Detection of Rogue Base Station using MATLAB

Ramanpreet Singh, Sukhwinder Singh

Abstract- 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.

Keywords: MATLAB, Received Signal Strength (RSS), Rogue Base Station detection and Sensitivity.

I. INTRODUCTION

Worldwide Interoperability for Microwave Access (WiMAX) is going to be an emerging wireless technology for future. With increasing popularity of Broadband internet wireless networking market is thriving. Wireless network is not fully secured due to rapid inventions of new technologies, market competition and lack of physical infrastructure. In the IEEE 802.11 technology, security was added later. In IEEE 802.16, security is considered as main issue while designing protocol. In meanwhile security mechanism of IEEE 802.16 (WiMAX) still remains a question. WiMAX is relatively a new technology; not deployed widely to justify evidence of attacks, threats and vulnerability in real situations [1].

The proliferation of wireless cellular networks with different access technologies made their security a more sensitive problem to encounter.

Various types of Man in the Middle (MiM) attacks such as rogue base station can be conducted due to absence of efficient security mechanism. An intruder could create a false base station and induce legitimate mobile users to connect to it. The objective is to access to sensitive information and create a Denial of Service (DoS) making the mobile users unreachable or the network resources unavailable to them. These types of attacks happen due to absence of mutual authentication mechanism between the Subscriber Stations (SS) and the Base Stations (BS).

Manuscript Received November 25, 2011.

Ramanpreet Singh Student, Department of Computer Science and Engineering, Yadavindra College of Engineering, Punjabi University, Patiala Guru Kashi Campus, Talwandi Sabo, Bathinda (Punjab), India. Mobile No. 9888535317, (E-mail: raman_rpr@yahoo.co.in)

Sukhwinder Singh Asst. Professor, Department of Computer Science and Engineering, Yadavindra College of Engineering, Punjabi University, Patiala Guru Kashi Campus, Talwandi Sabo, Bathinda (Punjab),India. Mobile No. 9501116441, (E-mail: sukhwinder.sran@gmail.com)

II. ATTACKS IN WiMAX

There are many types of attacks in WiMAX such as Rouge Base Station Attacks, DoS (Denial of Service), Data Link Layer, Application Layer, Physical Layer, Privacy Sub Layer, Mutual Authentication, Key Management, Threat of Identify Theft, Water Torture, Black Hat Threat. But the area of concern in this research is restricted to Rogue base station attacks only.

A. Rogue Base Station Attacks

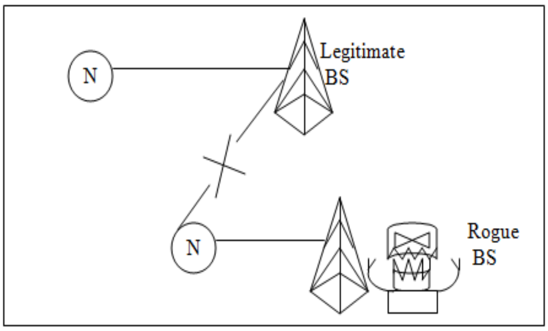

Fig 1: Working of Rogue Base Station Attacks

A rogue BS is a BS imitating to be a legitimate BS. The rogue BS tries to confuse the communicating MS's by posing as legitimate BS. The lack of mutual authentication between the SS and BS is the main reason behind this kind of attack. The SS authenticates itself through its certificate but the rouge BS intervenes & forces it to authenticate it and tries to initiate a session by transferring an AK (Authorization Key). These kind of attack also known as a forgery attack. Attacker generates his own Authorization Reply Message containing its own self-generated AK. And hence the attacker can register himself as a BS with the victim SS. There is a provision of mutual authentication in user networks in IEEE 802.16. It is based on the EAP. This attack arises due to lack of mutual authentication between BS and MS [2].

III. RELATED WORK

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 neighborhood 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. [3].

The scanning interval allocation request (MOB-SCN-REQ) 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 (MOB-SCAN-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.

IV. PROPOSED ALGORITHM FOR DETECTION

The proposed technique is based on the sensitivity of the base station. In this method we consider sensitivity, signal to noise ratio and path loss to detect malicious base station. A key specification for any radio is the receiver sensitivity. Receiver sensitivity for a WiMAX device is a measurement of how faint the radio signal is from the base station. The WiMAX Forum specifies the receiver sensitivity requirements for each certification profile at each of the varying modulation schemes. The WiMAX devices should be able to deliver as much as 5 dB higher receiver sensitivity than the WiMAX Forum requirements. The higher receive sensitivity offers the larger coverage radius for a cell site and greater tolerance for deep indoor penetration [4]. Signal-to-noise ratio is defined as the power ratio between a signal (meaningful information) and the background noise (unwanted signal).

$$SNR = \frac{P\ signal}{P\ noise}$$

Where p is average power. Both signal and noise power must be measured at the same and equivalent points in a system, and within the same system bandwidth.

This Sensitivity Algorithm is based on scanning interval of 2msc, running in each service area/cluster for the purpose of detecting rogue base station. Since each base station has infrastructure/access point having a statistics MAC address. It is easy for any attacker to exploit this fact. Therefore our algorithm basically scans all frequencies of all the channels of the base station for detecting rogue base station. It also calculates certain statistics which are helpful in detecting the malicious base stations. These significant statistics counter include outage counter, which keeps track of failure of base station infrastructure at any point of time. It also keeps sensitivity counter which takes care of the sensitivity of the base station. Our sensitivity algorithm keeps calculating the receiving power as well as the path loss encountered by the packets at regular interval based on optimal sampling frequency.

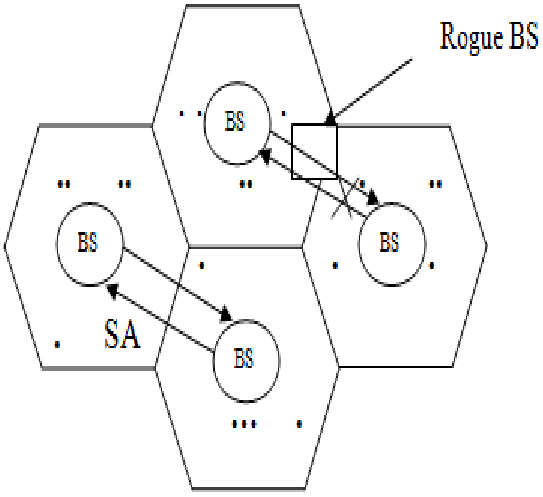

Fig 2: Deployment of Signals in WiMAX Network

It calculates unusual noise, interface or some abnormal signal around base station in every scan section with the help of SNR ratio. It keeps record of the sample packets checksum to ensure that the source and destination are legitimate.

V. FLOW CHART FOR DETECTING THE ROGUE BASE STATION

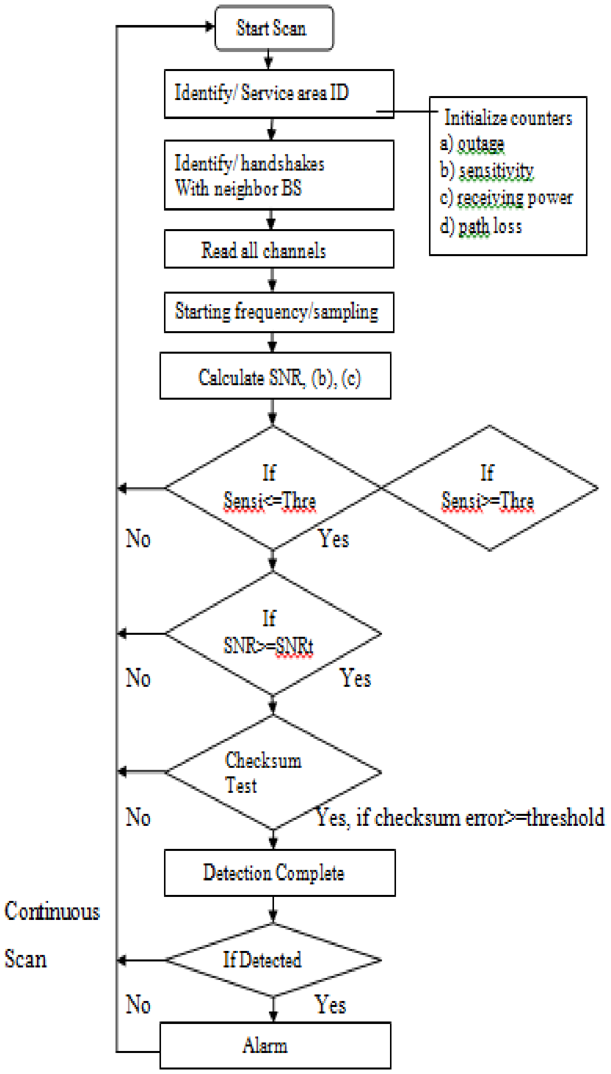

Fig 3: Flow chart for detecting the rogue base station

VI. COMPARISON BETWEEN EXISTING TECHNIQUE AND PROPOSED TECHNIQUE

Our proposed algorithm is more accurate, more reliable and more robust then the existing algorithm because proposed algorithm checks the inconsistencies in RSS and Sensitivity.

Table 1. Comparison between existing technique and proposed technique

Sr no.	**QoS Parameters**	**T1 Scanning interval (Existing Technique)**	**T2 Sensitivity based (Proposed Technique)**
1	RSS	True	True
2	Sensitivity	False	True
3	Path Loss	True	True
4	Outage	False	True

VII. CONCLUSION

It is only the low sensitivity or low receiving power of base station when the attacker might get an opportunity to legitimize its malicious/rogue to the base station. To detect such situations we have presented the detection mechanism in real time which offers alarm system with realistic assumptions and scenarios. It is the same opportunity scanning base on which it offers reliability and robustness to our algorithm. Since it also exploits scanning samples of time slot based on low receiving signal strength and minimal or zero or out aged sensitivity of stations.

FUTURE WORK

Our algorithm is taking sensitivity and RSS as the main parameters for detecting the rogue base station. This algorithm is very successful and accurate in detecting rogue base station. However these days faking & hacking are dynamic subjects and the scenario of such malicious rogue base station may appear again in overcoming our current scenarios and current algorithm. It will require constant updation in changing hacking scenario.

REFERENCES

1. Jamshed Hasan, "Security Issues of IEEE 802.16 (WiMAX)" Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, Page(s): 1-10, 2006.
2. Syed Shabih Hasan and Mohammed Abdul Qadeer "Security Concerns in WiMAX", IEEE First Asian Himalayas International Conference, Page(s): 1-5, November 2009.
3. Michel Barbeau and Jean-Marc Robert, "Rogue-Base Station Detection in WiMax/802.16 Wireless Access Networks", Page(s): 1-14.
4. "Optimizing Your WiMAX Device Investment" WHITE PAPER: WiMAX CPE, Page(s): 1-11.
5. Sang-Eon Kim, Byung-Soo Chang, Sang Hong Lee and Dae Young Kim, "Rogue AP Detection in the Wireless LAN for Large Scale Deployment", SYSTEMICS, CYBERNETICS AND INFORMATICS VOLUME 4 - No 5, Page(s): 78-85.
6. Alaaedine CHOUCHANE, Slim REKHIS, and Noureddine BOUDRIGA "Defending against Rogue Base Station Attacks Using Wavelet Based Fingerprinting", IEEE/ACS International Conference, Page(s): 523-530, May 2009.
7. Ekram Hossain, "IEEE802.16/WiMAX-Based Broadband Wireless Networks: Protocol Engineering, Applications, and Services", IEEE Fifth Annual Conference on Communication Networks and Services Research, Page(s): 1-2, 2007.
8. Sanjeev Dhawan, "Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX" 2007, IEEE 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Page(s): 1-9.
9. Lang Wei-min, Wu Run-sheng and Wang jian qiu, "A Simple Key Management Scheme Bsaed on WiMAX", IEEE Computer Science and Computational Technology, ISCSCT '08. International Symposium, Page(s): 3-6, Dec. 2008.
10. LANG Wei-min, ZHONG Jing-li and LI Jian-Jun, "Research on the Authentication Scheme of WiMAX", IEEE Wireless Communications, Networking and Mobile Computing, WiCOM '08. 4th International Conference, Page(s): 1-4, 2008.
11. Jim Martin, Bo Li, Will Pressly and James Westall, "WiMAX Performance at 4.9 GHz", IEEE Aerospace Conference, Page(s): 1-8, March 2010.
12. Mussa Bshara and Leo Van Biesen, "Available Measurement in Current WiMAX Networks and Positing Opportunities", Page(s): 580-585, Sep. 2009.

13. Pal Gronsund, Ole Grondalen, Tor Breivik and Paal Engelstad, “Fixed WiMAX Field Trial Measurements and the Derivation of a Path Loss Model”, Page(s): 1-6.
14. Mussa Bshara and Leo Van Biesen, “Localization in WiMAX Networks Depending on The Available RSS-based Measurements”, International Journal on Advances in Systems and Measurements, volume 2 no 2&3, Page(s): 214-223, 2009.
15. www.intel.com/technology/wimax/
16. www.wimaxforum.org/resources/featured-research
17. www.wimax industry.com/wimaxwhitepapers.htm
18. http://4g-wirelessevolution.tmcnet.com

AUTHORS PROFILE

Ramanpreet Singh, M.Tech Student, Department of Computer Science and Engineering, YCoE, Talwandi Sabo, (Punjabi University, Patiala) India.

Sukhwinder Singh, Asst.Professor, Department of Computer Science and Engineering, YCoE, Talwandi Sabo, (Punjabi University, Patiala) India.