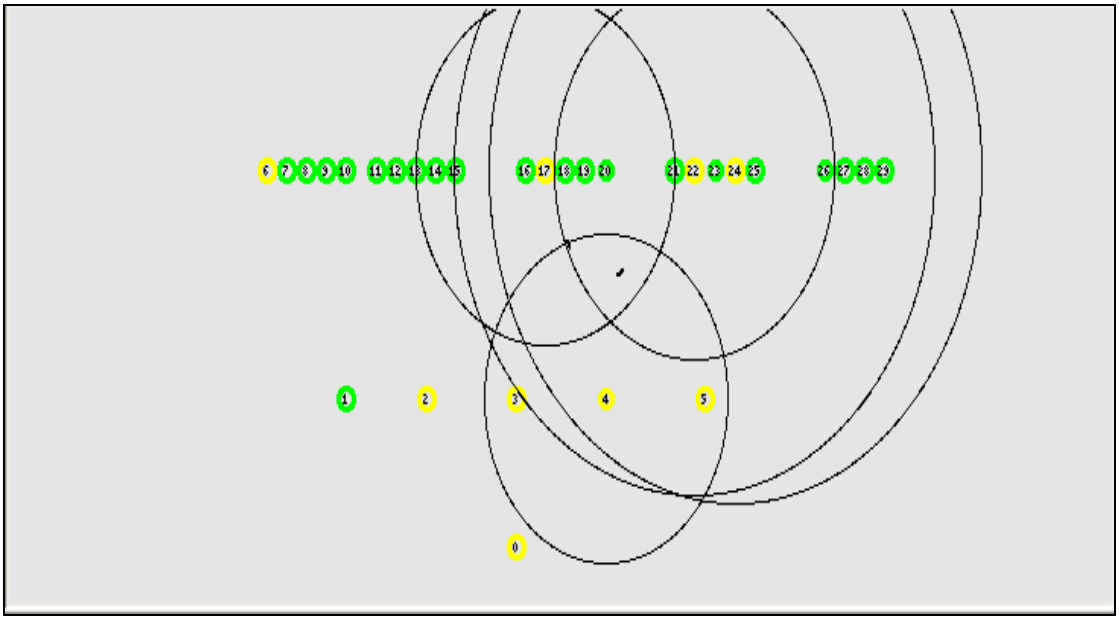

Fig 1: Design of the network

We have formed the cluster and selected the head node for each cluster which is more powerful and will be responsible for the entire cluster.

4.2 Anomaly Detection

```
Anomaly Detected for node: 3

Data Received Cluster5 = 87
Data Forwarded Cluster5 = 51
Anomaly Detected for node: 4

Data Received Cluster4 = 44
Data Received Cluster2 = 50
Data Forwarded Cluster2 = 33
Anomaly Detected for node: 1

Data Received Cluster5 = 88
Data Forwarded Cluster5 = 52
Anomaly Detected for node: 4

Data Received Cluster4 = 45
Data Forwarded Cluster4 = 22
Anomaly Detected for node: 3

Data Received Cluster2 = 51
Data Forwarded Cluster2 = 34
Anomaly Detected for node: 1

Data Received Cluster5 = 89
Data Forwarded Cluster5 = 53
Anomaly Detected for node: 4


[root@localhost ns-2.34]#
```

Fig 2: Detection of anomaly

Anomaly has been detected at head nodes of the clusters i.e. at nodes 1, 3 and 4

4.3 Performance Evaluation of Parameters

Network performance can be evaluated by considering following parameters.

4.3.1. Energy

In MANET each node has initial energy which get utilize for the communication. We have plotted a graph of utilization of energy vs. time and we concluded that due to attack detection energy utilization is more but after prevention of attach it get reduced, hence we have saved energy of nodes.

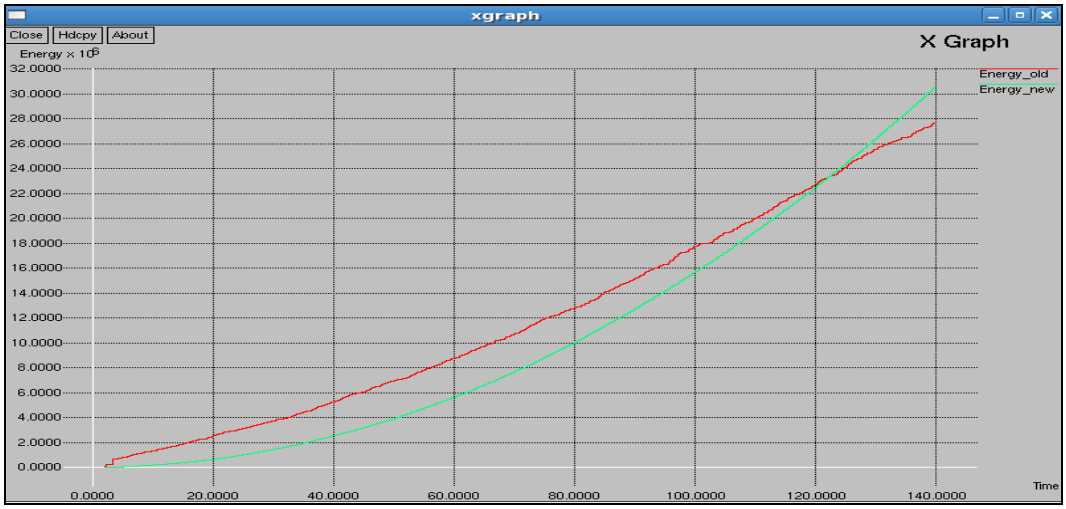

Fig 3: Energy Utilization vs. Time

4.3.2. Average End-to-end Delay

End-to-end delay is the time it takes for a packet to travel through the network from source to destination. The average end-to-end delay is the summation of all end-to-end delays divided by total data packets arrived at destination. We have plotted the graph of delay vs. time to evaluate the performance of after attack and after preventing the attack. It is observed that delay is more after prevention.

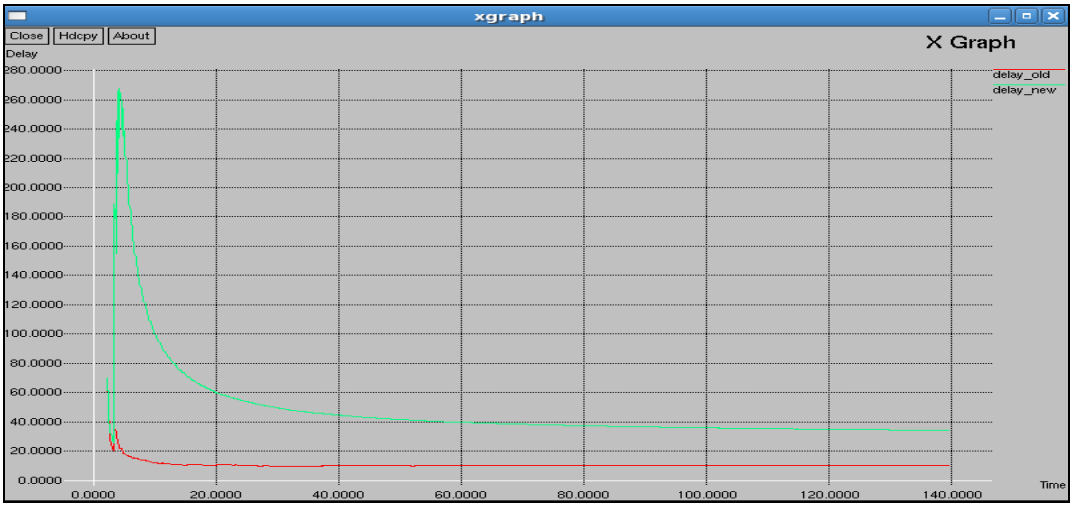

Fig 4: End to end delay Vs. Time

4.3.3. Packet Delivery Ratio (PDR)

Packet delivery ratio is resulting from the number of unique data packets arrived at the destination divided by the unique data packets sent from a source. By the graph we have concluded that due to detection of anomaly PDR was low but it has been improved by preventing the network.

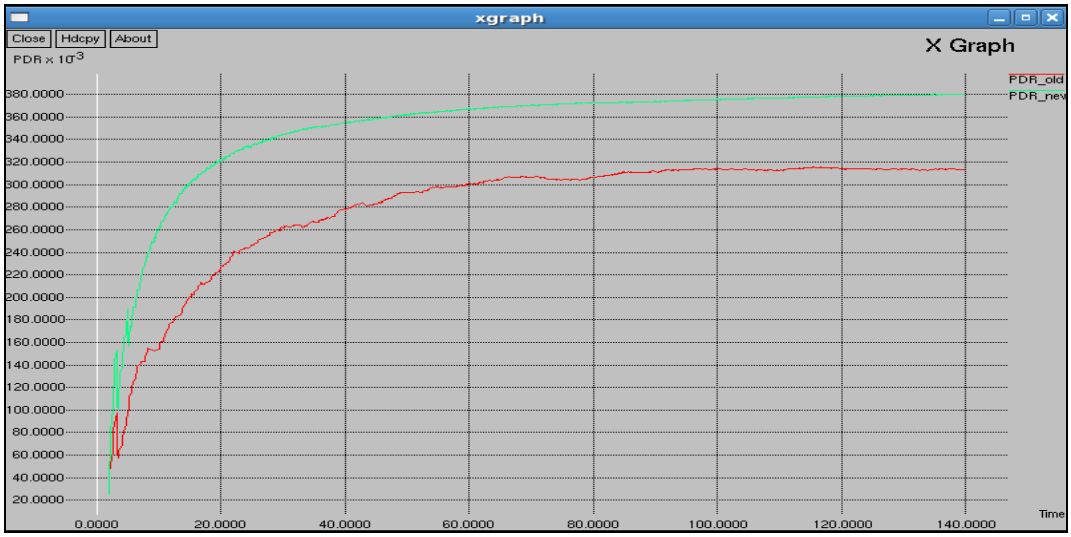

Fig 5: PDR Vs. time

4.3.4. Throughput

It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission. Along with these parameters one should also consider the energy utilization of the nodes, it is one of the important aspect when network nodes are mobile and infrastructure less. Throughput was low in the network where attack has been detected but it is increased when attack is prevented.

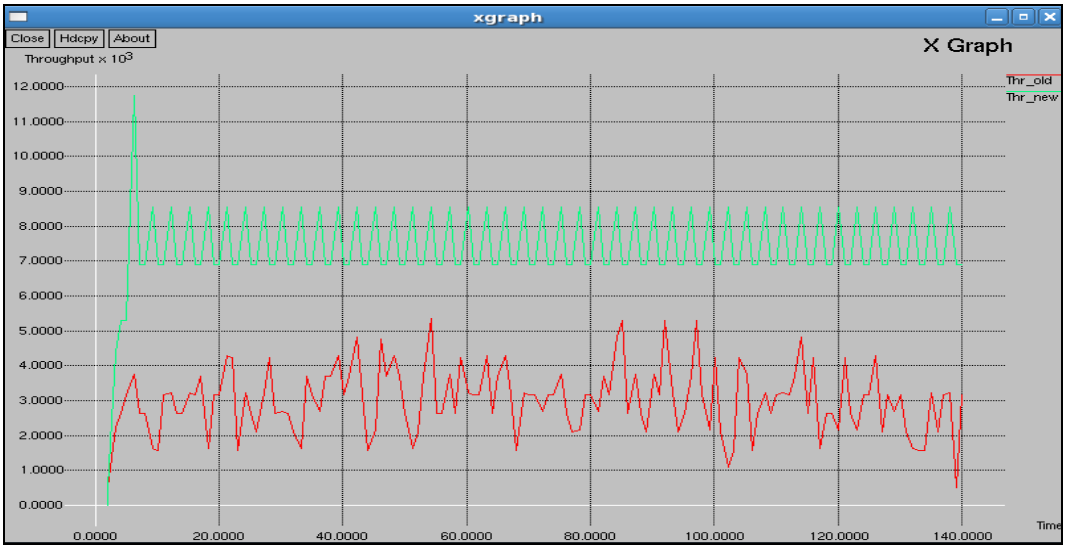

Fig 6: Throughput Vs. Time

CONCLUSION

We have detected the anomaly which is generated by the random malicious node. Due to the anomaly detection in the network PDR is degraded because of this delay is more also energy utilization is more and energy is getting reduced as time passes. Overall throughput is minimized due to anomaly in MANET. We have detected the attacks like anomaly behaviour of black hole attack, denial of service attack and flood anomaly.

As a preventive measure of the anomaly detection we have taken dual head per cluster .The two head nodes per cluster in our system not only cooperate for finding intrusion for other nodes in that respective cluster but also protect each other against intrusion. Also, power problem of nodes will also get solved as only one node will be active at a time. Hence, more permanent cluster will be formed. By using our proposed system, Anomaly based detection, problem of new attack will be resolved which was in signature based detection. So, new attack signature is formed for further use. Our preventive measure towards the anomaly detection will minimize the delay and saves the power of nodes to form the more permanent cluster.

ACKNOWLEDGEMENT

My sincere thanks to my honorable guide Prof. Saniya M. Ansari and others those who have contributed towards the completion of research work and preparation of this paper.

REFERENCES

[1] Zeba Ishaq, Secure MANET using two head cluster in Hierarchal Cooperative IDS, International journal Of Computer Applications (0975-8887), Volume 57-No.3, November 2012.

[2] Zhang Y, Lee W. Intrusion detection in wireless ad hoc networks. Proc. of 6th Ann. Int. Conf., (ACM MobiCom'00): Boston, MA, Aug 2000; 275-283.

[3] Albers P, Camp O, et,al.Security in ad hoc networks: a general ID architecture enhancing trust based approaches. Proc. of 1st Int: April 2002; 1-12.

[4] Vasudevan, Decleene B, Immerman N, et,al.Leader election algorithms for wireless ad hoc networks. In 3rd DARPA Information Survivability Conference and Exposition (DISCEX III): April 2003.

[5] Krishna P, Vaidya N H, et,al.A cluster-based approach for routing in dynamic networks.ACM SIGCOMM Computer Communication Review: 1997; 27, (2): 10-64.

[6] Krugel C, Toth T.Flexible, mobile agent based intrusion detection for dynamic networks. In European Wireless: 2002.

[7] Manmeet Kaur marhas, Anup Bhange and Piyush Ajankar, Anomaly Detection in Network Traffic: A Sattistical Approach, vol. 1, No. 3, IJIEASR, ISSN: 2319-4413, December 2012.

[8] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, Detecting blackhole Attack on AODV- based Mobile Ad Hoc Networks by Dynamic Learning Method, International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[9] Sagar D. Pandiya, Rakesh Pandit and Sachin Patel, A System for MANET to Detect Selfish Nodes Using NS2, IJESIT, and ISSN: 2319-5967, Vol 1, Issue 2, November 2012.

[10] D.Dasgupta, F.Gonzalez, K.Yallapu, J. Gomez, R.Yarramsettii, An agent-based intrusion detection system, Computers and Security (2005).

[11] Kapil Dhamecha, Rutvik Upadhyay and Bhushan Trivedi, Co-operative IDS Architectures for MANETs- A Survey. International Journal of Computer Applications (0975 – 8887), Volume 61– No.1, January 2013.

[12] Kachirski O, Guha R.K, 2003: Effective intrusion detection using multiple sensors in wireless ad hoc networks, Proceedings of HICS, 57.

[13] Kazienko P., Dorosz P: Intrusion detection systems. Part I. Intrusion types and symptoms. Tasks and architecture of IDS. Translation from Polish, IT FAQ 12/2002, pp. 21-27.

[14] M. Ramadas, S. Ostermann, and B. Tjaden, "Detecting Anomalous Network Traffic with Self-Organizing Maps," Proc. Sixth Int'l Symp. Recent Advances in Intrusion Detection, pp. 36-54, 2003.

[15] J.Brutlag, "Aberrant Behaviour Detection in Time Series for Network Monitoring," Proc. USENIX 14th System Administration Conf. (LISA), pp. 139-146, Dec. 2000.

[16] Nadeem, A & Howarth, M. (2009). Adaptive intrusion detection and prevention of denial of service attacks in MANETs. International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, Leipzig, Germa.

[17] Dr. Imad S. Alshawi, Dr. Kareem R. Alsaiedy, Vinita Yadav and Rashmi Ravat, "Defense Framework (Stream) for Stream-Based Ddos Attacks on Manet", International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 5, Issue 1, 2014, pp. 42 - 52, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.

[18] Prof. S.B. Javheri and Shwetambari Ramesh Patil, "Attacks Classification in Network", International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 4, Issue 3, 2013, pp. 1 - 11, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.

[19] Nada M. Badr and Noureldien A. Noureldien, "Review of Mobile Ad Hoc Networks Security Attacks and Countermeasures", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 6, 2013, pp. 145 - 155, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[20] Neha Kaushik and Ajay Dureja, "A Comparative Study of Black Hole Attack in Manet", International journal of Electronics and Communication Engineering & Technology (IJECET), Volume 4, Issue 2, 2013, pp. 93 - 102, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.