A Hidden Markov Model Based Approach to Detect Rogue Access Points

Gayathri Shivaraj[#1], Min Song [#2], Sachin Shetty[#3]

Wireless communication and Networking Laboratory,

Department of Electrical and Computer Engineering, Old Dominion University
Norfolk, VA.

gshiv001@odu.edu

msong@odu.edu

sshetty@odu.edu

***Abstract*—One of the most challenging security concerns for network administrators is the presence of rogue access points. In this paper, we propose a statistical based approach to detect rogue access points using a Hidden Markov Model applied to passively measured packet-header data collected at a gateway router. Our approach utilizes variations in packet inter-arrival time to differentiate between authorized access points and rouge access points. We designed and developed our Hidden Markov Model by analyzing Denial of Service attacks and the traffic characteristics of 802.11 based Wireless Local Area Networks. Experimental validations demonstrate the effectiveness of our approach. Our trained Hidden Markov Model can detect the presence of a Rogue Access Point promptly within one second with extreme accuracy (very low false positive and false negative ratios are obtained). The success of our approach lies in the fact that it leverages knowledge about the behaviour of the traffic characteristics of 802.11 based WLANs and properties of Denial of Service attacks. Our approach is scalable and non-intrusive, requiring little deployment cost and effort, and is easy to manage and maintain.**

***Index Terms*—Rogue Access Points, Hidden Markov Models, Compromised Rogue Access Points and Denial of Service.**

I. INTRODUCTION

Deployment of wireless local area networks (WLANs) in commercial and military domains has been growing at a remarkable rate during the past several years. The presence of a wireless infrastructure within an organization's premises, however, raises various network management and security issues. One of the most challenging issues in WLANs is Rogue Access Points (RAPs) i.e., wireless access points that are installed without explicit authorization from a local network administrator [1]. Although usually installed by employees of the organization for convenience or higher productivity, RAPs pose serious security threats to the local network. First, they potentially open up the network to unauthorized parties, who may steal confidential information or even launch Denial of Service (DOS) attacks in the network.

According to an early study by Gartner [2], rogue APs are present on about 20% of all enterprise networks. The main reason is advancements in hardware and software have made AP installation, AP discovery, and AP compromise an easy task for attackers. It is convenient to obtain an AP and plug into a network without being discovered for some time. Moreover, commodity Wi-Fi network cards have the capability to capture all 802.11 transmissions. This has led to increase in the process of driving around and looking for vulnerable APs (war-driving activities).

The main contribution of this paper is a novel approach for RAP detection based on measurements collected at the edge of a network. The approach detects a RAP by observing the traffic characteristics of the associated individual end hosts. It is probabilistic and uses Hidden Markov models (HMMs) to represent the likelihood of transitions between the different security states of an access point. This approach roughly works as follows. We first train the HMM model based on a training data set, which has information gleaned from packet traces. The packet traces are collected from a test-bed wherein traffic comprises of normal Internet activities and DoS [2] attacks. Once the HMM model is trained, we monitor the packet arrivals of different flows at the edge of the network. By observing the packet inter-arrival time of these flows, the HMM model detects an access point as a RAP or an authorized access point.

The rest of the paper is organized as follows. Section 2 briefly discusses the related work. The proposed HMM based RAP detection approach is elaborated in Section 3.The detailed analysis of the approach is provided in Section 4. The evaluation results are presented in Section 5. Finally, we conclude in Section 6.

II. BACKGROUND AND RELATED WORK

A comprehensive taxonomy of RAP detailing different categories of RAPs has been presented by Ma et al. [3]. The authors have categorized access points in the following four classes: improperly configured,

978-1-4244-2677-5/08/$25.00 ©2008 IEEE

unauthorized, phishing, and compromised. The brute-force approach of RAP detection used by most enterprises is to equip IT personnel with wireless packet analyser tools and scan the network traffic [4-5]. AirDefense [4] is one such product. It uses a combination of radio frequency sensors and an intrusion detection server to capture process, and correlate network events. However, the latest release, AirDefense 7.2, has a starting price of US $7,995. Also, the RF sensors make it difficult to guarantee a complete coverage of the network to ensure effective rogue AP detection.

To the best of our knowledge there are few research efforts on detecting RAP. Fault diagnostics in IEEE 802.11 networks is presented in [6]. Multiple APs and mobile clients perform RF monitoring to help detect the presence of RAPs. Each client is equipped with special diagnostic software, and RAPs are assumed to transmit beacon messages and respond to probe requests. Further, its detection ability is not based on the assumption that RAPs will function properly.

Bahl *et al*. [7] propose a distributed monitoring infrastructure called DAIR. It attaches USB wireless adapters to desktop computers for more comprehensive traffic capturing ability. The effectiveness of DAIR is dependent on AP functionality that can be easily turned off. Additionally, both of [6] and [7] assume that characteristics of IEEE 802.11 standards cannot be violated by the adversaries.

Differences in inter-packet spacing between traffic flows on wired and wireless networks is used in [8-9] for identification of rogue APs. However, the scheme does not differentiate between wireless traffic from authorized and unauthorized APs. It also assumes that APs will be connected within one hop to a switch monitoring the traffic, and relies on visual inspection of traffic characteristics. Multiple network sniffers are used in [2] for detecting rogue APs and eavesdroppers. Each sniffer has three network cards, and the intrusion detection capabilities are stymied by MAC address spoofing. Yeo et al. [6] improve the performance of wireless monitoring by merging packet captures from multiple network sniffers and carefully selecting sniffer placement. The techniques are exploited to characterize MAC layer traffic and perform retrospective diagnoses.

Recently, two passive online rogue AP detection algorithms are proposed in [10]. The core of these two algorithms is the sequential hypothesis tests applied to packet-header data that are passively collected at a monitoring point. Both algorithms exploit the fundamental properties of the 802.11 CSMA/CA mechanisms and the half duplex nature of wireless channels to differentiate wired and wireless LAN TCP traffic. Once TCP ACK-pairs are observed, prompt decisions are made with little computation and storage overhead. Yin et al. [11] propose a layer-3 rogue AP detection approach using the combination of a verifier and wireless sniffers. In this approach, a verifier on the internal wired network is employed to send test traffic towards wireless edge. Once wireless sniffers capture an AP relaying the test packets, the AP is flagged as rogue. In addition, binary hypothesis testing technique is adopted to improve the robustness of detection.

A router throttle mechanism was used for countering Distributed Denial of Service (DDoS) attacks directed at an Internet server [16]. This mechanism specifically targetted Neptune type of DDoS attacks. The authors have advanced a control-theoretic, server-centric model useful for understanding system behaviour under a variety of parameters and operating conditions. The adaptive throttle algorithm is effectively used to protect a server from resource overload, and increase the ability of normal traffic to arrive at the intended server. The results indicate that server-centric router throttling is a promising approach to prevent DDOS attacks, but several nontrivial challenges like low computation and memory overheads remain that prevent its immediate deployment in the Internet.

A tool for statically validating a TCP server's ability to survive SYN flooding attacks has been proposed [18]. The tool automatically transforms a TCP-server implementation into a timed automation, and it transforms an attacker model, given by the output of a packet generator, into another timed automation. Together the two timed automata for a system for which the model checker UPPAAL can decide whether a machine is in a bad state, in which the buffer overruns, can be reached.

Hidden Markov Models (HMMs) have also been used to classify Network Intrusions [17]. The HMMs were modelled to detect buffer overflow based attacks. The disadvantage of this method is it cannot be applied for detection of attacks that are performed over a long period.

Our proposed framework differs from previous work in which it provides an efficient and prompt detection of RAPs by analysing the traffic characteristics of WLANs. It also defends against a more insidious type of rogue APs, i.e., the compromised APs, that has never been addressed in the literature before. According to Queuing theory, "average service time must be less than the inter-arrival rate or the system is unstable". Our model can detect rogue access points, which are the source of specific DOS attacks. Moreover, the deployment of this model does not require modifications to the underlying wireless standard. This makes our framework an efficient and cost-effective solution.

III. PROBLEM DEFINITION AND APPROACH

In this section, we state our RAP detection problem and describe, at a high level, our approach towards solving this problem. Consider a wireless local area network, e.g., a university campus or a military network, as illustrated in Fig. 1. End hosts within this network only use 802.11 WLAN to access the network. A monitoring point is located at the gateway router of this wireless local network, capturing traffic flows coming in and

going out of the network. The end hosts are connected to three access points (AP1, AP2, and AP3). Each of these access points can be termed as authorized or rogue depending on the traffic generated by them. The end hosts authorized access points generate traffic indicative of normal Internet activities (web browsing, email, ftp transfer, etc.). The end hosts connected to the RAP are the source of DOS attacks. Our goal is to determine 1) what fraction of traffic flows are source of DOS attacks (2) for each traffic flow, what is the probability that this particular traffic flow originated from a RAP.

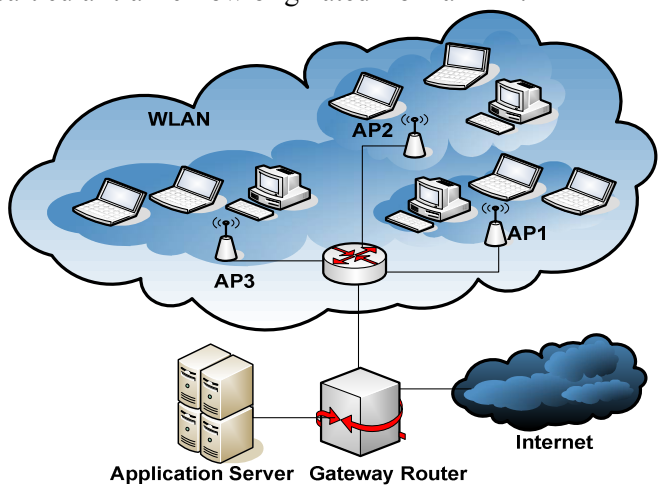

Fig. 1 Network Configuration

Our approach utilizes the intrinsic characteristics of WLAN connections and DOS attacks. The approach operates roughly as follows. For packets belonging to each traffic flow, the inter-arrival times are observed at the monitoring point. As will be shown in Section III, the inter-arrival times for packets originating from authorized access points and RAPs differ significantly. Our trained HMM exploits this difference to differentiate traffic originating from authorized access points and RAP.

In next section, we present the analytical basis of our scheme, which demonstrates how the inter-arrival times will differ for traffic flows originating from authorized access points or an RAP. We then describe the design of the HMM (the core of our classification scheme).

A. Hidden Markov Model Based RAP Detection approach

The use of Hidden-Markov Models (HMMs) as a method for detecting intrusion detection in an individual computer system has been proposed [12-14]. An HMM enables the estimation of a hidden state based on observations that are not necessarily accurate. An important feature of this model is that it is able to model the probability of false positives and false negatives associated with the observations. The method is based on Rabiner's work on HMMs [15].

In our problem setting, we use the HMM to describe the current security state of the access points in the network. The security state of the access point can be identified by observing the inter-packet arrival time in the packet traces. These packet traces help us determine the state of an access point and thereby detect the RAPs.

Assume that each access point AP can be modelled by N different security states, i.e. $S = \{s_1, ..., s_N\}$. The security state of an access point changes over time, which is an indication of normal or rogue activities. The sequence of states visited by an access point is denoted by $X = x_1, ..., x_T$, where $x_t \in S$. Traffic flowing through each access point is monitored at the gateway router. The monitoring process keeps track of the inter-arrival time of the traffic flow. A range of inter-arrival times is represented as an observation message. The ranges of inter-arrival times are represented as observation messages from the observation symbol set $V = \{v_1, ..., v_M\}$, where M is the total number of messages (or unique ranges). The sequence of observed messages is denoted by $Y = y_1, ..., y_T$, where $y_t \in V$ the observation message is received at time t. The HMM for each host consists of a state transition probability matrix P, an observation probability matrix, and an initial state distribution π . The HMM is denoted by $\lambda = (P, Q, \pi)$. The access points modelled in this paper are assumed to have three possible security states *S= {G, P, C}* which are defined as follows:

Good (G): The access point is not subject to any attacks. This state represents that the access point is not probed or attacked and it behaves normally in the network without any intrusive activity.

Probed (P): The access point is subject to probing. Port sweeping is a good example of probing. This shows that the access point can be compromised or attacked by unauthorized hosts in order to intrude into the network.

Compromised (C): It shows that an unauthorized user, which tried to intrude into the network, has compromised the access point. This is the state where the access point has been attacked and the access points begin to malfunction in the network and try to intrude in the network activities.

Fig. 2 shows the HMM model for the security states of the access point. The edge from one node to another represents the fact that when an access point is in the state indicated by the source node it can transit to the state indicated by the destination node. Note that the graph is fully connected, which indicates that it is possible to transit from any security state to any other security state.

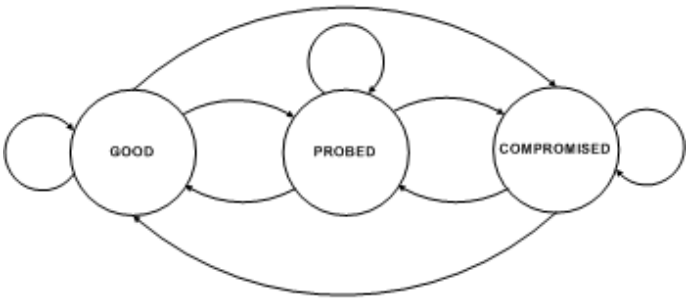

Fig. 2 Three state HMM model

The state transition probability matrix P describes the probabilities of transitions between the states of the model. The transition probability p_{ij} describes the probability that the model will transfer to state s_j at time $t+1$ given that it is in state s_i at time t, i.e.,

$$p_{ij} = P(x_{t+1} = s_j \mid x_t = s_i), 1 \le i, j \le N.$$

The observation probability matrix Q describes the probabilities of receiving different observations given that the access point is in a certain state. Each observation, $q_n(m)$ represents the probability of receiving the observation symbol v_m at time t, given that the access point is in state s_n at time t,i.e.,

$$q_n(m) = P(y_t = v_m \mid x_t = s_n), 1 \le n \le N, 1 \le m \le M.$$

In next section, we will describe in details the two main stages of the HMM based RAP detection: HMM Training and Detection.

IV. HMM TRAINING AND DETECTION

In this section, we present the details of the two main stages in our approach. Stage 1 is the training of the HMM based on packet traces. Stage 2 is the detection of RAP by the trained HMM.

The goal of HMM training is to estimate appropriate values for the model parameters ***P*** and ***Q***. A uniform initial distribution of the ***P*** and ***Q*** parameters is adequate as a basis for training the parameters, according to [15]. The initial parameters can alternatively be determined by network administrator based on traffic statistics collected over a period of time. These methodologies provide a framework for identifying threats and vulnerabilities and for determining probabilities and consequences of DOS attacks. Based on a HMM with initial parameters, there are several algorithms available for re-estimating the parameters (i.e., training the models). There is, however, no analytical solution to the re-estimation problem.

A standard approach for learning HMM parameters is the Baum-Welch method, which uses iteration to select HMM parameters to maximize the probability of an observation sequence. We adopt the Baum-Welch method to estimate the HMM parameters for our model. The first step in the estimation process is to generate the training set. We refer to a set of traffic flows from which the observation distribution is obtained as a training set.

We setup a network as illustrated in Fig. 1. Next, we present the three known DOS attacks detected by our model. There are two types of DOS attacks, logic and flooding attacks. We have mainly focused on the flooding attacks. The three DOS attacks considered in this paper are presented in Table 1. The attacks are generated by the end hosts connected to the RAP.

Attack	Description
Pod	DOS using oversized ping packets
Portsweep	Sweep through many ports to determine available services on a single host.
Neptune	Syn flood DOS

Table 1 - Attack Repertoire

The end hosts, which are connected to authorized access points generated traffic corresponding to normal web activities (browsing, email, ftp, etc). Packet arrivals in wireless LAN are modelled as Poisson process with exponential inter-arrival times [13-14]. For example, http traffic was represented by setting the web page inter-arrival time an exponential distribution with a mean value of 60 seconds and the number of pages also followed an exponential distribution with a mean value of 10 pages.

Packet traces for the three access points in Fig. 1 were collected over a one hour time frame. The key distinguishing characteristic between the traffic generated by the normal end hosts and the rogue end hosts is the packet inter-arrival time. So we use the packet inter-arrival as the observation parameter for our HMM model. Based on the distribution of the inter-arrival times, we have identified three prominent inter-arrival ranges R1, R2 and R3. These ranges address all the traffic in the packet trace. Suppose that a set of n_t packets are identified in the training set. Let x_i denote the inter-arrival times of the i^{th} packet. The value of x_i is discretized as follows: If x_i lies within the range of R1, it takes a value of 1, for R2 the value is 2 and finally for R3 the value is 3. Thus, the observation distribution is obtained from the discretized value of x_i, $i = 1, 2, \ldots, n_t$.

Having generated the observation distribution from the training set, the final step of the training phase is to estimate the parameters of the model. The parameter estimation was implemented in Matlab with the help of routines provided by Kevin Murphy in the Hidden Markov Model Toolbox for Matlab [14].

After training the HMM model, the next step is to perform detection of RAPs. The detection process was carried out by generating packet traces from the same network setup used for the training purposes. Observation distributions were extracted from the packet traces. For the detection process, we employed the Viterbi algorithm from the HMM toolbox [14]. Viterbi algorithm is a dynamic algorithm for finding the most likely sequence of hidden states called the Viterbi path, which results in a sequence of observed events. This algorithm gives the optimal state sequence for a particular HMM model. For our detection process, this algorithm will give the state of the access point in the network. The output of the detection procedure is a sequence of security states of the access point corresponding to each packet in the trace file. In the next section we evaluate the HMM model to analyse the accuracy and promptness of the detection process.

V. Simulation and Results

In this section, we use the network setup in Fig. 1 to obtain the performance results in terms of detection accuracy and promptness.

A. Network Model

The laptops are connected via IEEE 802.11b WLAN interface to the access points and the desktops are connected via Ethernet interfaces to the router. For each access point, traffic is generated from the laptop and the desktop respectively. For the rogue activity, there is an unauthorized host outside the network, trying to perform some intrusive activity in the network and get access into network by getting connected to one of the access points and compromise the access point. The goal is to detect the compromised Rogue access point attacked by the unauthorized client.

B. Detection Accuracy

Detection accuracy is evaluated by computing the successful detection of RAP, false positives, and false negatives. False positives indicate misidentification of an authorized access points as a RAP. False negatives indicate miss detection of the presence of RAP. In our experiment setup, the end hosts are laptops which communicate via IEEE 802.11b WLAN interface to the access points. The source of the rogue activity is a "roaming" laptop carrying out attacks depicted in Table 1. An access point which is currently under attack by this "roaming laptop" is a RAP. The goal of our model is to report all instances of the presence of RAP. Traffic was generated from all laptops for a period of 60 minutes. The traffic was collected at the gateway router and an offline detection process was carried out using the trained HMM model.

In Fig.3 the detection accuracy of the HMM model is presented for all three access points. The three access points exhibit all three security states during the 60 minute time limit. The detection accuracy measures the effectiveness of the model to detect the compromised security state. A compromised security state indicates that the access point is acting as a RAP. The detection accuracy is consistent for all the three access points. The model exhibits 85 % accuracy with very slight variance. With a larger training set, the detection accuracy of the model will increase. Fig. 4 illustrates the number of false positives encountered during the detection process.

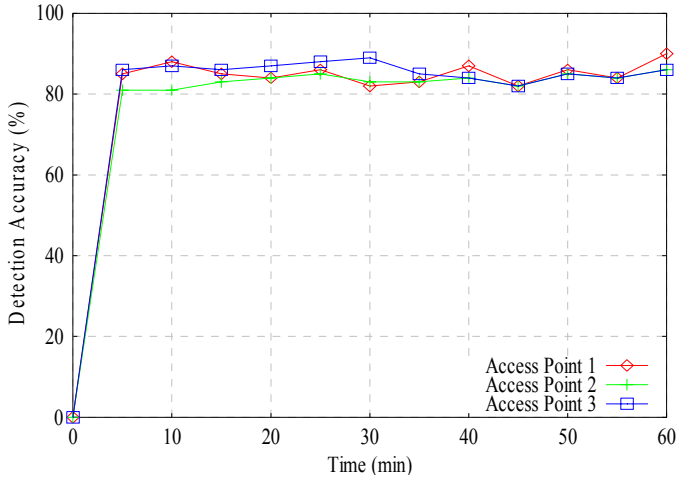

Fig. 3 Detection Accuracy

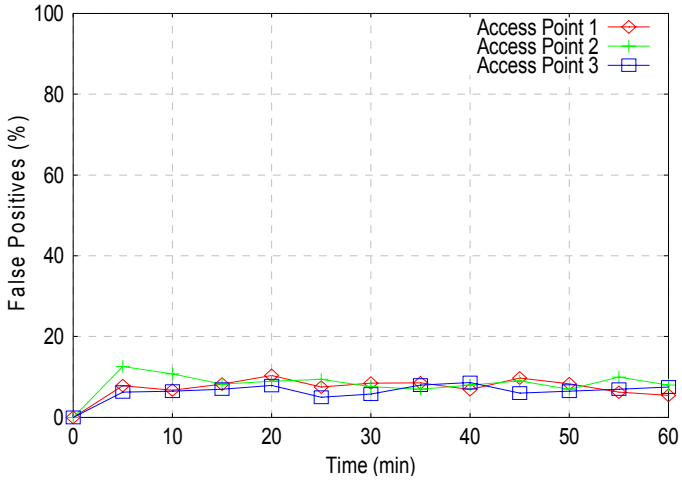

Fig. 4 False Positives

Fig. 5 illustrates the number of false negatives encountered during the detection process. The average number of false positives and false negatives are close to 8 % with slight variance. The number of false positives and false negatives can be decreased further, if the training is performed on a larger training set.

Finally in Table 2, we demonstrate the promptness of the detection process. Four attack instances are identified in the packet traces. The detection time in milliseconds for two access points are reported. The presence of a RAP is detected within less than a second. The quick detection of a RAP is equally important as increasing the detection accuracy.

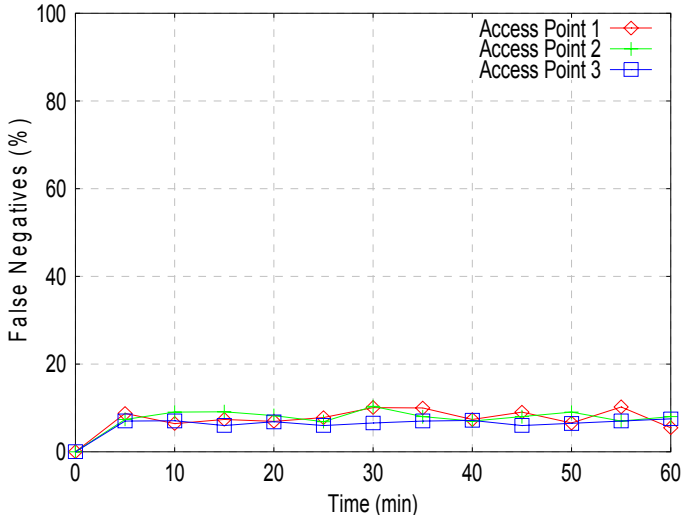

Fig. 5 False Negatives

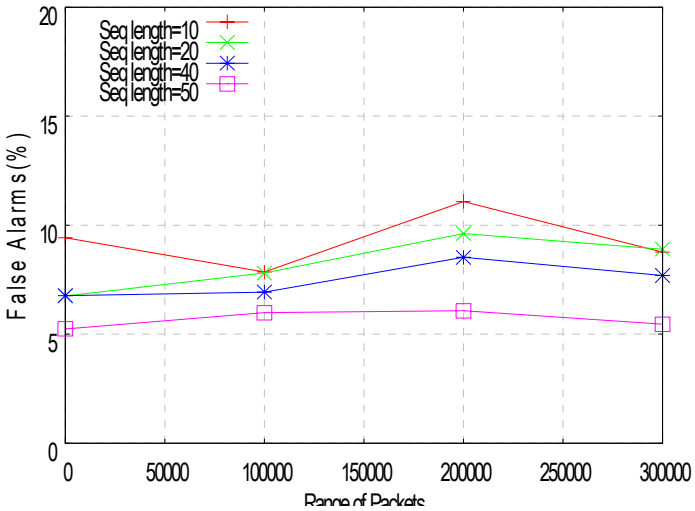

Fig. 6 False Alarms

Attack Instance	Detection Time (milliseconds)	
	Access Point 1	Access Point 2
1	345	552
2	797	66
3	797	537
4	803	174

Table 2 - Detection Time

C. Detection Accuracy for varied sequence lengths

The sequence length is defined as the length of the observation sequence taken into consideration by the Viterbi algorithm In Figs 3-5, the sequence length was equal to 10 packets. In this section, we present simulation results with sequence lengths varying between 10 to 60. Fig. 6 illustrates the number of false alarms (false positives) encountered during the detection process at AP3. It can be observed that the number of false negatives is not affected by varying the sequence lengths. This property ensures that our HMM is invariant to variation in sequence lengths. With a large training data set, it is possible that larger sequence lengths will be used for the detection process. Thus, the detection accuracy of our HMM will not be affected by larger training datasets.

Fig. 7 illustrates the number of missed detections (false negatives) encountered during the detection process. Similar to Fig.6, the numbers of false negatives are also not affected by varied sequence lengths.

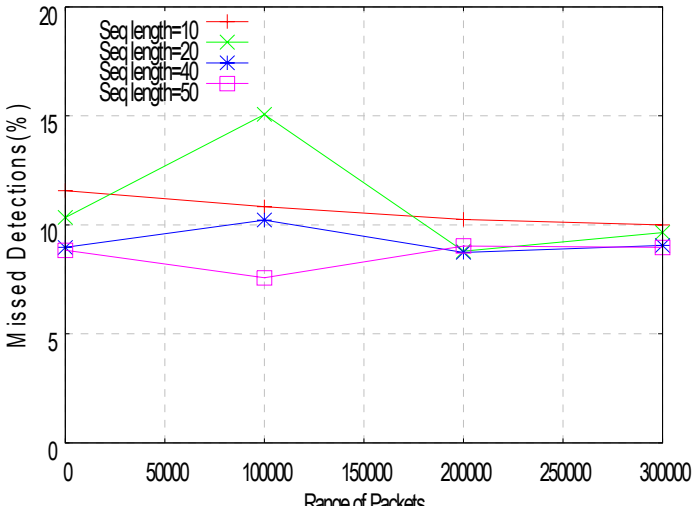

Fig. 7 Missed Detections

VI. CONCLUSION

In this paper, we designed an efficient and prompt HMM to detect the presence of RAPs in a WLAN. The HMM model is implemented at the gateway router where traffic is captured and analysed. Our approach comprises of two stages. The first stage is the training of a HMM and second stage is the detection of RAP based on the trained HMM. The presence of a RAP in our network is due to end hosts performing three specific DOS attacks. Our model is capable of detecting a RAP whenever an end host performs any of the DOS attack mentioned in the paper. The detection accuracy and promptness of the HMM has been evaluated by performing experimental results. The presence of RAP is detected within one second and the average detection accuracy is 85%. In our future work, we plan to improve the detection accuracy of our model. The performance of the model will be

evaluated using different network setups and various traffic scenarios.

REFERENCES

[1] White Paper, Rogue Access Point Detection: Automatically Detect and Manage Wireless Threats to your Network. [Online] Available at http://www.proxim.com.

[2] Kim, M-S., Kang, H.-J., Hung, S.-C., Chung, S.-H., and Hong, J.W., "A Flow-based Method for Abnormal Network Traffic Detection," *IEEE/IFIP Network Operations and Management Symopsium*, Seoul, 2004.

[3] Liran Ma, Amin Y. Teymorian, Xiuzhen Cheng, Min Song, "RAP: Protecting Commodity Wi-fi Networks from Rogue Access Points," *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine)*, August 2007, Vancouver, British Columbia.

[4] "AirDefense enterprise: a wireless intrusion prevention system." [Online]. Available: http://www.airdefense.net/.

[5] "AirMagnet: Enterprise WLAN management" [Online]. Available: http://www.airmagnet.com/.

[6] A. Adya, P Bahl, R. Chandra, and L. Qui, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastruture networks", *in MobiCom*, 2004.

[7] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the security of coporate wi-fi networks using DAIR," in MobiSys: *In Proc. Of the 4th International conference on Mobile systems, applications and services. New York*, NY, 2006.

[8] R. Beyah, S. Kangude, G. Yu, B. Stirckland, and J. Copeland, "Rogue access point detection using temporal traffic characteristics," *In proc. Of GLOBECOM,* Dallas, TX, 2004.

[9] S. Shetty, M. Song, and L. Ma, "Rogue access point detection analysing network traffic characterstics," *in MILCOM*, Orlando, Florida, October 2007.

[10] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, "Passive online rogue access point detection using sequential hypothesis testing with TCP Ack-Pairs," *In proc. Of the 7th ACM SIGCOMM conference on Internet measurement, New York*, NY, 2007.

[11] H. Yin, G. Chen, and J. Wang, "Detecting Protected Layer-3 Rogue APs," *In Proc. Of the Fourth IEEE International Conference on Broadband Communications, Networks, and Systems*, Raleigh, NC, September 2007.

[12] N. Ye, "A Markov chain model of temporal behaviour for anomaly detection," the *IEEE Systems Man and Cybernetics Information Assurance and Security Workshop*, West Point, NY, 2000.

[13] Y. Zheng, K. Lu, D.W. Fang, "Performance Analysis of IEEE 802.11 DCF in Imperfect Channels", *IEEE Transactions on Vehicular Technology,* Sep 2006.

[14] K. Murphy, "Hidden Markov Model(HMM) Toolbox for MATLAB," online at http://www.ai.mit.edu/~murphyk/Software/HMM/hmm.html.

[15] Lawrence R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *In Proc of IEEE*, Feb 1989.

[16] David K. Y. Yau, John C. S. Lui, Feng liang, Yeung Yam, "Defending Against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles," *IEEE/ACM Transactions on Networking*, 2005.

[17] Svetlana Radosavac, John S. Baras, "Detection and Classification of Network Intrusions Using Hidden Markov Models," *Conference on Information Sciences and Systems,* 2003.

[18] Krishna Nandivada. V, Jens Palsberg, "Time analysis of TCP servers for surviving denial-of-service attacks," *Proc. Of the 11th IEEE Real Time and Embedded Technology and Applications Symposium(RTAS'05).*