Middle-East Journal of Scientific Research 24 (1): 97-102, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.01.22824

Time Orient Flow Estimation Based Data Mining Approach for Intrusion Detection in Wireless Local Area Networks Using Delay Averaging Scheme

[1]P. Kavitha and [2]M. Usha

[1]Department of Information Technology,
Adhiyamaan College of Engineering, Hosur, Tamilnadu, India
[2]Department of Computer Science and Engineering,
Sona College of Technology, Salem, Tamilnadu, India

Abstract: The intrusion detection is the process of maintaining secure access of the services available and to provide more secured services in the wireless local area network. The generic nature of WLAN has no management of identity of users and the services provided have to be secured in order to achieve more throughput. There are many approaches have been discussed earlier to identify the intrusion performed by malicious users, but suffer with the problem of accuracy and modern attacks. The well defined data mining approaches can be used to perform intrusion detection in WLAN to achieve more accuracy in intrusion detection. With the motivation, we propose a novel approach which identifies intrusion detection in multiple ways using time window based flow estimation and average delay approach. The time orient flow estimation technique uses various features like hop names, hop counts, ttl value and so on. The method maintains various logs about the packets or services being accessed and based on that for each source being identified, the time window based flow is estimated and the delay averaging scheme computes the delay being introduced. Using both the estimated values the legitimate weight of the packet is being computed to classify the packet as genuine or malicious. The proposed method performs intrusion detection in more accurate manner and produces less time complexity.

Key words: Intrusion Detection · Wireless Local Area Networks · Delay Averaging Scheme · Time Orient Flow Estimation

INTRODUCTION

Unlike other wireless networks the Wireless local area network has some restrictions in its geographic region where it can be spread up to certain kilometers. The Wireless local area network can be a collection of set of other networks of wired or wireless. The nodes of the network are grouped to perform communication through wireless protocol and can be applicable for variety of application s in real world conditions. The WLAN are generally used in organizational sectors and universities where the units of them are connected through wireless channel and can communicate with wireless protocol.

The data mining is the process of extracting information from large knowledge base, same can be utilized to extract the malicious information present in the packets being received using different techniques. By storing the traces of packets being received, the features of learned packets can be extracted to match with the current packet in making decision about them.

The growth of internet technology has induced people to form various WLAN’s and they provide various services at some end points of a computer present in any WLAN. Each service is provided by any service provider but it could be accessed through a concern port number. Each service has protocol which specifies the rule to access the service and what input has to be given to them and so on.

The services provided in set of nodes can be accessed by different users or nodes of various networks. Each service has its own service capability in number of requests it can handle and number of bytes it can read

Corresponding Author: P. Kavitha, Department of Information Technology,
Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

and so on. There are many malicious nodes which generate much number of packets which is more than the capacity of the servicing node and there are few nodes which send the packets which is not relevant to the signature of the service.

The malicious signature packets reduce the capacity of the servicing node because the servicing node spends more time in verifying the signature which ends up in false result. This ultimately reduces the service throughput and the performance of the service and the network gets lower. We can conclude that not only the signature of the packet is malicious but also the legitimate of the packet can be verified using various other features like hop count, hop names and other features.

Any service cannot be accessed in a steady frequency at all the times and it will be vary at different time window because the users of the network may access the service with different frequency and the routes the packet being followed will also vary according to different traffic conditions. These factors can be used to identify the intrusion occurred in the network and the intrusion detection can be performed using these features of the packet also.

Delay averaging scheme is the method which computes the average delay may be present in any path of the network at different time window. The traffic will be varying in different manner at different time window which can be used to identify the intrusion also. Similarly the time orient flow of packets can also be used to perform intrusion detection. We propose such a method which combines different features and metrics to perform intrusion detection in this paper.

Related Works: There are many approaches has been discussed to perform intrusion detection in wireless local area networks and we discuss few of them here in this chapter.

In Network intrusion detection by artificial immune system, an artificial immune system (IMS) based network intrusion detection scheme is proposed. An optimized feature selection and parameter quantization algorithms are defined. The complexity issue is addressed in the design of the algorithms. The scheme is tested on the widely used KDD CUP 99 dataset. The result shows that the proposed scheme outperforms other schemes in detection accuracy. In our experiments, a number of feature sets have been tried and compared.

Host Based intrusion Detection system [1] presented an intrusion detection system which informs system administrator about potential intrusion incidence in a system. The designed architecture employs 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 NID [2], is designed as a data mining framework to automatically detect attacks against computer networks and systems. An unsupervised anomaly detection technique assigns a score to each network connection that reflects how anomalous the connection is proposed with association pattern analysis module to summarize those network connections that are ranked highly anomalous by the anomaly detection module.

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 can 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 have demonstrated the proposal's validity, providing detection.

An Activity Pattern Based Wireless Intrusion Detection System [3] was 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 users' 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] proposed and implemented a new intrusion-detection system named Enhanced Adaptive Acknowledgments (EAACK) specially designed for MANETs. EAACK consists 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 included a 2-b packet header in EAACK.

Security and cooperation in wireless network is discussed in [5] by considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network.

An Artificial Immune System Based on Holland's Classifier as Network Intrusion Detection [6-12], proposed as a new method for network intrusion detection which is not aimed to provide a comparative study but to give more understanding on the feasibility of combining Artificial Immune System and Holland’s Classifier to detect network intrusion. This new Artificial Immune System, named AIS-CS, can attain higher than 90% intrusion detection with a false negative percentage below 10% and a fairly low false positive rate on a network composed of 50 regular nodes and 50 intruders.

All the above discussed approaches have the problem of performing intrusion detection in accurate manner and they have more false positive results with higher time complexity.

Proposed Method: The proposed method has various stages of identifying intrusion detection namely preprocessing, Time orient flow estimation, delay averaging scheme and intrusion detection. We explain each of the functional components in detail in this section.

Preprocessing: At the preprocessing stage the packet received and its feature is being retrieved. We extract the following features namely set of host names the packet being traversed, the number of hops, the ttl values, the size of pay load data and source in and source port and so on. The extracted features are converted into feature vector which will be used to perform intrusion detection in the next stages of computing.

```
Input: Incoming Packet P
Output: feature vector Fv.
Step1: start
Step2: read input packet P.
Step3: Extract Source Address of the packet P
        Sip = $Sourcelp \in P$
Step4: Extract Source Port of the packet P
        Sport = $Sourcelp - Port \in P$
Step5: extract TTL from P
        TTL =TTL $\in$ P.
Step6: Extract set of all host names traversed
        HIP = $\sum_{i=1}^{size(hostnames)} hnames \in P$
Step7: Compute Hop Count
        Hc = size (HIP).
Step8: Extract Payload Size
        PS = size(payload $\in P$)
Step9: construct feature vector FV.
        Pv = {Sip, Sport, TTL,HIP, HC,Ps}.
Step10: stop.
```

Time Orient Flow Estimation: The time orient flow estimation is performed by splitting the packet traces available in the packet history into number of time windows. The proposed method splits the trace into many number of small chunks according to small time windows at which they received. For each time window we identify set of all packets being received. From the packets being received we extract the set of all features and based on that we identify the set of unique routes of packet traversal. For each packet traversal path we compute the traffic flow factor which represents the amount of traffic in the specific route.

Algorithm:

```
Input: Packet History PH, Packet Feature FV..
Output: Traffic Flow Factor Set TFFS.
Step1: start
Step2: for each time window Tw
        Extract the set of traces from the source ip and source port.
        Access trace At = $\int_{i=1}^{size(Tw)} \sum_{j=1}^{size(Ah)} Ah(i).sip \equiv Fv(Sip)$
        Identify set of all unique routes the packet traversed.
        URoutes = $\int_{i=1}^{size(At)} \sum Routes(At) \exists URoutes$
        for each route Ri from URoutes
            Compute average hop count AHC = $\int_{i=1}^{size(At)} \frac{\sum Hc(At(i))}{size(At)}$
```

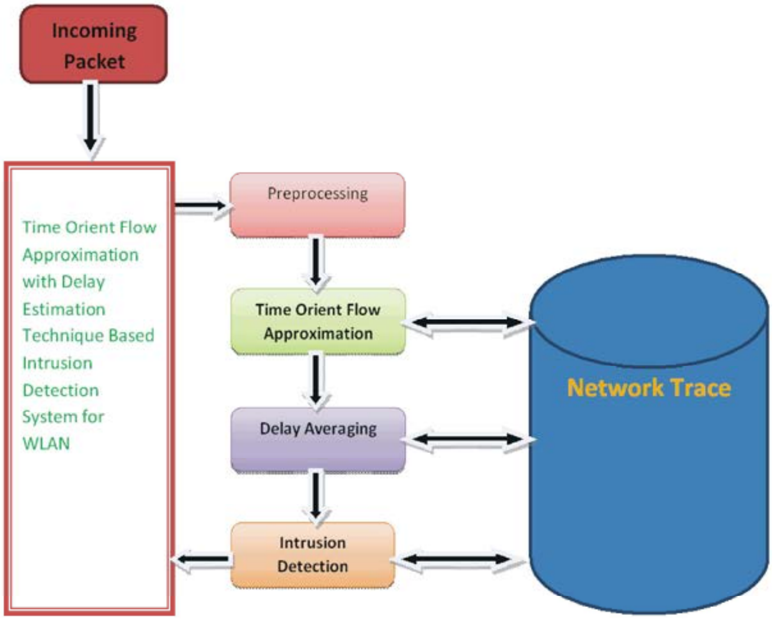

Incoming Packet
Time Orient Flow Approximation with Delay Estimation Technique Based Intrusion Detection System for WLAN
Preprocessing
Time Orient Flow Approximation
Delay Averaging
Intrusion Detection
Network Trace

Fig. 1: Proposed System Architecture.

```
            Compute Average Pay load APL = $\int_{i=1}^{size(At)} \frac{\sum PL(At(i))}{size(At)}$
            Compute Delay Averaging DAvg.
            Compute traffic flow factor TFF = $\frac{APL \times AHC.}{DAvg}$
            TFFS= ΣTFF + TFF
        end
    end
Step3: stop.
```

Delay Averaging Scheme: The delay averaging scheme is performed based on path the packet is being traversed. For each distinct path, we compute the average delay factor based on the number of packets being received at the specific route at specific time window and their payload details. The computed delay averaging value will be used to compute the traffic flow factor and to perform intrusion detection.

```
Algorithm:
Input: Path P, Packet History Ph.
Output: delay average Davg.
Step1: stop. start
step2: Extract set of all packets being received at the time window on the route.
        Ps = $\int \sum Packets \in Ph$
Step3: compute average delay DAvg.
        DAvg = $\sum_{i=1}^{PS} Delay(Ps(i))$
        DAvg = DAvg/size (Ps).
Step4: stop.
```

Intrusion Detection: Intrusion detection is performed whenever there is a packet is being received. For each packet being received we compute the legitimate weight using the time orient flow estimation technique and delay averaging scheme. Based on the traffic flow factor being computed for the specific time window if the packet has more than the value then it will be dropped otherwise the packet will be considered as legitimate.

```
Algorithm:
Input: Packet P.
Output: Boolean.
Step1: start
Step2: compute time orient flow factor TFF.
Step3: compute legitimate weight = $\frac{P.TTL \times P.Payload}{TFF}$
Step4: if Lw> Th then
            allow packet
      else
            add to packet trace and drop.
      end.
Step5: stop.
```

RESULTS AND DISCUSSION

The proposed time orient flow factor estimation with average delaying scheme based intrusion detection approach has been implemented and tested for its efficiency. The proposed method has produced efficient results in all the factors of quality of service of wireless local area networks.

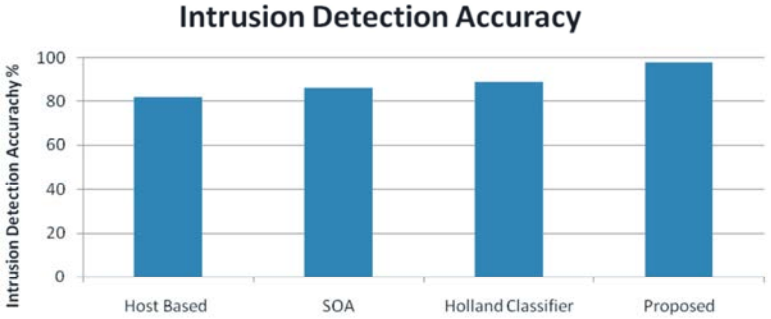
The Table 1, shows the results of different parameters of quality of intrusion detection produced by the proposed method.

The Graph1, shows comparison of intrusion detection accuracy produced by various methods and it shows clearly that the proposed method produces efficient accuracy.

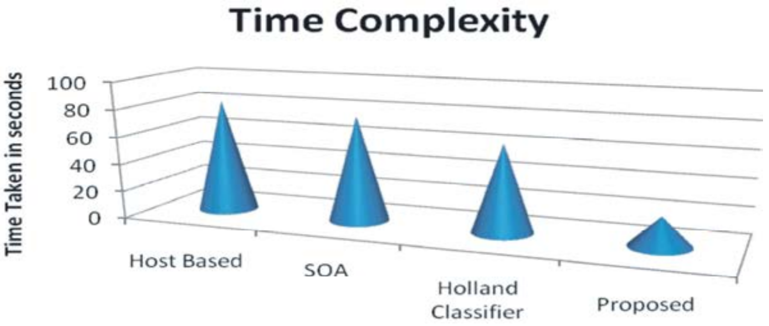
Table 1: Results produced with various numbers of rules

Number of			
Time window	Accuracy in %	Detection Rate %	False Alarm Rate. %
10	85.6	87.3	3.01
50	88.7	92.4	1.98
100	96.9	97.8	1.07

The graph 2 shows the comparison of time complexity generated by the different method in performing intrusion detection in hourly based time window of one month trace and the proposed method has produced less time complexity at different number of logs available. It shows that the proposed method has produces less time for much number of logs.



Graph 1: Comparison of different methods



Graph 2: comparison of Time complexity of different method.

CONCLUSION

We proposed a time orient flow approximation with delay averaging scheme for intrusion detection in wireless local area networks. The method splits the network trace into number of time window and based on the time window the packet being received we compute the traffic flow factor for the specific path the packet has travelled. The traffic flow factor has been used to compute the legitimate weight of the packet based on which the packet is allowed or dropped. The proposed approach has reduced the frequency of threats compared to other approaches and produces less time and space complexity values.

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 and 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, 1089. EAACK—A Secure Intrusion-Detection System for MANETs, IEEE Transactions on Industrial Electronics, 60(3).
5. Akbani, R., T. Korkmaz and G.V.S. Raju, 2012. Mobile Ad hoc Network Security, in Lecture Notes in Electrical Engineering, New York: Springer-Verlag, 127: 659-666.
6. Anantvalee, T. and J. Wu, 2008. A Survey on Intrusion Detection in Mobile Ad Hoc Networks, in Wireless/Mobile Security. New York: Springer-Verlag.
7. Gungor, V.C. and G.P. Hancke, 2009. Industrial wireless sensor networks: Challenges, design principles and technical approach, IEEE Trans. Ind. Electron., 56(10): 4258-4265.
8. Khattab, S., S. Gobriel, R. Melhem and D. Mosse, 2008. Live Baiting for Service-Level DoS Attackers, Proc. IEEE INFOCOM.
9. Thai, M.T., Y. Xuan, I. Shin and T. Znati, 2008. On Detection of malicious Users Using Group Testing Techniques, Proc. Int'l Conf. Distributed Computing Systems (ICDCS).
10. Sridevi, R., 2012. Genetic algorithm and artificial immune systems: A combinational approach for network intrusion detection, Advances in Engineering sciences and Management, pp: 494-498.
11. Junyuan Shen, 2011. Network intrusion detection by artificial immune system, IECON, pp: 4716-4720.
12. Randiranosolo, 2012. An Artificial Immune System Based on Holland's Classifier as Network Intrusion Detection, Machine learning and Approaches, 1: 504-507.