DETECTION OF ROGUE BASE STATIONS IN WIMAX/IEEE802.16 USING SENSORS

Abstract
This paper considers the problem of detecting rogue base station in Wimax/802.16 networks. IEEE 802.16 is an emerging standard for broadband wireless communications that is receiving a lot of attention. Security support is mandatory for any communication networks. For wireless systems, security support is even more important to protect the users as well as the network provider. Since wireless medium is available to all, the attackers can easily access the network and the network becomes more vulnerable for the user and the network service. 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. In this paper we will give an overview of Wimax and Rogue Base Station Attacks in Wimax. Our proposed algorithm make use of sensitivity parameters as well use of sensors for detecting rogue Base station.

Keywords: - Wimax/IEEE802.16, Rogue base station attacks, Existing Technique for detection, proposed method using Sensors

1. INTRODUCTION
WiMAX is a wireless digital communications system, also known as IEEE 802.16, that is intended for wireless "metropolitan area networks". WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. IEEE 802.16 consists of the access points like base station (BS) and subscriber station (SS). Base Station (BS) is a tower that broadcast signals. Wimax base station can normally covers the area of about 50 kilometers. Subscriber station (SS) is used to provide connectivity. Access to a Wimax base station is similar to accessing a wireless access point (AP) in a Wi-Fi network, but the coverage is more. They are also known as mobile stations which are used as a source of network connection for end user. Backhaul is a backbone and it is used to interconnect several base stations or towers with one another.

Basically there are two modes of operation in 802.16 i.e. P2MP (Point to Multi Point) and Mesh Mode of operation. In P2MP mode of operation a base station can communicate with subscriber station and/or base stations. It composed of a central base station (BS) supporting multiple subscriber stations (SS), providing network access from one location to many. The communication between BS and SS is established based on Req / Grant mechanism. In a mesh topology, every device has a dedicated point to point link to every other device, each station can create its own communication with any other station in the network and is then not restricted to communicate only with the BS. A subscriber station can directly communicate with another subscriber’s station within its communicating range. WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way WiMax is a wireless broadband solution that offers a rich set of features with a lot of flexibility in terms of deployment options and potential service offerings. Some of the more salient features that deserve highlighting are as follows:

- High speed broadband access to mobile internet.
- Mobility support.
Wireless rather than wired access.
• Much easier to extend to rural areas.
• Broad coverage area.
• Very high peak data rates
• Support for TDD and FDD

Security has become a primary concern in order to provide protected communication in Wireless environment. Since WIMAX uses air interface for the transmission medium, both the PHY and MAC layers are readily exposed to security threats. The various classes of wireless attacks are interception, fabrication, modifications, interruption and repudiation. Two main entities in WiMAX are Base Station (BS) and Subscriber Station (SS). A rogue base station attacks can also be conducted due to absence of efficient security mechanism. These types of attacks occur due to absence of mutual authentication mechanism between the Subscriber Stations (SS) and the Base Stations (BS). These types of threats are also known as identity theft threats.

2. ROGUE BASE STATIONS ATTACKS IN WIMAX/IEEE802.16

These are commonly known as identity theft attacks. The rogue BS (base station) makes the SS (subscriber station) believing that they are connected to the legitimate BS, thus it can intercept SSS’ whole information. SS can be compromised by a forged BS which imitates a legitimate BS. They are also known as Masquerade attack in which one system assumes the identity of another.

A rogue BS is a malicious station that impersonates or duplicates 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. The attacker generates his own Authorization Reply Message containing its own self generated AK. Hence attacker can register himself as a BS with victim SS. The attacker has to capture the identity of legitimate BS. Then it builds messages using the stolen identity. The attacker must transmit while achieving a RSS (receive signal strength) higher than the one of the fake base station. [9]

3. EXISTING METHOD

The existing method to detect the rogue base station is a Scanning-interval. The existing technique is based on the received signal strength. A handover can be initiated by a MS when the RSS from the serving BS falls below a certain threshold. A MS can explore the neighbourhood and discover other available BSs.

To conduct that exploration, the MS can make a demand to its serving BS for a time interval during which the MS scans the frequencies and assesses the RSS of available BSs. [9]

• The scanning interval allocation request (MOB-SCNREQ) message is sent by a MS to its serving BS.
• The BS replies with a scanning interval allocation response (MOB-SCN-RSP) message.
• The response contains Ids (i.e. MAC addresses) of recommended BSs. During the allocated scanning interval, the MS may perform association tests with the recommended BSs.
• The MS may conclude by sending a scanning result report (MOBSCAN- REPORT) message to the serving BS.
• The MS reports the RSSs of the recommended BSs.
The report consists of a list of pairs. Each pair consists of a BS ID and a corresponding RSS. This technique uses the RSS parameter mainly to detect the malicious stations.

4. PROPOSED METHOD

Our proposed method basically use the concept of dynamic threshold for calculating sensitivity of base stations (BS) and specific values for calculating the angle, height, distance for ultimately taking a decision for detecting the rogue base stations. By doing so we have developed the technique which works on dynamic threshold and precise values for detecting malicious stations.

The proposed detection algorithm primarily works as scanning algorithm which checks the sensitivity of Base station after every 2ms. This sensitivity is checked for each channel and each frequency of complete spectrum. The value of threshold sensitivity is calculated on the basis of mean value of sensitivity values of last twenty four hours (both high and low). In case of sensors which are calculating readings from various reference points allowable error threshold 0.1% is allowed and if error is more than this, there is some suspicious activity.

5. FLOWCHART FOR PROPOSED METHOD

![Flowchart for Rogue Base Station Detection]

Figure 3. Flowchart for Rogue Base Station Detection
6. COMPARISON BETWEEN EXISTING AND PROPOSED METHOD

The existing technique is based on scanning intervals and our proposed algorithm is based upon sensitivity and sensor readings. The proposed algorithm is more accurate and reliable than the existing algorithm because proposed algorithm is based on sensor readings and will calculate distance, angle and height of each base station for detecting any malicious activity.

<table>
<thead>
<tr>
<th>QoS parameters</th>
<th>Existing technique (based on scanning intervals)</th>
<th>Proposed algorithm (based on sensitivity and sensor readings)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSS</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>Outage</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>Distance b/w Base stations</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>Height of base station</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>Angle of base station</td>
<td>False</td>
<td>True</td>
</tr>
</tbody>
</table>

7. RESULTS

From figure 4 it is apparent in the graph that minimum number of epochs required to reach minimum gradient and minimum possible error based on which neural network classifier can stop learning further, ranges from 6 to maximum of 13 which are quite less in terms of reaching optimal solutions for solving classification problem between normal and abnormal behaviour. This graph is showing readings of seven IDS sessions or scanning reaching for identifying abnormal readings from the sensitivity, angle, distance, height measuring devices.

Figure 5. Time taken in classification per IDS Sessions

The graph shown in figure 5 shows time taken in classification in seven sessions of IDS.

![Time taken in Classification per IDS Sessions](image)

Figure 6. Performance Vs No of IDS Sessions

MSE measures the average of the squares of the "errors." The error is the amount by which the value implied by the estimator differs
from the quantity to be estimated. Its value must be close to 0 for the neural network classifier to accurately classified normal and abnormal behaviour. It is apparent from graph that most of readings out of 7 are close to 0, except some values which are close to 2.5 and less.

Figure 7. Accuracy Vs No of IDS Sessions

The accuracy is the proportion of true results both positives and negatives. From 7 sessions of IDS, accuracy remains on an average above 90%. As the session increases the accuracy remains in a bracket of above 85%, which is good enough for identifying true positive to verify normal and abnormal behaviour.

8. CONCLUSION

We have developed a framework in which we have tried to identify BS based on intrinsic functioning parameters like sensitivity and extrinsic parameters like height, angle, distance from reference points. In this process we also developed a basic scanning algorithm using neural network to identify suspicious/malicious BS. These scenarios may change however as there is evolving community of people who wants to exploit vulnerabilities of various wireless network. Therefore in future we suggest other scenarios must be explored to identify security framework which acts as defence or detection mechanism. These detection mechanisms can be might use usage of clustering, regression or other classifying methods to identify fake BS.

REFERENCES

[2] “A Simple Key Management Scheme Based on WiMAX” Lang Wei-min, Department of Information Warfare PLA Institute of Communication Command Wuhan, China E-mail: wemlang@sina.com, Wu Run-sheng, Wang jian-qi, Institute of Physics and Communication & Electronics Jiangxi Normal University Nanchang, China E-mail: wurunsheng1980@163.com 2008 IEEE
[3] “Research on the Authentication Scheme of WiMAX” LANG Wei-min, ZHONG Jing-li, LI Jian-Jun, Department of Information Warfare, PLA Institute of Communication Command, Wuhan, China E-mail: wemlang@sina.com, QI Xiang-yu, Armored Force Engineering Institute, Beijing, China E-mail: wemlang76@tom.com 2008 IEEE
[9] “Rogue-Base Station Detection in WiMax/802.16 Wireless Access Networks” La détection de fausses stations de base dans les réseaux d’accès sans fil WiMax/802.16 Michel Barbeau School of Computer Science, Carleton University, 1125 Colonel By Drive, Ottawa, ON, Canada K1S 5B6 Jean-Marc Robert Alcatel, CTO Security Research and Competence Center, 600 March Rd., Ottawa, 2006.
[10] “Rogue AP Detection in the Wireless LAN for Large Scale Deployment” Sang-Eon Kim, Byung-Soo Chang, Sang Hong Lee KT 17 Wooyeon-dong, Seocho-gu, Seoul 137-792, Korea and Daeg Young Kim Department of InfoComm Engineering.2006
X. Sen, M. Matthews, H. Chan-Tser, Department of Computer Science and

[18] “Overview of IEEE 802.16 Security,” D. Johnston, J. Walker, Published by

X. Sen, M. Matthews, H. Chan-Tser, Department of Computer Science and


Panos LekkasMcGraw-Hill 2002

[22] www.wimaxforum.org/resources/featured-research

[23] www.wimax.com