Applying Intrusion Detection Technique for Intercepting Rogue Access Point in Wireless Communication

Menal Dahiya

Assistant Professor, Department of Computer Science, Maharaja Surajmal Institute, Janakpuri, Delhi, India
menaldahiya@gmail.com

ABSTRACT

Due to the advancement in availability and flexibility of wireless communication the usage of wireless technology increases in recent years. Though wireless technology has many benefits, but on the other side, the risk of wireless security attacks also increases in many forms. The aim of the work is to design an efficient system that detects and prevents the organization from the rogue access points. Rogue access point prevention and detection are one of the major challenges for administration now days. This paper addresses a solution to prevent rogue access point in wireless networking using intrusion detection techniques. This proposed mechanism provides a cost effective solution to the network and requires no special hardware or other major equipment.

Keywords — Intrusion Detection Technique, Rogue Access Point, Wireless Security

1. INTRODUCTION

Wireless LAN is the most suitable topology for business and for the home environment. Employees easily access laptop, PDA, pocket PC and other services with LAN and they enjoy the flexible internet services. The standards for WLAN have three kinds of specifications IEEE 802.11a, 802.11b (Wi-Fi), 802.11g [1]. These wireless specifications are unsecure networks due to many reasons such as lack of physical infrastructure, emerging of new technologies, issues with designing protocols etc.. But from all these, Wi-Fi is very much unsecure as all these reasons made their security a most sensitive problem which definitely needs a solution [2]. Security is mandatory for any network, but it is more necessary in wireless networking, as it is available to all and attackers easily breach the network, which is not good for any network service and for the user also as they disturb the service on a regular basis.

The usage of smart phones and mobiles, increase the growth of Wi-Fi service through mobile devices. In present scenario many public places like airports, bus stations, malls, etc. provide free Wi-Fi facility to the users [3]. All these devices connect to wireless network through a device called as wireless access point (WAP). These WAP causes a risk of wireless security attacks. There are many attacks such as Denial of Service, rogue access point, key management, Data link layer, Application layer etc. [4]. Rogue access point is one of the major security threats now a day in wireless networking. A rogue access point is an unauthorized wireless access point that has been installed on a network or has been created to conduct man-in-the- middle-attack [5]. The intruders create a rogue access point to the users and perform attacks. So, if the rogue access point is undetected, then it leads to major loss to the users as attackers get sensitive information easily and use free internet service also. There are a number of solutions present for detecting and eliminating rogue access points.

In this paper, we propose an algorithm that prevents an enterprise networking from the rogue access points. This paper is divided into introduction, then followed by II section about rogue access point and intrusion detection techniques. In III

section, we explain the proposed algorithm and then end with the conclusion.

2. ROGUE ACCESS POINT

The performance of wireless technology is degraded by the attacks which are done on wireless networks and on wireless network resources as they destroy an organization's privacy. There are many wireless networking attacks, but the most common and challenging issue of wireless security is rogue access points [6]. A rogue access point is an unauthorized point that can be easily deployed by end users. The most common attack in wireless networks is man-in-the-middle-attack. An attacker places himself in the network and starts sending messages to the users and this is very easy as the access points are inexpensive and easy to purchase. These access points present inside the enterprise as well as outside the enterprise. By configuring the access point to default setting it becomes unnoticed. If any new access point is placed in the network it will detect and notify it to network administrators [7]. Network administrator decides whether it is a rogue access point or an authorized access point. He denies the service for that access point which detect as unauthorized and it will allow the user to connect it to the enterprise network if it is an authenticated user and it also verifies the authentication of access point by matching the security policies of the enterprise network and the newly set up access point. These are the novel solutions for preventing the rogue access point in an organization. There are many solutions proposed by researchers and academicians for preventing the rogue access point, but no solution can fully protect the organization by these rogue access points [8], [9]. Here, we propose a technique which surely helps the wireless LAN from rogue access points.

2.1 Intrusion Detection Techniques

It is very difficult for a system to differentiate between authorized and unauthorized users in a wireless network. The traditionally MAC address list is used by the network administration for detecting authorized users. The MAC address is an address that is assigned to a device that helps it identify uniquely. But attackers apply MAC spoofing technique to break down this task. MAC address spoofing is an attack or we can say that an illegal task which is done by hackers where they access the MAC address of the authorized user and enter into the network as an authorized user. To overcome these problems we use intrusion detection systems. Network intrusion detection systems (NIDS) are the most efficient way of defending against network-based attacks aimed at computer systems [10], [11]. Basically, there are two types of techniques: Signature based system and Anomaly based system. Signature based system [12], [13] based on pattern recognition technique and Anomaly based system [14] builds a statistical model which describes normal network traffic and any abnormal behavior that deviates from the model is identified.

2.1.1 Signature Based Detection

The signature detection method involves predefined attack patterns called signatures. The main benefit of this technique is that once we know the network behavior we are easy to develop and understand the signatures. And the only limitation of this mechanism is that they only detect the attacks whose signatures are already stored in the database; a signature must be created for every attack. This technique does not work properly when user uses advanced techniques and it can be easily deceived as they are based on simple string matching mechanism.

2.1.2 Anomaly Based Detection

The anomaly based detection is based on the predefined network behavior. The network behavior is learned by the specifications of the network administrators. The intrusion detection engine of this technique, process the protocols and saves the detailed knowledge about the accepted network behavior which is developed by the administrator, i.e. normal behavior as a baseline characteristics. Therefore, rules and protocol must be built properly, than an anomaly detection system works well. If the current behavior of the user falls under the accepted behavior, then it goes unnoticed and if the current behavior of the user deviates from the baseline, then it will detect it as an unauthorized user. Anomaly detection technique works on the set of predefined rules, classes and attributes carried out from the training data set of rules and procedures. Anomaly based detection contains various techniques as shown in figure 1

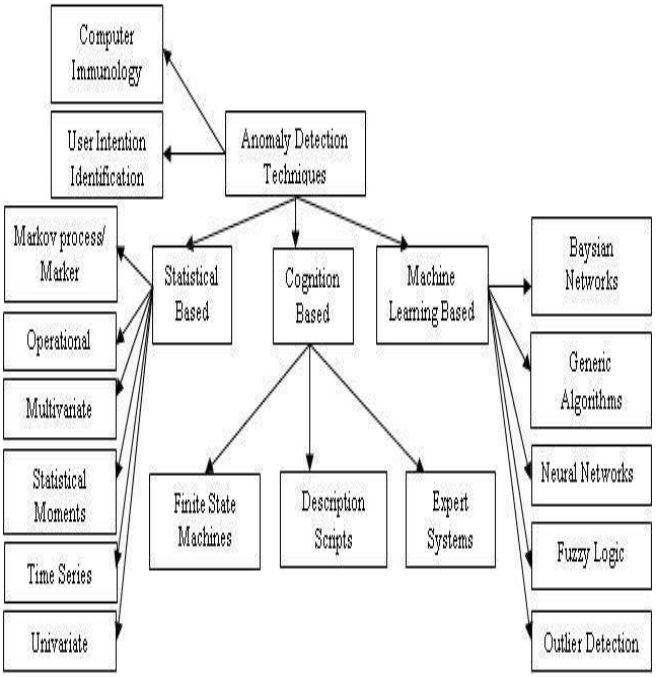

Fig-1: Various Anomaly Detection Techniques

3. PROPOSED TECHNIQUE

We propose a solution in which rogue access points detection starts by collecting wireless data that includes Beacon, probe messages and client data frames. This collected data will be normalized to remove irrelevant information out. On side by side the normalized data are compared with previously maintained company's database, if it is present there, then it is authenticated or verified, but if it is not present there then it goes through anomaly detection technique mechanism.

Here, in this work we apply Neural Network procedure, a layered feed forward topology in which each unit performs a biased weighted sum of their inputs and pass this activation level through a transfer function to produce their output [15]. After applying neural network, an output is obtained which is being evaluated and compared with the predefined threshold value. A threshold value is defined to know whether the user is authorized a minimum percentage of synchronous. If this compared value is less than one than it is a rogue access point and if it is greater than one, then it is not a malicious point and store it in the company's database. Figure 2 explains the algorithm and figure 3 shows the flowchart of the algorithm.

Step 1: Input Wireless Packets
Step 2: Normalize the data packets
Step 3: If normalize data packets equals to stored data, then it is a valid access point and go to step 6.
Step 4: Evaluate the data using Anomaly Detection Technique and Compute, x as output.
Step 5: If x is greater than the predefined threshold value, then it is not a rogue access point and stores it in a database else it is a rogue access point
Step 6: Stop.

Fig-2: Rogue access point detection algorithm

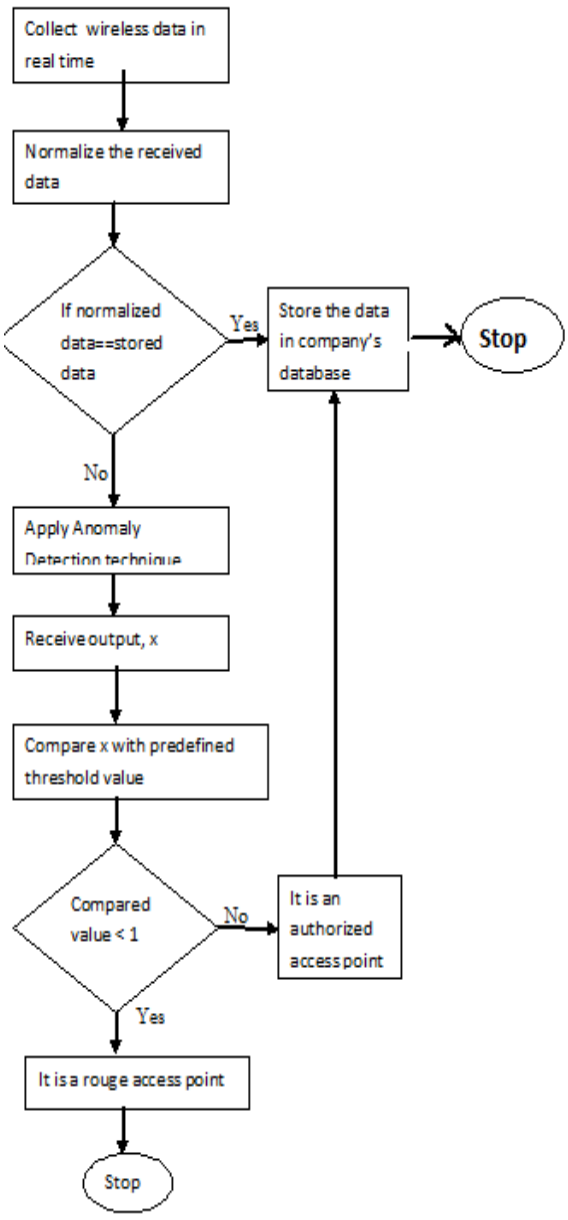

Fig-3: Flow chart of the proposed algorithm

4. CONCLUSIONS

In this paper, we proposed a solution for detection the rogue access point and also to prevent the setting up of new rogue access point within an enterprise network. The elimination of rogue access points in a wireless network has been a major research area. Our proposed solution is cost effective and also effective for existing wireless LAN. This technique works on Neural Network where the accepted network behavior is learned by the specifications of the network administrators.

REFERENCES

[1] A. Nayyar, "Security Issues on Converged Wifi & WiMax Networks", National Conference on Recent Advancements in Computer Science (RACS), Jan 2011.

[2] L.M.S.C of IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Standard 802.11g, 2003.

[3] Gopinath. N, H. Chaskar, "A quick reference to Rogue AP Security threat, rogue AP detection and mitigation", http://www.rogueap.com/rogue-ap-docs/RogueAP-FAQ.pdf, Airtight Network Report, 2009.

[4] B-T. Wang, H. Schulzrinne, "An IP Trackback Mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Vol.2, pp. 901-904, 2nd-5th May 2004.

[5] L. Zhou, Z. Haas, "Securing Ad Hoc Networks", IEEE Network, Vol.13, Issue-6, pp. 24-30, Nov-Dec 1999.

[6] R. Beyah, A. Venkataraman, "Rogue Access Point Detection: Challenges, Solutions and Future Directions", IEEE Security & Privacy, Vol.9, Issue-5, pp. 56-61, Sept-Oct 2011.

[7] S. Nikbakhsh, A. Manaf, M. Zamani, M. Janbeglou, "A Novel Approach for Rogue Access Point Detection on the Client-Side", 26th International conference on Advanced Information Networking and Applications Workshop (WAINA), Japan, pp. 684-687, 26th-29th March 2012.

[8] K. Kao, I-En. Liao, Y-C. Li, "Detecting Rogue Access Points using Client-Side Bottleneck Bandwidth Analysis", Computer & Security, Vol.28, Issue.3-4, pp. 144-152, May 2009.

[9] T. Kim, H. Park, H. Jung, H. Lee, "Online Detection of fake access points using received signal strengths", 75th IEEE Vehicular Technology Conference (VTC Spring), 6th-9th May 2012.

[10] H. El-Bakry, N. Mastorakis, "A Real-Time Intrusion Detection Algorithm for Network Security", WSEAS Transactions on Communications, Vol.12, Issue-7, pp. 1222-1234, Dec 2008.

[11] H. Debar, M. Dacier, A. Wespi, "A Revised Taxonomy for Intrusion-Detection Systems", Annales Des Telecommunications, Vol.55, Isuue-7, pp. 361-378, July 2000.

[12] M. Roesch, "Snort-Lightweight Intrusion Detection for Networks", 13th USENIX Conference on System Administration, USA, pp. 229-238, 7th-12th Nov 1999.

[13] H M. Shirazi, "Anomaly Intrusion Detection System using Information Theory, K-NN and KMC Algorithm", Australian Journal of Basic and Applied Science, Vol.3, Issue-3, pp. 2581-2597, 2009.

[14] K. Wang, S J. Stolfo, "Anomalous Payload-Based Network Intrusion Detection", 7th International Symposium on Recent Advances in Intrusion Detection, Springer-Verlag, Vol.3224, pp. 203-222, 15th-17th Sept 2004.

[15] Y. Yao, Y. Wei, F. Gao, G. Yu, "Anomaly Intrusion Detection Approach using Hybrid MLP/CNN Neural Network", 6th International Conference on Intelligent Systems Design and Applications (ISDA), USA, 16th-18th Oct 2006.

