Work Flow based on a Mathematical Model to Detect the Presence of Rogue AP's in Wi-Max Networks Using the Various Values of Size of Contention Window

Amit Verma [1*], Mandeep Kaur [1], Bharti Chhabra [3]

[1*] *Professor and Head of Department, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India*

[1]*M. Tech. Research Scholar, Computer Science & Engineering, Chandigarh Engineering College, Landran, Punjab, India*

[3]*Assistant Professor, Computer Science& Engineering, Chandigarh Engineering College, Landran, Punjab, India*

Abstract – Problem Statement: Due to the multi-hop nature of the WMNs, the routing mechanisms are essential to the smooth, effective running of the network. Compromising this area could seriously damage network performance. It is therefore of utmost importance that it is kept secure. Possible threats that a WMN can succumb to if its routing mechanisms are not secure:

• Deteriorating performance of the network by increasing the length of communication paths between the WHS and the TAPs.

• Isolation of a TAP which could inadvertently mean the isolation of a geographic region (which connects to the network by means of the isolated TAP).

• Redirecting traffic through a particular TAP in order to monitor the traffic. This work is being performed to detect the presence of a malicious node in a network of ten nodes. In this simulation all the nodes will try to take the access to the other nodes on the basis of the size of the contention window size. The algorithm set the minimum, maximum and threshold values of the contention window. The rouge AP tries to take access by setting the size of the contention window to satisfy the threshold value and after getting successful the RAP will take channel access through subnet mask of the node.

Analysis/ Objectives:

To develop a Wi-Max Network Environment having Base Stations and Access Points.
Simulate Rogue Access Points Attack.
Develop an Algorithm to detect.
Calculate the accuracy of intrusion detection system.

Findings:

In the first step of the research work all the nodes are trying to get the access of the serving AP by accessing the IP address and subnet mask of the serving AP.
And the network scanning is going on for all the nodes trying to get access.
In this research this simulation will repeat for ten time and in each simulation every demanding AP can try for maximum seven times.

I. INTRODUCTION

After conducting a thorough study on the research we tried to simulate the scenario in which a Rouge Access Point tries to influence the routing path of the users acting it. In this attack the RAP tries to get channel access by reducing its contention window and at the same time getting its credentials validated and thus by multiple attempts it successfully diverts the routing towards its preferred subnet mask. In this research I tried to identify possible parameters based on which we can do detection and identify the abnormal behavior in the network.

II. MATHEMATICAL MODEL

1.) Let n be an array of nodes representing AP
AP = {a1, a2, ...an }

2.) Let L be the length and B be the breadth of the network service area.
L = 100 , B = 100

3.) Let APx, APy, APz be the array representing co-ordinate positions in vector space model of each AP.

4.) Let Cn be the number of channels in the spectrum and T represents time slots.

5.) Let cwmin and cwmax be the value representing minimum and maximum window size.

6.) Let submask be set of subnet mask working with all APs.

7.) Let Tcw be threshold represent the maximum allowable window size.

8.) Let MaT be a variable represents message arrival time

Let PL be the packet length.
According to the model the algorithm verifies and validates the two primary parameter i.e.:-

- Channel access parameters
- Key credentials

```
for each message arrived
    for each channel in spectrum
        for each time slot
            for source and destination
                validate channel access parameters
                validate Key credentials
                if channel access parameter
                invalid
                mark = suspicious
                if Key credentials not matching
                mark = suspicious
            end
        end
    end
end
```

For both source and destination in each time slot for every channel in the spectrum on the arrival of every new message at the every node. If the channel access parameters satisfy the threshold value then it next verify the key credentials. If both the parameter satisfy the condition then it will assign the flag 1 and allow the communication. If any one of the parameter is being compromised the system will mark it as suspicious node and assigns the flag 2 and locate it as RAP.
A handover can be initiated by a AP when the Channel Parameters and Key credential fall below a certain threshold. As a prelude to a handover, a AP can explore the neighborhood and discover other available APs. To conduct that exploration, the AP can make a demand to its serving AP for a time interval during which the validation of the parameters is being conducted. The process is termed a scanning interval and is depicted in The scanning interval allocation request (AP-SCN-REQ) message is sent by a AP to its serving AP. The AP replies with a scanning interval allocation response (AP-SCN-RSP) message. The response contains IDs (i.e subnet mask) of recommended APs. During the allocated scanning interval, the demanding AP may perform association tests with the recommended APs. The AP may conclude by sending a scanning result report (AP-SCAN-REPORT) message to the serving AP. The demanding AP

reports the parameters of the recommended APs. The report consists of a list of pairs. Each pair consists of a AP ID and a corresponding key credentials.

If both the parameter satisfy the condition then it will assign the flag 1 and allow the communication. If any one of the parameter is being compromised the system will mark it as suspicious node and assigns the flag 2 and locate it as RAP. A handover can be initiated by a AP when the Channel Parameters and Key credential fall below a certain threshold. As a prelude to a handover, a AP can explore the neighborhood and discover other available APs. To conduct that exploration, the AP can make a demand to its serving AP for a time interval during which the validation of the parameters is being conducted. The process is termed a scanning interval and is depicted in Figure 1. The scanning interval allocation request (AP-SCN-REQ) message is sent by a AP to its serving AP. The AP replies with a scanning interval allocation response (AP-SCN-RSP) message. The response contains IDs (i.e subnet mask) of recommended APs. During the allocated scanning interval, the demanding AP may perform association tests with the recommended APs. The AP may conclude by sending a scanning result report (AP-SCAN-REPORT) message to the serving AP. The demanding AP reports the parameters of the recommended APs. The report consists of a list of pairs. Each pair consists of a AP ID and a corresponding key credentials.

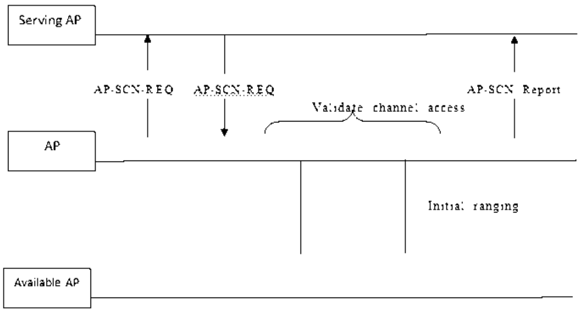
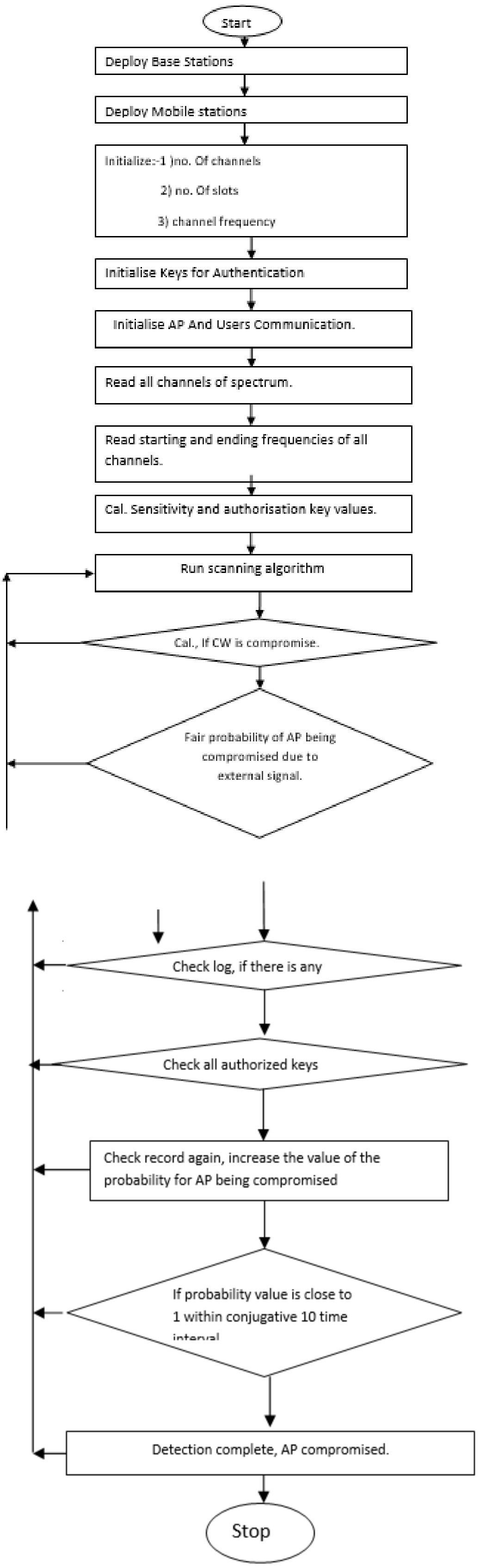


Fig: Scanning Interval Procedure

The model is documented in a book of Rappaport and Rappaport [14]. The model described in that book has been validated experimentally by a number of authors, for example see the work of Seidel et al. [17] and Sarkar et al. [18] and numerous additional references on that topic.

III. WORK FLOW BASED ON ABOVE SUGGESTED MODEL


Start
Deploy Base Stations
Deploy Mobile stations
Initialize:-1)no. Of channels
2) no. Of slots
3) channel frequency
Initialise Keys for Authentication
Initialise AP And Users Communication.
Read all channels of spectrum.
Read starting and ending frequencies of all channels.
Cal. Sensitivity and authorisation key values.
Run scanning algorithm
Cal., If CW is compromise.
Fair probability of AP being compromised due to external signal.
Check log, if there is any
Check all authorized keys
Check record again, increase the value of the probability for AP being compromised
If probability value is close to 1 within conjugative 10 time interval
Detection complete, AP compromised.
Stop

IV. LITERATURE SURVEY

Rogue-Base Station Detection in WiMax/802.16 Wireless Access Networks. This paper basically works on a scenario which is recorded in WiMax documentation in which a rouge base station having malicious intent in personates and creates a denial-of-service threat. The intrusion detection system designed in this have been based on the concept of global management system which consist of observing the scanned log of RSS(received signal strength) and multiple mobile stations. It finds inconsistent an arbitrary behavior in the scan log and a detection is assumed.

Rogue Access Point Detection by Analyzing Network Traffic Characteristics.

In this paper a research has been done to automate the process of detecting AP's which are behaving as rouge and have unauthorized access in the WLAN which is heterogeneous in nature. In the end of paper effectiveness of this technique have been discussed based on the threshold mechanism of the cross-access.

A Hybrid Rouge Access Point Protection Framework for Commodity Wi-Fi Networks.

In this research a protection framework for commodity WiFi network and system have been developed to create defense mechanism for AP's. This paper basically talks about three types of classes of rouge AP compromises. The major focus of this research is the use of the concept of finger printing to make the IDS robust. The result of this paper are promising based on the ROC curve discussed.

The Sneeze Algorithm:

This paper is doing bimimigary to design IDS. They are calling this algorithm
as sneezing and it is getting its inspiration from the biological sneezing.

Detection of Rouge Base Station Using MATLAB.

This paper considers the problem of detecting rogue base station in WiMAX/802.16 networks. A rogue base station is an attacker station that duplicates a legitimate base station. The rogue base station puzzles a set of subscribers who try to get service which they believe to be a legitimate base station. It may lead to disturbance in service. The strategy of attack depends on the type of network. Our approach is based on the inconsistencies in sensitivity and received signal strength (RSS) reports received by mobile stations can be seen if a rogue Base Station (BS) is present in a network. These reports can be assessed by the legitimate base stations, for instance, when a mobile station undertakes a handover towards another BS. A new algorithm for detecting a rogue base station is described in this paper.

A Novel Header Matching Algorithm For Intrusion Detection Systems

This paper proposed a novel algorithm to detect the intruders, who's trying to gain access to the network using the packets header parameters such as; source/destination address, source/destination port, and protocol without the need to inspect each packet content looking for signatures/patterns. However, the “Packet Header Matching” algorithm enhances the overall speed of the matching process between the incoming packet headers against the rule set. We ran the proposed algorithm to proof the proposed concept in coping with the traffic arrival speeds and the various bandwidth demands. The achieved results were of significant enhancement of the overall performance in terms of detection speed.

V. CONCLUSION

In this work, we developed a practical frame work targeting pre-empting attacks that can create rouge AP’s and detecting the presence of such devices when they exist. This is the first framework that correlates alerts containing all data from position surveillance of all nodes of a network. An attractive feature of this scenario it require neither specialized hardware nor modification to existing security standards. Further, it can be connected to or implemented on all APs trying to take access. It also make use of freely available mature software in order to provide a cost-effective security solution.

In this research a new algorithm, which is based on the size of contention window is being processed to detect the presence of rouge access point in the network. The basic idea behind the algorithm is that the system will set the minimum, maximum and threshold values of the channel parameters in a network. Whenever a malicious access point will try to get the access to the other authorized access point to divert the path of the packets, it has to satisfy the threshold value of the channel parameters. This algorithm will assign Flag2 that RAP as it is a suspicious and will allow that RAP to try for some fixed number of times. If the RAP became successful in handshaking with any other authorized AP then it will be get isolated with respect to the location so that further action can be taken.

Lastly, it can detect the presence of rouge APs even when assuming that adversaries have the ability to use customized equipment that violates the IEEE 802.11 standard. Our framework is the first one that can successfully detect the presence of malicious nodes of a network of any size using the threshold value of content window.

VI. FUTURE WORK

Our algorithm is taking the size of content window as the main parameters for detecting the rouge APs. This algorithm is very successful and accurate in detecting the presence of rouge APs. However these days faking and hacking are dynamic subject and the scenario of such malicious rouge access point may appear again in overcoming our current scenarios and algorithm. It will require constant updation in changing hacking scenarios.

Also we plan to evaluate the proposed framework in more open environment, where there are more background noises that may cause false positives. Additionally, we are anticipating the inclusion of new features for the framework that can further improve its network security abilities. One such feature is a Sneezing algorithm that can be used to better pre-empt various attacks.

VII. REFERENCES

[1]. IEEE Standard for Wireless Lan- Medium Access Control and physical Layer Specifications, ANSI/IEEE Standard 802.11, 1999 Edition (2003)

[2]. Thomas M. Chen, Geng-Sheng Kuo, Zheng-Ping Li, “Intrusion Detection in Wireless Mesh Networks”, “Understanding Intrusion Detection Systems”, SANS Institute InfoSec Reading Room, 2001

[3]. Vital Mynampati , Dilip Kandula , Raghuram Garimilla , Kalyan Srinivas “Performance and Security of Wireless Mesh Networks”

[4]. Aguayo, Bicket, Biswas and Morris (2005), “Architecture and evaluation of an Unplanned802.11b Mesh Network”. In Proceedings of MobiCom.

[5]. Felegyhazi and Hubaux (2006), “Wireless Operators in a Shared Spectrum”. In Proceeding of InfoCom.

[6]. Ica www.epfl publications Website (2005), “Over view of WMNs Technology”, http://lcawww.epfl.ch/Publications/BenSalem/BenSalemH05b.pdf

[7]. Mitola III (2000), “Software Radio Architecture: Object-Oriented Approaches to Wireless System Engineering”, Wiley Inter-Science, New York.

[8]. Kodialam and Nandagopal (2005), “Characterizing the Capacity Region in Multi-Radio Multi-Channel Wireless Mesh Networks”. In Proceedings of MobiCom.

[9]. Poor (2004), “Wireless mesh links everyday devices, Electronic Engineering” Times.

[10]. Aguayo, Bicket, Couto and Morris, (2003), “A High-Throughput Path Metric for Multi-Hop Wireless Routing”,. In ACM Mobicom.

[11]. Locustworld.com website (May 2009): http://www.locustworld.com

[12]. RAPPAPORT (S.), RAPPAPORT (T.), Wireless Communications: Principles and Practice, 2nd Edition. Prentice Hall, 2001.

[13]. SEIDEL (S.Y.), RAPPAPORT (T.S.), Jain (S.), Lord (M.L.), Singh (R.), Path Loss, Scattering and Multipath Delay Statistics in Four European Cities for Digital Cellular and Microcellular Radiotelephone, IEEE Transactions on Vehicular Technology, 40, no. 4, pp. 721-730, November 1991.

[14]. SARKAR (T.K.), ZHONG (J.). KYUNGJUNG (K.), MEDOURI (A.), SALAZARPALMA

[15]. (M.), A Survey of Various Propagation Models for Mobile Communication, IEEE Antennas and Propagation Magazine, 45, no. 3, pp. 51- 82, June 2003.

[16]. IP ADDRESSING AND SUBNETTING workbook version 1.1

[17]. Adaptive contention window scheme for WANs. An International Arab Journal of Information Technology, Vol.4 , No.4, 2007

[18]. On the Effects of contension window sizes in IEEE, 802.11b Networks, IP Addressing and Subnetting for New Users