Detection of Rogue AP's in Wi-Max Networks with the use of a new Algorithm based on the 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:** This research is an event based simulation which is called monte-carlo simulation. This simulation 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. .

Methods/Statistical Analysis:

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.

Applications/Improvements: Finally, it is concluded that the Monte-Carlo simulation is very useful for detecting the location of malicious node in a network. In the first step of the research work the simulation is being performed to detect the presence of a malicious node in a network of ten nodes where the nodes trying to get access by satisfying the threshold value of content window. So, the node which will exceed the number of times trying to satisfy the threshold value of content window can be detected easily. In future the number of nodes can be increased and more measures can be taken on the basis of traffic for every node.

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 behaviour in the network.

II. PROBLEM STATEMENT

This research is an event based simulation which is called monte-carlo simulation. This simulation 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.

III. 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 wimdow 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.

```
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
```

According to the model the algorithm verifies and validates the two primary parameter i.e.:-

- Channel access parameters
- Key credentials

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.

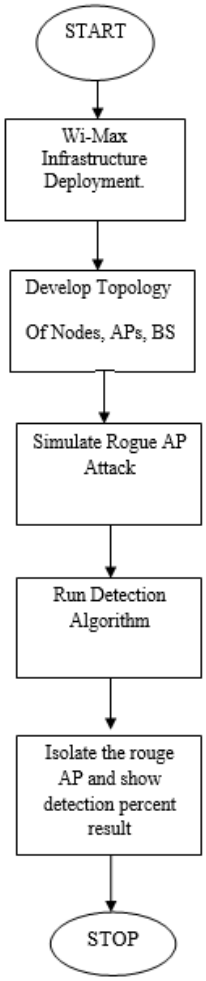
IV. LITERATURE SURVEY

1. 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 behaviour in the scan log and a detection is assumed.
2. 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 unauthorised 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.
3. 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 defence 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.
4. 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.
5. Detection of Rouge Base Station Using MATLAB. This paper considers the problem of detectingrogue base station in WiMAX/802.16 networks. A roguebase 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 nother BS. A new algorithm for detecting a rogue base station is described in this paper.

6. 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. METHODOLOGY



VI. 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. Locustworld.com website (May 2009): http://www.locustworld.com

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

[12]. 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.

[13]. SARKAR (T.K.), ZHONG (J.). KYUNGJUNG (K.), MEDOURI (A.), SALAZARPALMA (M.), A Survey of Various Propagation Models for Mobile Communication, IEEE Antennas and Propagation Magazine, 45, no. 3, pp. 51- 82, June 2003.

[14]. IP ADDRESSING AND SUBNETTING workbook version 1.1

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

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