Volume 4, Issue 6
December 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

©2012-16 International Journal of Information Technology and Electrical Engineering

Study on Base Station Authentication Techniques in Wi-Max

Omair Gull
Department of Computing, SZABIST Islamabad, Pakistan
Omair_gull@hotmail.com
Ahtasham Sajid
Department of Computing, SAZBIST Islamabad, Pakistan
gullje2008@hotmail.com
Sumaira Zulfiqar
Department of Computer Sciences, IIUI, Pakistan
Sumaira.zulfiqar@yahoo.com

Abstract:

Wireless communication always has a greater edge from the wired network, because of its diversified nature and services. Wireless MAN allows organizations to move one step forward from Wi-fi and deploy the Wi-MAX to cover the large distances by using their own private network. Certain security mechanisms are required to ensure data availability, integrity, confidentiality, and verification of the participants in communication process. All those threats which are commenced in previous communication techniques are also applied in Wi-Max technology and some new loop holes are also identified. This research focuses on the threats and security issues of Base stations and then mentions some authentication and authorization techniques for the Base Station.

Key Words:

Watermarking, Discrete wavelet transform, Arnold transform, Peak signal to noise ration.

I. INTRODUCTION

To cover up the "last mile" issue IEEE come up with the new solution called 802.16 in 2001. It brings the positive change in wireless communication and resolves the problems of 802.11. Wi-MAX provides its services to remote areas where wired connection is not possible to approach. It supports huge data transfer rate of 70 Mbps for both data and telecommunication services. Wi-MAX provides easy installation and deployment of Wi-max device in any area which can be calculated according to other installed stations, and from that point any Wi-MAX receiver like mobile device or any fixed internet router may connect with that station. [4]

Wi-max works at different frequencies which make it more flexible and easy to adopt. In the earlier development of Wi-max non line of sight (NLOS) transmission is not supported by the standard. Initially it supports the spectrum of 10-66 GHZ which mainly prefer point-to-multipoint and broadband wireless access. The other developments were little modified and enhanced like 802.16a so they also coordinate with NLOS service, multiple radio modulation, licensed and unlicensed band implementation, and TDM and packet services. The third generation of Wi-MAX facilitates the Mobile users to get connected and avail services from their ISP's no matter where they are.

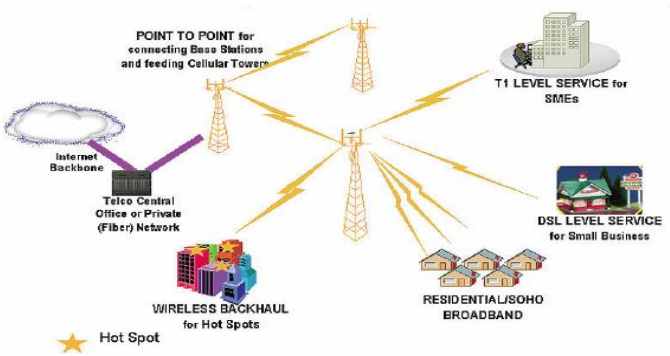

Fig 1: Wi-MAX Architecture and Services available for different areas [4]

Volume 4, Issue 6
December 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

©2012-16 International Journal of Information Technology and Electrical Engineering

The figure 01 mention different categories of users like SOHO, wireless backhaul, SME's, and private organizations who own their personal network. All of them are connected through Wi-MAX base stations and transmitting their data to various destinations, these stations may be connected with internet for worldwide connectivity.

In such versatile network where system allows everyone to become a part of network and exchange data, such place become open to threats and security of parties and data is a question, so many attacks are identified related to Wi-MAX environment such as rouge base station attack, man in the middle attack, replay attack, eves dropping, water torture attack, jamming or blocking, and DOS attack. Some attacks are specifically designed for Physical layer because all the security techniques are operated in MAC layer and they don't have designed any solution to protect PHY layer where as some attacks are also there to disturb the functions of MAC layer.

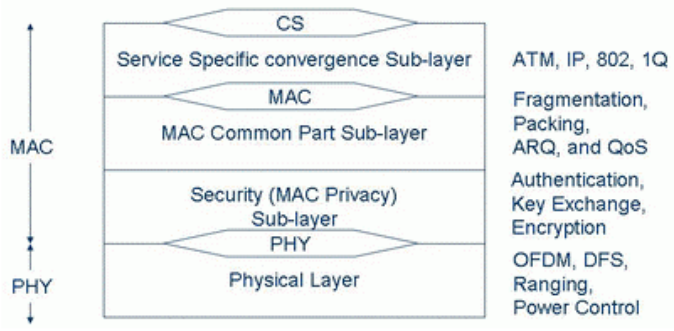

Fig 2: Wi-MAX Layer Architecture [8]

As shown in figure 2 Wi-MAX architecture consists of 4 basic layers, which are considered as two basic layers (MAC and PHY) according to OSI model definition. The Mac layer is further distributed in to three layers which are junction Sub-Layer, regular Part Sub-Layer, and protected Sub-Layer. The initial categorized layer is responsible for the segregation of data and forwarding it to the next sub-layer, it also manages the bandwidth allocation and Quality of Service (QoS). The next one which is Common part sub-layer sends the bandwidth and authentication request, it supports connection oriented services. The last sub-layer which relates with the security of the data may include two component protocols such as encapsulation and key management protocol. The physical layer in the model is used to forward the stream towards the destination which it receives from the MAC layer. [9]

To secure the connection and traffic between the SS and BS Wi-MAX provides the solution that is PKM.PKM protocol consists of certain phases to authenticate and authorize both parties and generate further keys so that whole communication can be secured. The old encryption technique DES was used in PKM that's why it become weak and easy to break, a new version PKMv2 is introduced which enhances the security features of Wi-MAX transmission because it uses RSA instead of DES, and EAP authentication is used for authentication of SS and BS. [13]

II. BACKGROUND STUDY

Security is always a major concern is all type of communication, it doesn't matter what type of data is being transmitted and what channels are used, how many far the destination is, what protocols are used and what are the communication devices which are participating in the process the only thing to be manage is the secure transmission of data towards destination. Many researchers have been done in this aspect that how parties secure their data from intruders and unauthorized access and modification.

The purpose of this is study is to find out the previous work done the security techniques in Wi-MAX communication process. In Wi-MAX network two major parties are involved which are the SS(Subscriber station) the machine who wish to transmit the data and the BS (Base Station) who provides the services to the SS. The SS could be at any fixed location like PC or it can be any Mobile station (MS). In case of Mobile station several other issues can be raised but they are out of scope from our discussion. It is necessary to identify the SS/MS before starting communication. Our basic purpose is to identify and explore those researches which are used to identify the Base Station because there is a new way to hack the SS and easily access their data. SS don't know much about the BS so that makes it easy for hackers to hack SS and misuse them.

Security was examined in numerous papers, where a great deal of security vulnerabilities is illustrated when the distribution of the versatile Wi-MAX change, the majority of these vulnerabilities were unraveled. The security of Wi-MAX

©2012-16 International Journal of Information Technology and Electrical Engineering

was examined by a couple of papers, some inspected in the 3-way TEK trade and the sanction process and it couldn't uncover any security spill. Additionally dissected the key administration convention. It breaks down programming. This is additionally talked about that the interoperation with different conventions could be a security issue, if these conventions have more level security qualities. Information security is extremely imperative in the Wi-MAX system. The point when exchanging information starting with one place then onto the next spot. In which, the plan's disappointment to secure against falsifications or answers, the most genuine dangers against any remote information security conspire. Encryption just read ensures the WMAN path it doesn't safe the channel from composes, still somebody who doesn't have the encryption technique. [6]

Not many conventions likewise show an extreme lapse in its utilization of cryptographic method. IEEE 802.16 utilization DES by implementing the CBC mode. Its usage require an irregular introduction vector to secure the design. However IEEE 802.16 utilization a foreseeable introduction vector. Redressing this matter compensates producing every for every casing introduction vector arbitrarily and embeddings them into the payload. Despite the fact that this builds the cryptographic transparency, no other elective exists.

As of late it has been identified that private keys follow the different method of creation, too. It is dependent upon synchronization of system by shared studying. The key is produced by the progress of an intricate physical methodology, specifically the rivalry between stochastic engaging and horrendous strengths which follow up on the weights of the two dynamical frameworks which synchronize by shared indicators have preference on any party who is responsible for synchronize the communication process.

2.1 Rouge Base Station Recognition by Using Sensors

Fundamentally the author mention two types of processes in the Wi-MAX standard which are one connection to many connections and the other is engaged connection. (Deepti, 2012)In the first type a service provider can correspond with other service provider or with any subscriber who request for any service. It made out of a focal Service provider supporting numerous receivers, furnishing system access from one area to a lot of people. The correspondence between both parties is made dependent upon the request and grant instrument. In such lattice layout, each gadget is devoted and connected with each other mechanism, every node can make its own particular correspondence with any viable point in the system and they are not bound to speak just with only the connected Service provider. A consumer/client can specifically correspond by way of any alternate client station inside specified imparting extend. Wi-MAX is one of the most blazing broadband remote advances around today. Wi-MAX frameworks are relied upon to convey broadband access administrations to private and venture clients in a temperate way Wi-MAX is a remote broadband result that offers a prosperous place of uniqueness through a great deal of adaptability as far as sending choices and potential administration advertising. [1]

The proposed identification calculation principally functions as filtering calculation which checks the affectability of Service provider after each 2ms. This affectability is checked for every channel and every recurrence of complete range. The quality of limit affectability is computed on the support of mean esteem of affectability values of last twenty four hours (both high and low). If there should arise an occurrence of sensors which are computing readings from different reference focuses reasonable blunder limit 0.1% is permitted and if lapse is more than this, there is a few suspicious action.

2.2 Mutual Authentication between Base and Subscriber Station

In IEEE 802.16 system, a SS must be verified and confirmed by the BS to get the system accreditations and to be a part of the system as a honest to goodness hub (Mohammad Hossain, 2011). At the same time, there is no such confirmation or verification system by which a SS can check and confirm a BS before it begins to give all its accreditations to the obscure BS. The simple thing is that a BS can additionally pass through some check method by which the SS

©2012-16 International Journal of Information Technology and Electrical Engineering

will comprehend that it is speaking with a true blue BS and not with the maverick one. In this way, common validation is must to build a both side secure and reliable transmission. It is somewhat a smart thinking to chip away at the process other than running behind the gatecrashers. Distinctive assaults are talked over so far which are identified pretty much just since the service provider verification is not display in the existing verification convention. The point when the maverick BS acquired all the certifications from the Ss being an authentic BS, it can put the SS out of the system by rehashing the gained messages from SS to the authentic BS once more what's more once more. The point when the preparatory message over and again comes, the BS quits accepting any more messages from the source thinking of it as a cheat or aggravating component. Along these lines, the existing convention must be restored to guarantee secure and dependable correspondence particularly in keeping money, government exercises or other critical segments just to uphold high security from the interlopers also programmers. [2]

During the transmission process, a Client launches the session. It transmits its recognizable pieces of proof, capacities and different prerequisites to the BS. In the wake of checking the reports the reply has been sent back to the client by the service provider. This reply can be generated by rebel Service provider so it can be verified by using some method. The client which is participating the process have no way to verify the service provide so they go to the unbiased company for its verification. To verify the service provide client sends the detail of service provider to that verification party who verify the service provider as an original one and feasible to communicate with. That verification party also verifies the client because client can be any hacker who can launch any attack on service provider so they also send the data of client to verification party. After the completion of such process both parties are known to each other and may start their communication.

2.3 Proxy Service provider based Authentication

If any station start sending any vague messages toward BS and Base Station put all of its effort to reply to those message and didn't reply to any other genuine so we can notify it as successful DOS attack on that BS, there could be a certain solution to that DOS situation arises on the BS, so they can not the provide their services to any of the client any more until you resolve that issue. The author seems keen in finding out the solution of such problem and identifies an new authority which is denoted as proxy station. By the use of proxy station in the communication all the initial process are transmitted through the proxy station who collects the basic data from the client and then passes it to BS where it verifies the certificate of the client machine, if client get cleared from that process then they allow to share the key with the BS and continue the communication.[16]

In the first message client requests the verification towards the PS which holds the certification of client's machine X.509 authentication certificate is being used. The authentication documentation contains details like form, serial number, the authentication guarantor, legitimacy period, open key of client, actually the PS which is an intermediate which approving the whole demand, all that basic process is handled by the PS so it cut off the additional effort of the base station. In the next message which is followed by message 1 the client sends the special unique value generated by its own system which called a Time stamp value the purpose of this value is to identify the time of the message because hacker can reuse the message at any stage. The other unique value is the Nonce which is also known to the client and he generates it for the verification. Client also send security certificate and its identification number and then it signs the whole message which help to avoid non-repudiation of the message and also helps in controlling the down grade attack.

2.4 Mutual Authentication Protocols for Mobile Wi-MAX Networks against Rogue Base Stations

Maverick BS or RS ambush is a standout amongst the most widely recognized ambushes on remote validation conventions. In such a strike, a pernicious hub mimics a true

©2012-16 International Journal of Information Technology and Electrical Engineering

blue BS or RS hub with fake qualifications and tries to persuade a joining RS or MS to associate with it. On the other hand, an assailant may attempt to bargain a genuine BS or RS to get control over it. IEEE 802.16j utilization PKMV2 to counter conceivable maverick BS ambush by utilizing shared confirmation. On the other hand, there is a certain presumption in PKMV2 that BS is dependably dependable, subsequently PKMV2 does not furnish any insurance measure to discover and counter the ambush from a bargained BS. Also, the circulated security mode in MMR Wi-MAX systems additionally makes rebel RS strike more conceivable.[1]

This is since the validation technique between RS hubs is most certainly not performed by a concentrated server, yet is dependent upon the trust between hubs. In the event that one hub is traded off, its trust with different hubs is likewise traded off. We have presented the identified finish up security issues in MMR Wi-max systems and have indicated that present principles are not sufficient for tending to the maverick BS and maverick RS ambushes. In this area, we introduce two new secure conventions to give powerful validation in MMR Wi-MAX systems. Particularly, our conventions can protect against maverick BS and RS ambush by utilizing a trusted validation server to give double confirmation and security zone key.

2.5 Security Scheme in WMAN Based

In this paper the author identifies the security issues which can be occurred during initial phases of when the parties have to verify themselves as a legitimate device. They focus the point to multi point network architecture. By using that specific architecture any client may join the communication network who may identify itself and exchange the basic information. Such process is accomplished in two parts first part is related with the verification of both parties to each other, the other part identifies those privacy methods in which they to proceed the further communication. That research identifies so many flaws in that real design of that way of communication and mention some of its own generated solution which they later also execute on the artificial environment and shows the much better results.[14]

The working process of existing system is quite simple that all rights holds by the service provider which firstly verifies the client by getting their basic confidential data and then they have to decide the further communication process like how they secure their data and what are the keys to use for coding and decoding of data, if any client wish to communicate with any other client that is not possible directly they have to use service provider as an intermediary. In this paper author just identifies the threats to the media access layer of the parties.

The first problem with such verification process is that the service provider is not verified by any client so any one can be claim to be the service provider and easily occupy any client. The other issue is that the message which is initially transmitted between the parties are not recognized by any unique values so they are open threats because they can be used further in any communication. The communication process relies on the basic key which is sent by the service provider but that key did not contain any standard to be verified during connection establishment. The next issue relates with the second part where the parties identifies the privacy issue of their traffic, that secure key didn't assure it's reality and time when it is generated and the size of that key is also an issue. The last problem is the standard used for encoding and decoding of data, that standard is already proved an open to attack and can be easily hacked by using simple software. [14]

Now for the solution of such problems author follows the standard of IEEE802.16 which is WKMI architecture, this technique follow the certificate which is available to both parties and allow them to identify themselves to each other before start the communication. After that the next phase is also supported by this technique which is key sharing. This solution of WKMI works in three phases. In the first phase they verify the parties by using any third party. The next step is to verify the service provider by getting their personal data, and in the last step the client negotiates on the further key sharing and starts its communication with the authorized Service provider.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

©2012-16 International Journal of Information Technology and Electrical Engineering

2.6 Wavelet Based Fingerprinting

In this work the authors concentrated on relieving vulnerabilities of cell systems to artificial service provider strike. The author suggested narrative method for describing sign finger impression dependent upon discrete wavelet transformer. Each radio wire transmits the same arrangement of bits under which the indicator unique finger impression will be registered at the recipient part new methodology requires such dynamic solution. The result is incorporated to CODERA(Cooperative Location and Reaction Architecture) building design in request to propose an answer for MIM ambush identification in remote cell systems. Our effects with respect to the effectiveness of the processed unique finger impression indicated that (an a minor geometric change on the sign because of distinction in receiving wires, does not present adjustment on the unique mark; and b) a little change on the sign due to commotion in proliferation channel presents a change on the unique mark that could be endured utilizing a discovery edge.[15]

To verify that fingerprint process the author suggested some basic rules. The signals which are collected from different service providers but they exist in the same order their finger prints have to be different from each other. Next we have to find out the difference between those fingerprints and the uniqueness behavior they contain and that value must be void if any fake party tries to use them. If any interruption occurred during the communication process it would not affect the value of the fingerprint.

The basic goal of this technique is to identify the specific attack communication which any service provider may send author uses following notation $f\ a, \epsilon, p(t)$ to identify such communication. By applying such formula we can identify the location of fake station. By using an demonstrated application software the researcher put an artificially created signal in to that application to check the response according to the above mentioned formula. The result is the variation has been caught which is occurred in the different fingerprints. Modifications are mentioned in the paper.

2.7 Detection of Rogue Base Station Using MATLAB

A fake BS is a BS which represents itself as emulating to be an honest and real service provider BS. The maverick BS tries to confound the conveying MS (Mobile Station) by acting like genuine BS. The absence of shared verification between the SS and BS is the primary explanation for this sort of ambush. The Ss verifies itself through its testament yet the rouge Bs mediates & compels it to confirm it and tries to start a session by exchanging an AK (Authorization Key). These sort of assault otherwise called a phony ambush. Aggressor or hacker creates their own Sanction Reply Message holding their interrelated particular personally established AK to start the fake communication process. Also consequently the aggressor can enlist himself as a BS with the exploited person SS. There is a procurement of shared verification in client organizes in IEEE 802.16. It is in view of the EAP. This assault emerges because of absence of common verification between BS and MS/SS. [10]

This Sensitivity Algorithm is dependent upon filtering interim of 2MSC, running in every administration area/cluster for the motivation behind recognizing maverick service provider. Since every service provider has infrastructure/access focus having a detail MAC address. It is simple for any ambusher to endeavor this reality. Accordingly our calculation essentially examines all frequencies of every last one of channels of the service provider for identifying maverick service provider. It additionally computes certain detail which are accommodating in recognizing the noxious service providers.

2.8 Authentication with Neural Cryptography

Like all the papers we have seen in that study the similar problem is identified by the author that there is no fair mechanism is available for the authentication and verification of the service provider, which provide an open platform to attacker to become a service provider an easily hack any system and access their data. The other issue could be the arise of replay attack which is also caused by the poor setup. So the

©2012-16 International Journal of Information Technology and Electrical Engineering

main focus of the author is to identify the service station by using mutual authentication process, but they mention a new way for mutual authentication that is the use of neural cryptography approach.

Counterfeit is a process in which the client didn't know that his system is communicating with the fake service provider or with the real one to authenticate the service provider possible method could be the generation of challenge message by the client for the service station to verifies itself for the client before initialize the communication. When IEEE announces and major modification in Wi-MAX which is an usage of mobile wireless there are certain other issues which came to know, like its is not easy for the parties to differentiate the parts of protocol from one another which creates another loop hole in the system. The key which is used for the verification of the communication have no standard to be followed, the size of the key is also not mentioned in any rules, so if the authorization is key can be reused in any random communication process it can be used to hack any other transmission because its uniqueness is not known and guaranteed. So both parties have to contribute for the generation of the key which can be encrypted properly. [10]

As a solution of all those issues mentioned above the author proposed a neural cryptography scheme through which they allow both parties to make every possible exchanges before start the communication. They identified a tree parity machine(TPM), that TPM is basically consist of three parts which are some hidden units, weight vectors and input vectors. The resultant value depends on the dynamic numbers both parties select before starting the process. To initialize the process they exchange their numbers on the open path and according to those values they adjust their other corresponding values.

2.9 Improved Secure Network Authentication Protocol (ISNAP)

In occasion of utilizing a mix of timestamps with nonce, the resynchronization strategies are to be characterized. Also, the overhead ought to be lessened to take into consideration best execution of the validation calculation. The validation technique in PKM v2 is just backed utilizing nonce which is lacking if there should arise an occurrence of smother replay and interleaving strike.

Along these lines a methodology must be resolved keeping in mind the end goal to improve a confirmation display which is strong to the displayed dangers, takes into consideration resynchronization component and presents low overhead Keeping in perspective the aforementioned situations, a model has been created for Wi-MAX (altered or portable), called ISNAP proposed to the issues examined in paper and additionally the improvement of system security over a verification cycle has been underlined. The verification convention is an amplification of the half and half methodology utilizing timestamps within conjunction with nonce. There are four steps of the convention. In step 1, the SS starts the sanction convention by sending the INIT message. It comprises of timestamp (Tss-1), nonce (Nss-1) and Mcerss. Tss-1 enactments as a freshness identifier what's more will anticipate the replay of Init, in this way, sparing the system's preparing assets and anticipating the DOS assault. BS accepts the Init message and computes the outing time as: Tprop-1 = Tpresent – Tss-(1), where Tpresent is the time at which Init is gained. [12]

The proposed model can stand against the ambushes like replay and smother replay, interleaving strike, DOS issue, variety assault, endeavors to fumes the framework's abilities and Man-in-the-Middle attack. The half breed methodology deflects the replay of messages furthermore the resynchronizations deal with the smother replay ambushes. Interleaving strike is likewise held because of the vicinity of timestamps as though the nonce is anticipated; timestamps set the message to lapse. Because of the resynchronization system, the timekeepers are kept whole on all the system substances along these lines fortifying the operation of timestamps and countering replay. The event of endeavors to empty out the framework's transforming assets and along these lines expediting Dos strike is evacuated by the sentinel timestamp set in the Init message. This likewise evacuates the probability of vicinity of any half-opened security affiliations.

III Wi-MAX Security Weaknesses/Potential Solutions

©2012-16 International Journal of Information Technology and Electrical Engineering

Regardless of the possibility that Wi-MAX engineering has complex validation what's more commission techniques and exceptionally solid encryption strategies is still defenseless on diverse assaults or dangers. Being still another innovation, an extraordinary consideration for security changes is needed in IEEE 802.16 standard. We trust that later on they will come to be fewer and resolvable.

Wi-MAX standard has two sorts of testaments, one for SS what's more one for the producer, and not for BS. This comes to be an issue. Subscriber testament recognizes a subscriber by its Mac address. SS testaments are ordinarily made and marked by the producer utilizing open key, this empowers the BS to accept a SS testament along these lines distinguish a certain mechanism as veritable. This kind of weakness is called shared confirmation issue. [14]

Concerning issues, the 224bit ECC (Elliptic Curve Cryptography) offers 2048bit RSA security in place of 160bits ECC which offers 1024bit RSA. In this way, 224bit ECC will carry a speedier computational productivity with the same level of security, memory, and transfer speed and vigor reserve funds. Inside PKM-MSH informing, replay strike are maintained a strategic distance from utilizing irregular numbers. In the event that a message is hacked and the assailants resend the irregular created number in the message it could be located by the collector. In finishing along these lines, the beneficiary overlooks the message in light of the fact that the arbitrary number arrangement doesn't match. In the event that the irregular number is discovered, the assailant still needs to check the signature. The confirmation can't be finished in light of the fact that the assailant cannot give the private key.

IV. Critical Analysis

In this sutyd many variant methods in the previous discussion to ensure and verify the Service provider as well as the Mobile station. Every researcher identifies their own techniques and solutions to avoid the communication with any suspicious or fake Service provider. Now we have to analyze every solution according to the recent threats on the Wi-MAX environment.

There are numerous attacks on the physical and MAC layers like Replay, DOS, Forgeries, Interleaving, Identity Theft, Downgrade Attack, Band width spoofing, Rogue Service provider, Man in the Middle attack, water torture, jamming and Scrambling, Service provider spoofing, and MAC spoofing. As far as our concern we especially focus on the attacks related with the Service provider and the techniques provided to the user or SS to identify its Service provider before starting the communication. [17]

Table 1: The Methods and the Solutions according to the specific Threats

Threats	Solutions	Method
Base Station Spoofing	PKM v1,v2	Sensors, Visual Cryptography
Replay/DOS Attack	Time Stamp, Nonce	ISNAP
Authentication	Mutual Authentication	Neural Cryptography
Rouge Base Station	Discrete Wavelet Transform (DWT)	Wavelet based Fingerprinting
MAC Address Spoofing	Mutual Authentication	DES (Data Encryption Standard)
Man-in-the-Middle Attack	HMAC-Hash	PKM-MSH

The table 01 above mentions the possible threats and the upcoming threats because of Rouge Service provider, not all of the solutions deal with all types of threats because of their versatile behavior and attacks on specific areas, so to deal with every single threat we have specific Solution as we have mentioned in the table

v. Conclusion and Future work

The effort done on this work should focus on the accessibility of Wireless services in a well secured manner. Make sure that the subscribers share their data more freely and rely on the services of Service provider. The Service provider shouldn't be an anonymous entity anymore because we have mentioned so many authentication and authorization techniques. The mutual authentication is quite helpful for making a secure connection that no intruder may intercept between BS and SS. The threats and attacks can be deal more efficiently by deploying some new proposed solutions. The usage of sensor gives a new way to authenticate the Bs, the

©2012-16 International Journal of Information Technology and Electrical Engineering

Neural Cryptography mention the challenge message for the service provider. Time stamp and Nonce which are the old techniques are used with a new combination and proved a good solution. Local policies avoid the Bandwidth spoofing, some solutions like discarding the fake frames and using high signals make Physical Layer more reliable.

VI. REFERENCES

[1]. Deepti, Deepika Khokhar. (August 2012). DETECTION OF ROGUE BASE STATIONS IN WIMAX/IEEE802.16 USING SENSORS. *Int.J.Computer Technology & Applications*. Vol 3 (4) (4), 1577-1582

[2]. Huang, J. and Huang, C. 2011. Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations. pp. 1--5.

[3]. Hossain, M., Parvez, M. and Islam, M. 2011. Mutual authentication between base and subscriber station can improve the security of IEEE 802.16 Wimax network. *International Journal of Engineering (IJE)*, 5 (4), p. 292.

[4]. Jacobs, S. 2011. WiMAX subscriber and mobile station authentication challenges. *Communications Magazine, IEEE*, 49 (11), pp. 166--172.

[5]. Fuden Tshering, Anjali Sardana. (April 2011). A Review of Privacy and Key Management Protocol in IEEE 802.16e. *International Journal of Computer Applications*. Volume 20– (No.2), 25-31.

[6]. Sikkens, B. 2008. Security issues and proposed solutions concerning authentication and authorization for WiMAX (IEEE 802.16e)

[7]. Shahid Hussain, Muhammad Naeem Khan, Muhammad Ibrahim. (July 2012). A Security Architecture for Wimax Networks. *International Journal of Computer Applications*. Volume 50 (No.9), 35-39.

[8]. Singh, R. and Singh, S.. Detection of Rogue Base Station Using MATLAB. *International Journal of Soft Computing and Engineering, ISSN*, pp. 2231--2307.

[9]. Eren, E. 2007. Wimax security architecture-analysis and assessment. pp. 673--677

[10]. Hu, D. and Wang, Y. 2008. Secure Authentication on WiMAX with Neural Cryptography. pp. 366--369.

[11]. Altaf, A., Sirhindi, R. and Ahmed, A. 2008. A novel approach against DoS attacks in WiMAX authentication using visual cryptography. pp. 238--242.

[12]. Hashmi, R., Siddiqui, A., Jabeen, M., Shehzad, K., Zubair, A. and Alimgeer, K. 2009. Improved Secure Network Authentication Protocol (ISNAP) for IEEE 802.16. pp. 101--105.

[13]. Kumar, A., Sharma, P. and Gupta, V.. Review of Security Threat and Solution in WiMAX (802.16 e).

[14]. Yang, F., Zhou, H., Zhang, L. and Feng, J. 2005. An improved security scheme in WMAN based on IEEE standard 802.16. 2 pp. 1191--1194.

[15]. Chouchane, A., Rekhis, S. and Boudriga, N. 2009. Defending against rogue base station attacks using wavelet based fingerprinting. pp. 523--530.

[16]. Tshering, F. and Sardana, A. 2011. A proxy base station based authentication protocol for IEEE 802.16 e. pp. 578--582.