Multilayer Intrusion Detection in MANET

J. Godwin Ponsam
Research Scholar
SRM University, India

R. Srinivasan, PhD
Professor Emeritus
Directorate of Research
SRM University, India

ABSTRACT
Intrusion detection system plays a major role in Mobile Adhoc Network (MANET). There are lots of attacks in MANET due to its vulnerabilities. Many Intrusion Detection System (IDS) like standalone IDS, Hierarchical IDS, Distributed IDS, Cooperative IDS are available in MANET but still suffers due to multilayer attacks such as (Denial of Service) DOS attack. In this paper we have proposed a Multilayer Intrusion detection to detect intrusions in MANET. We have used fixed clustering algorithm for detecting the intrusions. We have done experiments on multiple layer ids and single layer ids and found multiple layer ids can detect intrusions better than single layer ids.

General Terms
Security, Fixed Clustering Algorithm

Keywords
IDS, DOS, MANET, Attacks

1. INTRODUCTION
There are various challenges in MANET due to its dynamic nature, lack of centralized monitoring and limited resources and battery power. In MANET attack may happen in network layer or MAC layer or in upper layers. Identifying the attack using single layer information will not be sufficient to provide security. There is a need for multifence security solution in MANET[1]. In this paper we have compare compared single layer intrusion detection with multiple layer intrusion detection. Based on our simulation experiments we have shown how Multiple layer Intrusion detection increases the detection efficiency. We base our experimental evaluation on AODV protocol. Our simulation results clearly show that there is an increase in detection efficiency and also also shows the limitation inability of single layer ids for intrusion detection. To identify the intrusion we have used fixed width clustering algorithm for detecting in both single and multiple layer IDS. This paper is organized as follows. In section 2, we will discuss related work. Section 3 we have described Multiple Layer IDS. Section 4 describes simulation setup and Performance Evaluation.

2. RELATED WORK
There are various MANET IDS architectures available like Cooperative IDS, Distributed IDS, Mobile agent based IDS. Mishra[2] has given an overview of various IDS architectures. He explains about various IDS architectures and compares among those IDS. Different types of IDS features are investigated in his paper. Although lot of study is done among IDS architectures but still no analysis done on detection. Yang[3] proposes a model based on protocol behavior using protocol description language. Here the author analyzes the protocol violations for understanding security vulnerabilities in MANET. Zhang [4] proposes proposed a model for measuring the efficiency of IDS. Here the author evaluates the application based intrusion detection architecture. IDS models are analyzed based on operational cost and effectiveness. For assessing the model detection, accuracy and false alarm parameters are used.

3. MULTIPLE LAYER INTRUSION DETECTION SYSTEM
MANET is vulnerable to multiple layer attacks due to its mobility [1]. Intrusion detection with single layer detection will not be sufficient for a secure MANET. To do a secure communication there is a need for multiple layer intrusion detection in MANET. If routing and MAC layer are combined then many routing attacks can be detected. Using this multiple layer IDS it can detect attacks launched from any layer with better detection efficiency. The information like congestion and interference will be obtained from MAC layer. Data collected from multiple layers are collected and sent to the data analysis to identify the intrusion. This multiple layer IDS architecture will work based on the collected information from MAC layer and routing layer. If single IDS are employed then the routing may select any route and can include malicious node. It is better to incorporate MAC layer for IDS to detect DOS attack as it is better detected in this layer. To avoid congestion and route data MAC and routing layers should cooperate with each other with IDS to avoid insertions of malicious nodes in new routes. MAC layer will contain information about congestion and interference. By combining multiple layers for detection provides better detection accuracy.

Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

3.1 Intrusion detection Phase
Many traditional intrusion detection techniques are limited with collection of training data from networks and labeled as normal and abnormal. We have used Apriori association algorithm which is followed by clustering algorithm for detecting intrusions. The association rule and clustering are used as the base on anamoly detection of attacks in MANET. Our proposed architecture is shown in Fig.1. The anomaly detection system creates a normal base line profile which contains normal activities of the network. The traffic which diverts from normal activity will be called as abnormal traffic or intrusion. The main advantage of anomaly based detection is it identifies new and unknown attacks. The anomaly

detection comes in two basic steps. One is training and another one is testing. We build the profile from audit data. Then we apply data mining technique to find intrusions.

3.2 Construction of Data Set

The data obtained from the audit data contains local routing information and control information from Link and routing Layers. We have used clustering algorithm to perform anomaly detection. The cluster width w is chosen will be the maximum of threshold radius of a cluster.

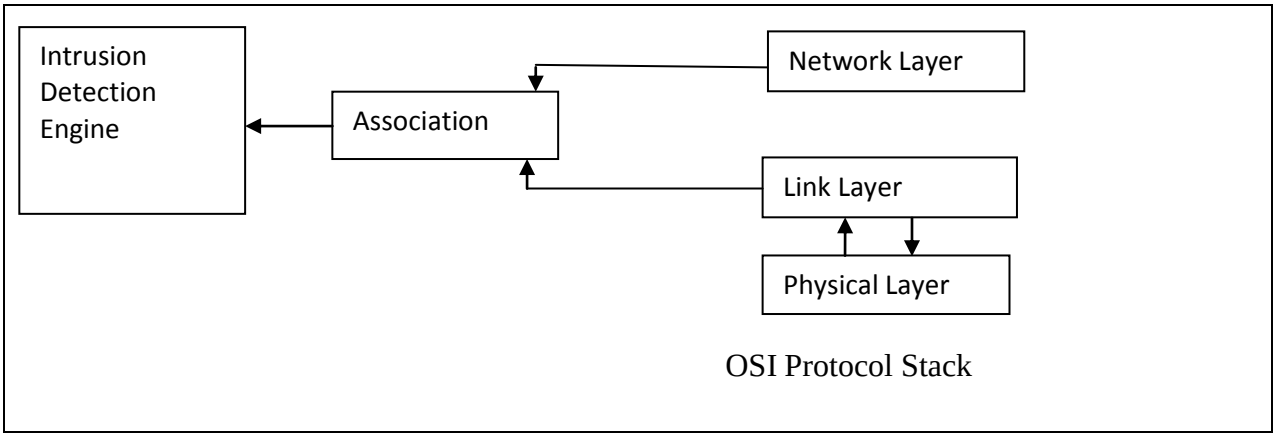

Fig 1. Mulitlayer Intrusion Detection Architecture

Training samples $S_{T=}$ { Si,i=1,2……NT}

Where each sample has dimension d

Initial set of clusters ψ ={}, the number of clusters C=0

Normalising S_T

For each training samples SiεS_T

If C=0 then

Make new cluster with ψ 1 with centroid ψ1from si

ψ 1 = { s1}, ψ 1*:=Si ψ:={ ψ 1}, C=C+1

Else

Find the nearest cluster ψ n to si

n= argmink {Distance (si, ψ1*), where k=1 …..C

if distance to nearest cluster distance (si, ψ 1) < w then

Add Si to cluster ψn and update cluster centroid ψn*

ψn ={Si} U ψn

Else

Make new Cluster ψC+1with centroid ψ C+1 from Si

ψC+1={Si},

ψC+1*=Si

ψ={ψc+1} U ψ1

E:=C+1

For Each Cluster

Find the outermost point Smax in cluster ψk

Smax:=argmin{Distance (Sψk*)} where Siεψk and i=1……NT

Set width wk of cluster ψk

Wk=Distance (Smaxψk*)

Cluster Labeling

If ψk/NT<classification threshold τ then

Label τ as anamolous

Else

ψ k as normal

Fixed width Clustering algorithm

A set of sample are extracted from the training purpose. Each sample s_i in the training set is represented by d dimensional vector of attributes. Initially the adhoc network cluster will be null. When calculating the distance between points, normalization is done before mapping into feature space to ensure all features have same outcome. New cluster ψ 1 is formed with centroid ψ 1* from sample s_i. At every point we will find the distance of sample s_i to the centroid of each cluster ψ*. If the distance to the nearest cluster ψn is within w of cluster center then point will assigned to cluster. If cluster contains less than threshold % of the total set of points then it is considered as anomalous. Otherwise clusters are normal.

4. PERFORMANCE EVALUATION

We have simulated the detection ability of both multiple layer IDS and single layer IDS based on changing mobility conditions. For this performance evaluation, AODV routing protocol is used for routing packets. In our simulation we have included 20 mobile nodes. During training phase attacker nodes are not included to obtain normal traffic. We have simulated malicious node to perform sink hole attack. Mobility makes network topology to be dynamic so detector should be up to date to detect attack with low false positive and negative rates. The data collected from multiple layers are sent to the Intrusion detection engine to compare with the normal profile. If the traffic samples at the destination node does not match with traffic generated by fixed width algorithm then intrusion is detected. In our simulation we have compared the multiple layer IDS with single layer IDS and found the detection efficiency of multiple layer IDS is good when compared to single IDS.

Parameter	Value
Coverage Area	1000m by 1000m
Normal Nodes	20
Malicious nodes	1 or 2(fixed/moved)
Transmission range	250m
Mobility	Random way point model
Traffic type	UDP- CBR
Packet size	512
Max Speed	20 m/s

Table 1. Experimental Parameters

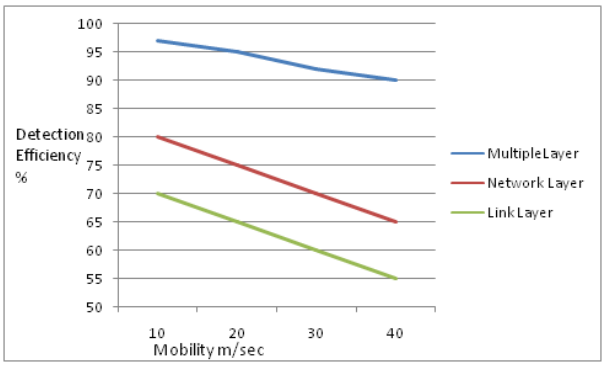

Fig. 2. True Positives

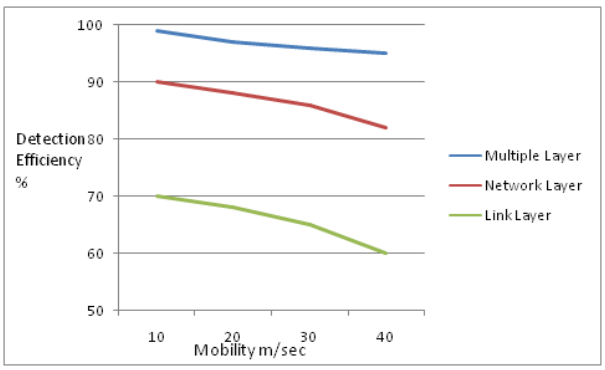

Fig.3. True Negatives

In True positive a legitimate attack which triggers an IDS to produce an alarm. In True negative an event will be triggered with no attack takes place and no detection is made.

Figure 2 and Figure 3 show the true positives and negatives of Sinkhole attacks. True positives are the detection rate of malicious events and the true negatives are the rate of benign events. The scope of this paper to show the strength of multiple layer IDS is better than single layer IDS. Single layer detection systems Link layer, Network Layer is compared with multiple layer detection systems. The multiple layer

detection system shows better detection efficiency when compared with single layer detection system. This shows the inadequacy of single layer IDS to detect routing attacks. It can be noted that detection accuracy is reduced when mobility is increased. But still the detection efficiency is not affected due to mobility. Even though the adhoc network changes due to mobility conditions still the detection efficiency is not degraded.

5. CONCLUSION

In this paper we have analyzed the detection efficiency of multiple layer IDS and Single layer IDS. For this purpose attacks over routing protocol are simulated and analyzed the performance of both detection systems. We have used fixed width clustering algorithm for detecting intrusions using both IDS. The experimental result clearly shows the detection efficiency of Multiple layer IDS is better than Single layer IDS. This multiple layer IDS can detect Sink hole attack, DOS attacks efficiently when compared to single layer IDS.

6. REFERENCES

[1] J. Godwin Ponsam, R.Srinivasan, " A Survey on MANET Security Challenges, Attacks and its Countermeasures, in IJETTCS, 2014

[2] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion Detection in Wireless Ad-Hoc Networks," in IEEE Wireless Communications, pp. 48- 60, February 2004.

[3] L. Yu, L. Yang, and M. Hong, "Short Paper: A Distributed Cross-Layer Intrusion Detection System for Ad Hoc Networks," in Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, Athens, Greece, pp. 418-420, September 2005.

[4] Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," ACM J. Wireless Networks, pp. 545- 556, 2003

[5] V. Srivastava and M. Motani, .Cross-layer design: A survey and the road ahead,. in *IEEE Communications Magazine*, pp. 112. 119, December 2005.

[6] Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah, "A Survey on MANET Intrusion Detection," International Journal of Computer Science and Security, 2007, Volume (2): Issue (1), pp. 1-11.