American-Eurasian Journal of Scientific Research 11 (1): 32-37, 2016
ISSN 1818-6785
© IDOSI Publications, 2016
DOI: 10.5829/idosi.aejsr.2016.11.1.22821

Time Orient Frequency Estimation Technique Based Intrusion Detection System for Cluster Routing in Mobile Adhoc Networks at Battle Field Conditions Using Fuzzy Rule Sets

[1]W. Gracy Theresa and [2]S. Sakthivel

[1]Depatment of Computer Science, Adhiyamaan College of Engioneering, Hosur, India
[2]Department of Information Technology, sona College of Technology, Salem, India

Abstract: Mobile adhoc network which has no restrictions in its deployment and movement of nodes makes easier for the defense industries to deploy rapid network to collect various information about battle situations. In order to collect the information they use cluster based routing where the nodes routes the data through the cluster heads to reach the controlling station which is more prone for various malicious activities performed over the packets being sent. To identify and overcome such intrusion detection performed by the malicious nodes there are many approaches has been discussed earlier, but suffers with the problem of intrusion detection accuracy and efficiency. We propose a time orient frequency estimation technique based intrusion detection with the support of fuzzy rule sets. The method maintains the set of rules among them each of the rule describes, various values for the format of the control packets has to be sent and the range values mentions the possible values of features of the packet. Similarly, the method performs time orient frequency estimation technique to perform intrusion detection system with the help of rule sets available. The method identifies the intrusion in an efficient manner and produces efficient results. The method reduces the frequency of the intrusion and improves the efficiency of intrusion detection in all the factors.

Key words: Mobile Adhoc Network · Cluster Routing · Time Orient Frequency Estimation · Fuzzy Rule Sets

INTRODUCTION

The mobile adhoc network is the collection of set of mobile nodes which has no restrictions in their mobility and could be deployed in few minutes. The advantage of the feature of the mobile adhoc network could be used in various situations like war field and battle field conditions. In such situations there is a necessary to collect the information about the battle field conditions like war troops, medicine requirement, weapon supply and many more. Such information has to be delivered to the controlling point so that decisions can be taken in time to get more control of war field conditions.

To collect the information about the war field, the application of cluster based routing can be employed where a single node collects the information from the rest of the nodes. For example, there area many camp offices present in the war field each of them is a mobile node and each delivers information about the various status of war filed to the controlling point or sink in a periodic manner. The nodes routes the packets in a cluster based routing manner to reach the sink node or the root node.

The problem here is there may be the presence of malicious node which can learn the feature of the packet being routed and can generate malicious packets to reduce the efficiency of the war field condition based decision making approach. The malicious node can perform modification attacks or can generate malicious number of packets towards the cluster head or the malicious node can generate false informatics packet towards the cluster head. Based on the information being received from the nodes of the network the cluster head will take decision about the actions to be taken in the war field conditions.

There are many approaches has been discussed in the literature but they suffer with the problem of accuracy and efficiency of performing intrusion detection. The time orient frequency estimation is the process of computing

Corresponding Author: W. Gracy Theresa, Depatment of Computer Science, Adhiyamaan College of Engioneering, Hosur, India.

the frequency of packets with different types being sent from any node at any time window. By performing such computation the reception of malicious packet can be identified and intrusion detection can be performed. The frequency of reception of the control packet is highly based on the number of nodes present under any cluster head or the number of nodes present in the layer being specified. So by using such computation the process of intrusion detection can be performed efficiently.

Fuzzy Rule Sets are one which contains N number of instances of rules; each has set of features with set of values mentioned. The Rule has different set of features and the set of values each feature of the rule present. Using the rules present in the fuzzy rule sets, we can identify the trustworthy of the packet being received.

Related Works: There are many approaches has been discussed in literature and we discuss few of them here in detail in this section.

Host Based intrusion Detection system [1] presents intrusion detection system which informs system administrator about potential intrusion incidence in a system. The designed architecture employees statistical method of data evaluation, that allows detection based on the knowledge of user activity deviation in the computer system from learned profile representing standard user behavior.

Network Intrusion Detection System [2] is proposed which embedded a NIDS in a smart-sensor-inspired device under a service-oriented architecture (SOA) approach. Using this embedded NIDS we can able to operate independently as an anomaly-based NIDS, or integrated transparently in a Distributed Intrusion Detection System (DIDS). It combines the advantages of the smart sensor approach and the subsequent offering of the NIDS functionality as a service with the SOA use to achieve their integration with other DIDS components. It also addresses the construction of a physical sensor prototype. This prototype was used to carry out the tests that has demonstrated the proposal's validity, providing detection.

An Activity Pattern Based Wireless Intrusion Detection System [3] is designed for wireless network. it exploits pattern recognition techniques to model the usage patterns of authenticated users and uses it to detect intrusions in wireless networks. User activity is monitored and their discriminative features are extracted to identify intrusions in wireless networks. The detection module uses PCA technique to accumulate interested statistical variables and compares them with the thresholds derived from user's activities data. When the variables exceed the estimated thresholds, an alarm is raised to alert about a possible intrusion in the network. The novelty of the proposed system lies in its light-weight design which requires less processing and memory resources and it can be used in real-time environment.

EAACK [4], propose and implement a new intrusion-detection system named Enhanced Adaptive Acknowledgment (EAACK) specially designed for MANETs. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK) and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in EAACK.

ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack [9], present a comprehensive study to show the danger of Botnet-based DDoS attacks on application layer, especially on the Web server and the increased incidents of such attacks that has evidently increased recently. Botnet-based DDoS attacks incidents and revenue losses of famous companies and government websites are also described. This provides better understanding of the problem, current solution space and future research scope to defend against such attacks efficiently.

DDoS Attacks Detection by Means of Greedy Algorithms [10], focus on DDoS attacks detection by means of greedy algorithms. In particular we propose to use Matching Pursuit and Orthogonal Matching Pursuit algorithms. The major contribution of the paper is the proposition of 1D KSVD algorithm as well as its tree based structure representation (clusters), that can be successfully applied to DDos attacks and network anomaly detection.

Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art [11], present a comprehensive study to show the danger of Botnet-based DDoS attacks on application layer, especially on the Web server and the increased incidents of such attacks that has evidently increased recently. Botnet-based DDoS attacks incidents and revenue losses of famous companies and government websites are also described. This provides better understanding of the problem, current solution space and future research scope to defend against such attacks efficiently.

Analyzing Feasibility for Deploying Very Fast Decision Tree for DDoS Attack Detection in Cloud-Assisted WBAN [12], propose classifying data mining techniques which uses, Very Fast Decision Tree (VFDT) and considered as the most promising solution for real-time data mining of high speed and non- stationary data streams gathered from WBAN sensors and therefore is selected, studied and explored for efficiently analyzing and detecting DDoS attack in cloud-assisted WBAN environment.

A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment [15], proposes a method of integration between HTTP GET flooding among Distributed Denial-of-Service attacks and MapReduce processing for fast attack detection in a cloud computing environment. In addition, experiments on the processing time were conducted to compare the performance with a pattern detection of the attack features using Snort detection based on HTTP packet patterns and log data from a Web server. The experimental results show that the proposed method is better than Snort detection because the processing time of the former is shorter with increasing congestion.

All the above discussed approaches have the problem of identifying the intrusion detection in efficient manner and struggles with the accuracy of intrusion detection.

Proposed Method: The proposed method has various stages of identifying the intrusion namely; Time orient Frequency Estimation, Rule Set Generation and Intrusion Detection. We explain each of the functional components in detail in this section.

Time Orient Data Frequency Estimation: The time orient data frequency estimation is performed based on the packets being received from unique source and the network trace being maintained by the intrusion detection system or the cluster head. For each time slot of the time window, the method computes the data frequency of concern source node. From the log being available, we first identify the number of packets being received at each time window and based on the computed number of packets at each time window; we compute the data frequency using the pay load data of each packet being received.

Algorithm:
Input: Network Trace Nt, Source Address SA.
Output: Data Frequency Factor DFF.

```
Step 1: start
Step 2: Identify the time window Ti
```

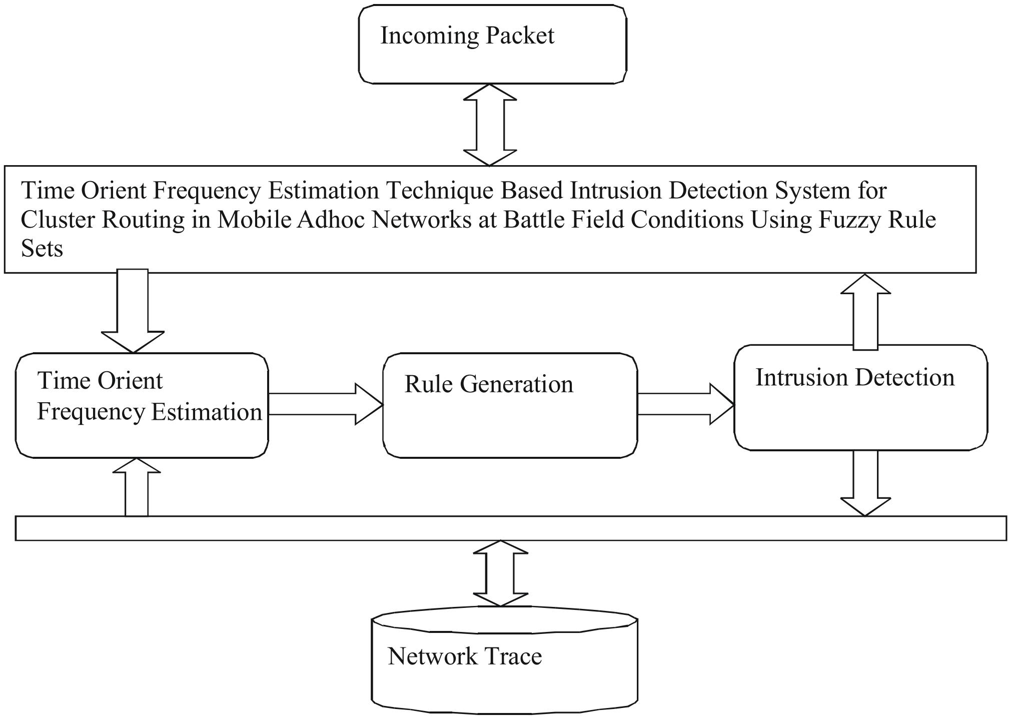

Incoming Packet
Time Orient Frequency Estimation Technique Based Intrusion Detection System for Cluster Routing in Mobile Adhoc Networks at Battle Field Conditions Using Fuzzy Rule Sets
Time Orient Frequency Estimation
Rule Generation
Intrusion Detection
Network Trace

Fig. 1: Proposed System Architecture

Ti = $\int Ti \in tw$

Step 3: Identify the set of all packets being received at the time window Ti.

Packet Set Ps = $\int \Sigma\, Pi\ (Nt) \in Ti$

Step 4: Compute Time orient data frequency factor

DFF = $\int \frac{\Sigma Payload(Ps)}{size\ of} \times size(Ps)$

Step 5: Stop.

Rule Generation: Rule generation is the process of generating the blue print which represents the set of all possible and approved patterns of features of packets can be received by the cluster head where the intrusion detection is performed. For each service being available in the network the method maintains a set of protocol and which represents the form how the services can be accessed. With the protocol and the trace being available, the method generates number of rules for each of the source. For each source, it identifies different features like the frequency of packets being transmitted, the pay load it can have, the service packet frequency it can has and so on. Using the generated rules, the other process will perform the intrusion detection.

Algorithm:
Input: Network Trace Nt, Protocol set Prs.
Output: Rule Set Rs.

```
Step 1: Start
Step 2: for each service Si available in the network
            For each time window Ti
                    For each Source Si
Compute the time orient data frequency estimation DFF.

Compute average pay load Ap = $\int \frac{\Sigma Pi(Nt)}{Number\ of\ packets\ at\ time\ window\ Ti}$

Generate rule set Rs = {DFF, Ap, Ti}.

Add to rule set Rs = $\Sigma\ (Ri \in Rs) + Rs$

                    End
            End
        End
Step 3: stop.
```

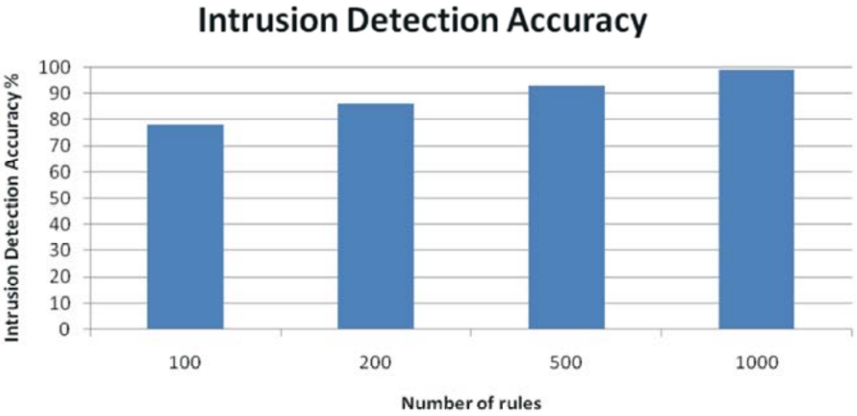
Intrusion Detection: The proposed method performs intrusion detection using the support of time orient data frequency estimation and the rule sets generated. Whenever the cluster head receives the packet from the nodes of the cluster, the intrusion detection is performed. First the packet feature are extracted like the source address, payload, service type, time window are identified. With the extracted features, the method identifies the presence of maligns from the malicious history present in the cluster head. Once there is no match has been found in the malicious history, then it generates the rule set and performs matching process with each of the rule available in the rule set. For each rule we compute the trustworthy measure with each of the rule and if the measure has more value than the threshold then the packet will be allowed otherwise it will be considered as malicious and added to the malicious history.

Algorithm:
Input: Malicious History Mh, Packet P.
Output: Null

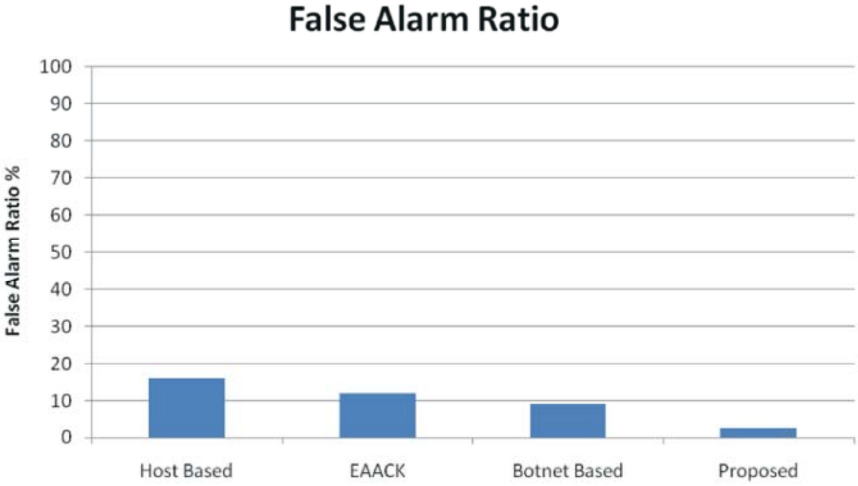
```
Step 1: Start
Step 2: Extract the features of the packet P.
        FV = { Source, payload, service type, Time}
Step3: for each record ri from Mh
        Check for the presence of feature.
        If True
                Generate the history.
        Else
Perform time orient data frequency estimation DFF.
    Generate rule set Rs.
    For each rule Ri from Rs

Compute trustworthy Tw = $\frac{\Sigma Features(Fv) \in Ri}{size(Ri)}$

If Tw> TTh //Trustworthy threshold
                        Allow packet.
                        Else
                                Drop packet.
                        End
                End
        End.
    End.
Step 4: Stop.
```

RESULTS AND DISCUSSION

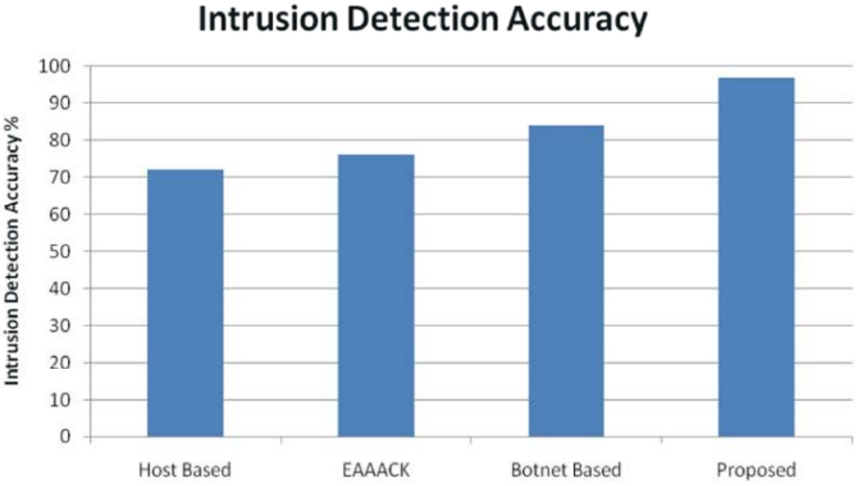
The proposed time orient frequency estimation based intrusion detection system using rule sets has been



Graph 1: Comparison of intrusion detection accuracy



Graph 2: Comparison of false alarm ratio



Graph 3: Comparison of intrusion detection accuracy

implemented and tested for its efficiency. The method has produced efficient results and has reduces the time complexity and false alarm ratio as well. The methods has improved the performance of the accuracy of intrusion detection higher and achieve great accuracy.

The Graph 1, shows the accuracy of intrusion detection according to the number of rules being used. The method has produced higher rate of accuracy with the growing number of rules.

The Graph 2 shows the comparison of false alarm ratio produced by different methods and it shows clearly that the proposed method has produced less false alarm ratio than others.

The graph 3 shows the efficiency of intrusion detection accuracy of different methods and it shows clearly that the proposed method has produced higher accuracy than other methods.

CONCLUSION

We propose a time orient frequency estimation technique based intrusion detection using rule sets in mobile adhoc network. The proposed method computes the time orient data frequency of each source from where the packet being received. Whenever the packet has been received, it computes the time orient data frequency and generates number of rules or rule sets. Based on the rule set generated and packet being extracted, we compute the trustworthy of the packet. Based on the trustworthy of the packet the intrusion detection is performed. The proposed method produces higher accuracy than other methods and reduces the time complexity as well. The proposed method has produced less false alarm ratio than other methods.

REFERENCES

1. Vokorokos, L., 2010. Host Based Intrusion Detection System, Intelligent Engineering Systems (INES), pp: 43-47.
2. Macia´-Pe´rez, F., 2012. Network Intrusion Detection System Embedded on a Smart Sensor, Industrial Electronics, IEEE Transactions on, 58(3): 722-732.
3. Haldar, N.A.H., 2012. An Activity Pattern Based Wireless Intrusion Detection System Information Technology, pp: 846-847.
4. Elhadi, M. Shakshuki, 2013. EAACK-A Secure Intrusion-Detection System for MANETs, IEEE Transactions on Industrial Electronics, 60(3): 1089.
5. Akbani, R., T. Korkmaz and G.V.S. Raju, 2012. “Mobile Ad hoc Network Security,” in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, pp: 659-666.
6. Akbani, R.H., S. Patel and D.C. Jinwala, 2012. “DoS attacks in mobile ad hoc networks: A survey,” in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, pp: 535-541.
7. Kang, N., E. Shakshuki and T. Sheltami, 2011. “Detecting forged acknowledgements in MANETs,” in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp: 488-494.
8. Gupta, B.B., R.C. Joshi and Manoj Misra, 2012. "ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack," International Journal of Network Security (IJNS), 14(1): 36-45.
9. Gupta, B.B., R.C. Joshi, ManojMisra, 2012. "ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack," International Journal of Network Security (IJNS), 14(1): 36-45.
10. Tomasz Andrysiak, Łukasz Saganowski and MichałChoraœ, 2013. D. DoS Attacks Detection by Means of Greedy Algorithms, Image Processing and Communications Challenges 4, Advances in Intelligent Systems and Computing, 184: 303-310.
11. EsraaAlomari, SelvakumarManickam, B.B. Gupta, Shankar Karuppayah and Rafeef Alfaris, 2012. Article: Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. International Journal of Computer Applications, 49(7): 24-32.
12. Rabia Latif, Haider Abbas, Saïd Assar and Seemab Latif, 2014. Analyzing Feasibility for Deploying Very Fast Decision Tree for DDoS Attack Detection in Cloud-Assisted WBAN, Springer, Intelligent Computing theory, 8588: 507-519.
13. Katkamwar, N.S., A.G. Puranik and P. Deshpande, 2012. Securing Cloud Servers against Flooding Based DDoS Attacks. International Journal of Application or Innovation in Engineering and Management (IJAIEM) 1(3) (November 2012).
14. Lonea, A.M., D.E. Popescu and H. Tianfield, 2013. Detecting DDoS Attacks in Cloud Computing Environment. Int. J. Comput. Commun., 8(1): 70-78.
15. Junho Choi, Chang Choi, ByeongkyuKo and Pankoo Kim, 2014. A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment, Springer, Soft computing, 18(9): 1697-1703.