IJCSC International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 69–71

DETECTION OF ROUGE ACCESS POINT IN 802.11G USING MA

S.V. Athawale and S.B. Vanjale

Department of Computer COE, Bharati Vidyapeeth University, Pune, India,
E-mail: sv_athawale@rediffmail.com and *svanjale @rediffmail.com.*

ABSTRACT

In the recent years, growth of the network has exploded with the appearance of information age today, network and computer technology along with the services and information available on the network are growing so fast that we will soon reach to the point where hundreds of millions of people will have fast, pervasive access to a substantial amount of information from anywhere and anytime. The mobile agent technology offers very promising solution to these problems. A present detection solution like RF Scanning, Monitoring SSID, etc. It is a challenge, however, to accurately, efficiently detect rogue AP that is protected by other security measures. Our solution uses mobile agents to quickly scan all possible rogue APs, without generating network Loads of traffics on the Network, hence saving reducing, scan and reporting time. We show that the proposed approach can energetically and successfully detect rogue APs reduce network overhead.

Keywords: Rouge Access Point, Radio Frequency ,Secure Set of Identifier.

1. INTRODUCTION

The proposed system in this paper, gives a new *Rogue* AP detection method to address the describe problem. Our solution uses Intelligent Mobile Agents to fast scan all possible rogue APs, without increasing the network Loads of traffics on the Network, hence saving resources reporting time. However we are concentrating on the mobile agent security policy and its interfacing to the deployed efficient system. Distributed mobile agent approach is used to achieve the load balancing and better network performance. Many small organizations that has a network should have some of the rogue AP detection, especially organizations that do not have wireless networks. Observing the growing demands of mobile agent users, it can be predicted that the next generation wireless networks will be burdened with bandwidth-intensive traffic generated by applications such as web browsing and web cashing. Rogue Access Points (RAPs), such as those brought into the origin of campus by employees, a security threat as they may be weakly and less secure and inefficiently managed. Any attacker in the territory can easily get onto the internal network through these illegal rogue APs, bypassing all security parameter. The mobile agent paradigm presents an efficient and clearly unique method to problem solving in the distributed environment. Using experiments, we show that the proposed approach can reduce network latency, robustly detect rogue APs with minimizing network overhead.

2. PRESENT WORK

Rogue access points are devices that are deployed in secure WLANs without permission or knowledge of the network administrator. The presence of such rogue access point poses severe threats to the WLAN security as it could compromise security of the entire wireless LAN. This problem has been in existence ever since WLANs have become popular in commercial applications [15, 16]. There have been reports of data theft, identity theft by using these rogue access points. Increasing use of wireless technologies defense establishments along with above mentioned reasons have compelled researchers all over the world to find a solution for this problem. WLANs face the same security challenges as their wired counterparts, and more. Because the medium for wireless is air, WLANs have the added issue of securing data that travels the airwaves [18]. There are three recent research efforts [7, 8, and 9] also use RF sensing to detect various rogue APs. In [1], wireless clients are to collect information about nearby APs and send the information to the centralized server for rogue AP detection. This approach is not resilient to spoofing. Secondly, it is assumed that rogue APs use standard beacon messages in IEEE 802.11 and respond to probes from the clients, which may not hold in practice. Lastly, all unknown APs (including those in the vicinity networks) are flagged as rogue APs, which may lead to a large number of false positives. The main idea of [2] is to enable dense RF monitoring through wireless devices attached to desktop machines. This study improves upon [1] by providing more accurate and comprehensive rogue AP detection. However, it relies on proper operation of a large number of wireless devices, which can be difficult to manage. In contrast, our approach only requires a single monitoring point, and is easy to manage and maintain. The focus of [3] is on detecting protected layer-3 rogue APs. Our approach is equally applicable to detect data link layer or network layer rogue devices.

2.1 Propose System Scenario

The System will divide the complete Network into different Region and the mobile agent located in that respective network. After assigning the specific area of these Mobile Agents will scan their respective area and sends the results back to the main located Server which will apply the different security Policies and rules to generate the secure and optimal Result.

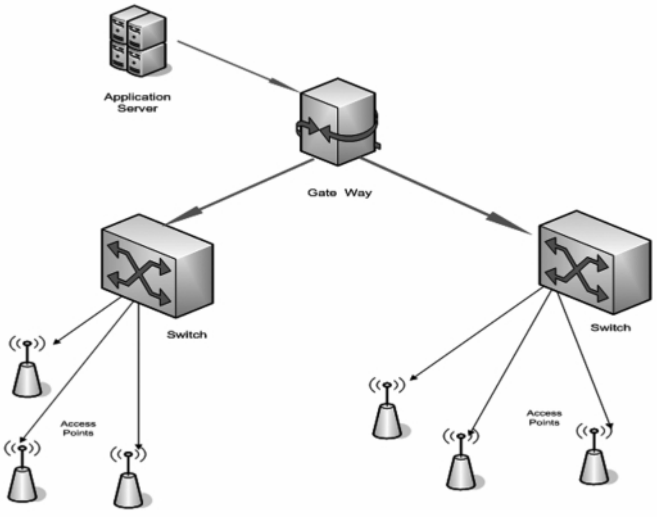

Fig. 1: Overview Propose System

2.2 Proposed Algorithm For MA

The equations are shown the time requirement for execution for the mobile agent.

$$T_{MINIMUM} = CT_E + AR_T$$

Our aim to minimize the function mobile agent that are addition of the code execution time and agent reporting time initially it start from 10 sec. In the algorithm of the mobile agent minimizing the time of mobile agent execute the particular task. In this paper, we take into account the amount of the data encounter by the mobile agent each visited node. And then give the response to the centralize server. Mobile agent always start from the processing node. In the moving node is required message, and dispatch the mobile agent to execute one second.

$$T_L = \sum_{K=10}^{N} t \cdot k \; N \geq 10 \leq 20$$

The total life span of the mobile agent to process and execute the particular query is the less than 10. Mobile agent just gives the optimal solution for rouge access point scanning and detection because it require very less memory space as compare to other technology. There are various advantages why mobile agent perform well because work on each port level with effective scanning . Mobile agent replicated so fast and reduce network load, the main objective behind using mobile agents is to move the communication to the specific data rather than the data to the computations. Distributed systems often required multiple interactions to complete the various computational task. But using mobile agent allows us to conversation among the process and send it to the destination host. Thus all the communication now take place effective and locally. The result is potentially makeable reducing the network traffic.

3. RESULT AND DISCUSSION

The results presented in this section follow the same general pattern. Each figure shows a distribution function time (DFT) of the mobile agent wireless traffic. As such, the *y*-axes of each value time graph peaks, representing the cumulative maximum value, while the *x*-axes are displayed in amount of code in size *k* are shown on the following:

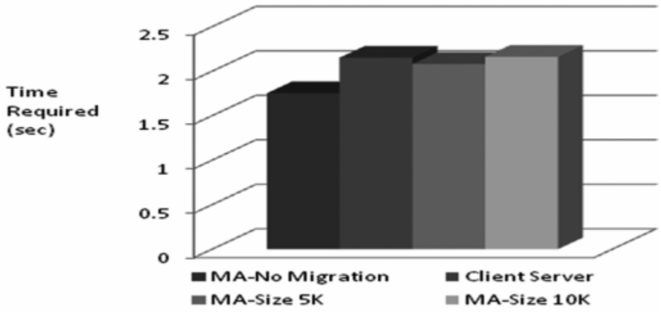

Fig. 3: Toal Time Reuired for MA/Client Server

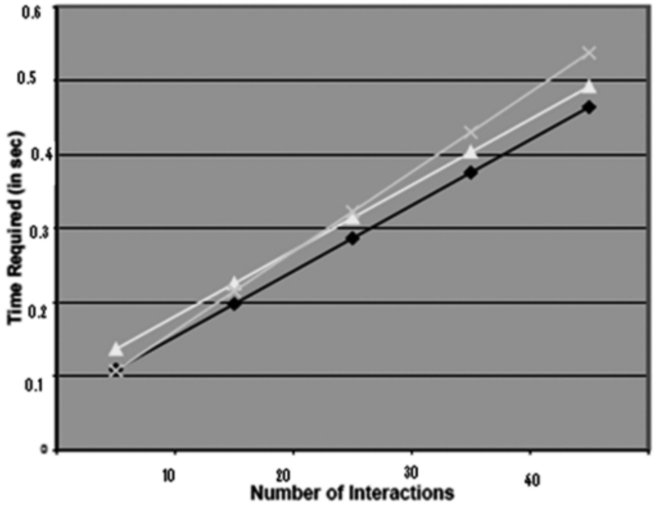

Table 1
True Test Results

Total time required (in sec)	0.1	0.2	0.3	0.4	0.5	0.6

Table 2
Imposter Test Results

Number of interaction	10	20	30	40

4. CONCLUSION

The proposed system in this paper takes advantage of mobile agents technology. Mobile agent consists of many advantages over network management system. With the help of mobile agents, the performance of the network management system is tremendously increased. At the same time, with the network system management achieves the very high stability and guarantee of performance as a result due to the effective reporting mechanism. The model will make it easier to implement and efficient network management system that can satisfy the needs in the future computing.

REFERENCES

[1] Lili Qiu, Paramvir Bahl, "Architecture and Techniques for Diagnosing Faults in IEEE 802.11 Infrastructure Networks". *In Proc. ACM MOBICOM*, September 2004, Philadelphia, Pennsylvania, USA.

[2] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the Security of Corporate Wi-Fi networks using DAIR". *In Proc. ACM MOBISYS*, 2006, Uppsala, Sweden.

[3] H. Yin, G. Chen, and J. Wang., "Detecting Protected Layer-3 Rogue APs". *In Proceedings of the Fourth IEEE International Conference on Broadband Communications, Networks and Systems*, (BROADNETS), Raleigh, NC, September 2007, Raleigh, NC, USA.

[4] R. Beyah, S. Kangude, G. Yu, B. Strickland, and J. Copeland, "Rogue Access Point Detection using Temporal Traffic Characteristics". *In Proc. IEEE GLOBECOM*, Dec 2004, Atlanta, GA, USA.

[5] C. Mano, A. Blaich, Q. Liao, Y. Jiang, D. Salyers, D. Cieslak, and A. Striegel. "RIPPS: Rogue Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts Through Network Traffic Conditioning", *ACM Transactions on Information Systems and Security*, Notre Dame, Indiana, USA.

[6] Wei Wei, Kyoungwon Suh, Bing Wang, "Passive Online Rogue Access Point Detection using Sequential Hypothesis Testing with TCP ACK-Pairs", IMC'07, October 24 – 26, 2007, San Diego, California, USA.

[7] Shetty, Sachin, Song, Min, Ma, Liran, "Rogue Access Point Detection by Analyzing Network Traffic Characteristics", *Military Communications Conference*, 2007. MILCOM 2007, Orlando, FL, USA.

[8] Srilasak S., Wongthavarawat K., Phonphoem A., "Integrated Wireless Rogue Access Point Detection and Counterattack System", *Information Security and Assurance*, 2008. ISA 2008, Pathumthani, Thailand.

[9] Beyah R. Kangude, S. Yu G., Strickland B., Copeland J., "Rogue Access Point Detection using Temporal Traffic Characteristics", *Global Telecommunications Conference*, 2004. GLOBECOM '04, Atlanta, GA, USA.

[10] Songrit Srilasak, Kitti Wongthavarawat, and Anan Phonphoem, "Integrated Wireless Rogue Access Point Detection and Counterattack System", 2008. *International Conference on Information Security and Assurance*, Busan.

[11] Kishor D., Audumbar C., "Rogue Access Point Detection Response Mechanism", *IEEE WoWMoM-SPAWN*, Jun 2008, Illionas, USA.

[12] Suman Jana Sneha K. Kasera, "On Fast and Accurate Detection of Unauthorized Wireless Access Points using Clock Skews", *International Conference on Mobile Computing and Networking*, 2008, San Francisco, California, USA.