PERFORMANCE ANALYSIS OF WIMAX SECURITY USING OPTIMIZATION ALGORITHMS

Kondragunta Rama Krishnaiah[1] Seelam Koteswara Rao[2], Pavan Kumar Gabbiti[3], M.Varasundar4, A.KarnaRao[5]
[1]Professor, Computer Science Engineering, R K College of Engineering, Vijayawada, India
[2]Professor, ECE, Kallam HaranathaReddy Institute of Technology, Chowdavaram, Guntur
[3]Assistant Professor, Kallam Haranadhareddy Institute of Technology, Chowdavaram, Guntur
[4]Associate professor in ECE, Kasi Reddy Narayana Reddy college of Engineering and Research, Abdullahpur mettu, Hyderabad.
[5]Assistant Professor, Department of Electronics and Communication, DVR and Dr HS MIC college of Technology,Kanchikacherla, NTR District,521180

Abstract :

Finding rogue base stations in WiMAX/802.16 networks is the focus of this paper. An intruder's station that imitates a valid base station is known as a rogue base station. As a group of subscribers attempt to connect to what they think is a real base station, the rogue station throws them for a loop. Disruption to service might result. The attack strategy is specific to the network type. A method for detecting rogue bases and implementing mutual authentication is presented in the cited paper. There are three steps to complete the solution. The sensitivity algorithm in the first section allows it to deliver rouge-based detection. Authentication via the Extensible Authentication protocol—Transport Layer Security is possible in the second stage. In order to overcome DDoS attacks, the third stage involves carrying the SAI algorithm. Authentication of mobile nodes and identification of rouge base stations are both covered in this work. We have improved the DDoS detection to offer a better solution. To guarantee Broadband Wireless Access (BWA), the IEEE 802.16-based wireless radio data transmission system known as WiMAX (Worldwide Interoperability for microwave Access) was developed.

Keywords: WiMAX/802.16, DDoS attacks, BWA

1. INTRODUCTION

Their primary objective is to establish and disseminate standards, with the end result being the issuance of "WiMAX Certified™" certificates to hardware manufactured by different companies. These certifications attest to the product's conformity with the previously approved IEEE 802.16 standard [1]. The Mobile Station (MS), the Access Service Network (ASN), and the Connectivity Service Network (CSN) are the three fundamental components of the WiMAX architecture. On the customer's premises, there is a mobile station (MS), also called customer premises equipment (CPE). An ASN is made up of multiple BSs, or base stations. The IP link to the WiMAX radio equipment is provided via the link Service Network (CSN)[2].

Some of the security flaws and dangers with WiMAX have been fixed. Among these are: • Rougette base stations • DoS attacks • Man-in-the-middle attacks • Manipulation of networks via falsified management frames [3].Issues with 1.1: Unauthenticated messages, management communications that are not encrypted, and shared keys in the multi and broadcast services. Mobile WiMAX enables IETF EAP protocol-based device and user authentication with support for SIM-based, USIM-based, digital certificate, or username/password-based credentials. The EAP protocol supports the corresponding EAP-SIM, EAP-AKA, EAP-TLS, and EAP-MSCHAPv2 authentication methods. Methods that derive keys are the only ones that are supported by EAP [4]. An X.509 certificate encrypting with RSA is utilized for RSA-based authentication. Authentication protocols based on EAP (EAP-AKA, EAP-TLS, EAP-TTLS). EAP-RSA RSA-based authentication is a two-step process.

When the time comes for authentication, the PKM protocol takes care of it. So far, two iterations of the PKM protocol have been introduced. The PKM V1 and PKM V2 pathways. The PKM protocol is

responsible for overseeing the exchange and distribution of keys.among the SS and the BS. X.509 digital certificates and the RSA public-key encryption technique are used for this purpose. Key encryption keys (KEKS), authorization keys (AKs), and traffic encryption keys (TEKs) are all part of the suite of keys (5).HMAC and CMAC digits make it easy to authenticate non-authenticated management messages transmitted to the main or basic management connection. An additional 168 bits are required for this authentication, and its acceptability must be determined. Adding a single number would make most messages many times longer than they already are because of how brief they are. This feature necessitates striking a balance between the protocol's efficacy and security (6). When an attacker copies an action and then replays it, they are committing a replay attack. This can happen even with legitimate packets. The current version on 802.16 allows for this kind of assault. Including a sequence number makes anti-replay a breeze to implement [4].A malicious BS masquerading as a legitimate BS is known as a rogue BS. The malicious BS poses as legitimate BS in an effort to trick the communicating MSs. This form of attack is mostly caused by the fact that the SS and BS do not have mutual authentication. The malicious BS tries to start a session by transferring an AK (Authorization Key), but the legitimate SS stops it and makes it authenticate itself using its certificate. A forgery attack describes this type of assault. The aggressor creates his own AK. The criminal can then pose as a business service provider to the victim's service provider. The IEEE 802.16 standard includes a mechanism for user networks to implement mutual authentication. From the EAP, it is derived. Because BS and MS do not authenticate with each other, this attack can happen [7].

By impersonating other legitimate nodes or making up their own identities, a malevolent node can launch a Sybil attack and assume the identities of numerous clients. One example is when a Sybil node pretends to be a large client by flooding an access point with association request messages using arbitrary MAC addresses. Once an AP's association slots or channel slots are consumed by the Sybil node, access is blocked to legal clients. Sybil attacks, a subset of denial-of-service attacks, pose a significant threat to the reliability of wireless networks and the services they provide. There are three steps to complete the solution. The sensitivity algorithm in the first section allows it to deliver rouge-based detection. Authentication via the Extensible Authentication protocol—Transport Layer Security is possible in the second stage. In order to overcome DDoS attacks, the third stage involves carrying the SAI algorithm.

Section 2 of this paper defines the problem and lays out the solution's methodology. Section 3 explains the algorithm that determines whether a base station is rouge. Figure 2 shows an algorithm with a modular diagram. In section four, we learn about the mutual authentication that takes place via the sensitivity algorithm and the Extensible Authentication protocol—Transport Layer Security. To counter distributed denial of service (DDoS) assaults, Section 5 details the shared authentication information (SAI) algorithm and its modular design[15].

2. SUGGESTED APPROACH

To guarantee the safety and authenticity of data packets in the WiMAX network, we have presented an effective method for secure data transfer in this article. Both mobile and base station assaults have been the primary focus of previous research on WiMAX security. Base stations should be genuine so that they can authenticate workstations and identify assaults. Thus, it is necessary to safeguard both base stations and work stations through the creation of security techniques.

2.1 Suggested approach

Routine base detection is the initial step in the process, as shown in the architectural design Fig-1. The next step is the mutual authentication procedure. There is a clear description of both processes in their respective phases.

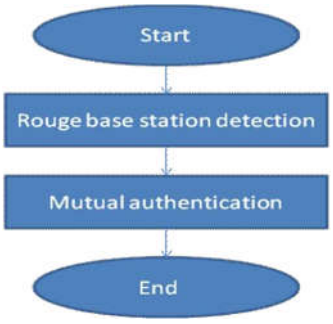

Fig-1 Architecture Diagram

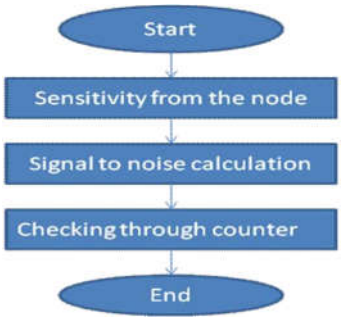

Fig-2 Modular Diagram to detect Rouge Base Station

2.2 Identifying Severe Base Stations :

The following method can be used to identify malicious base stations. For the purpose of identifying rogue base stations, the sensitivity algorithm checks each channel and frequency of the base station. To aid in the detection of the malevolent base stations, it also computes specific statistics. An example of one of these important statistic counters is the outage counter, which records the frequency and duration of base station infrastructure failures. The sensitivity of the base station is likewise handled by the sensitivity counter. Based on the ideal sampling frequency, this algorithm continuously calculates the receiving power and the route loss that the packets face at regular intervals. The suggested method relies on the base station's sensitivity. Determining whether a base station is malicious requires taking into account sensitivity, signal-to-noise ratio, and path loss. A radio's receiver sensitivity is an important feature. The WiMAX device's receiver sensitivity is a measure of the weakness of the radio signal emanating from the base station. The WiMAX Forum details the different modulation techniques and the receiver sensitivity requirements for each certification profile. When it comes to cell sites, the most sensitive receivers allow for a wider coverage area and are more tolerant of deep inside penetration. When comparing two signals, one representing useful information and the other representing undesired noise, the signal-to-noise ratio is the metric used.

$$SNR = P_{Signal} / P_{Noise}$$

Where P is average signal power

At the same locations and within the same bandwidth, the power of the signal and the noise are both measured. For the aim of detecting rogue base stations, this Sensitivity Algorithm runs on each service area/cluster at a scanning period of several milliseconds, as illustrated in Figure 2. At the end of each scan, it uses the signal-to-noise ratio to determine whether the area surrounding the base station has any unexpected signals, interfaces, or noise. To verify the legitimacy of the sender and receiver, it records the sample packet's checksum.

3.1 Algorithm to detect rouge base station

The outage counter (OC), sensitivity counter (SC), and path loss counter (PL) are all variables to consider.

Let Pr denote the received power.

Each threshold value should be represented as an integer between OCth and Er th.

Perform a full channel scan on every BS. Carry out a frequency survey

Find the SNR, OC, SC, PL, and Pr. The condition where BS is deemed rouge is when the following

hold: SC < SCth, SNR > SNRth, PL > PLth, OC > OCth, and checksum error > Erth. If nothing changes, keep scanning the channels. Come to a close if

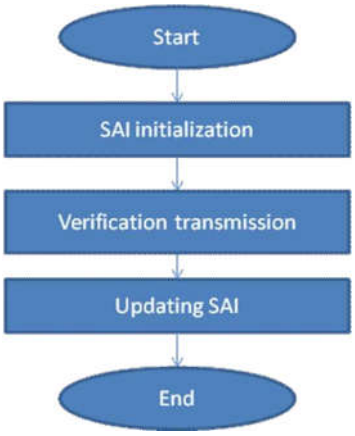

Fig-3 modular diagram of EAP-Transport Layer Security phase

4. PHASE OF MUTUAL AUTHENTICATION :

Extensible Authentication protocol-Transport Layer Security (EAP-TLS) is used at normal base stations to provide mutual authentication after identifying rogue base stations, as illustrated in Fig. 3. Mutual authentication via EAP-TLS is possible between mobile base stations that have their own authentication servers. When MBS1 WMN (mobile base station 1 of the wireless mesh network) successfully identifies itself, the AAA (Authentication, Authorization, and Accounting) server will start the EAP-TLS and send messages to MBS2's WMN module.MBS2 can send back a response message containing the data without consulting its AAA server[13].
MBS1 and MBS2 are able to share the TLS server key thanks to the X.509 certificate. The MBS1 WMN module will send the certificate to the AAA server, which will attempt to approve it, after receiving the final EAP response from MBS2. Following approval, MBS1 will use the premaster secret key to generate a temporary encryption key (TEK), which it will then use to send the completed EAP-TLS message back to MBS2.The master key (MSK), which will ultimately be used to encrypt and decrypt data transmission between the two devices, can then be generated by MBS1 and MBS2. The last handshake is exchanged to complete the authentication procedure following the successful generation of the MSK.
4.1 Four-way handshaking and key derivative :
When an MBS tries to authenticate itself, it will go through the core mutual authentication procedure if it doesn't contain MSK to any other MBS.
Mobile station authentication for n > 1 - After an MBS generates multiple MSKs successfully, it encrypts and unicasts its own MSKs to all other authenticated MBS2 MBS1 AAA Server WMN Module WMN Module X.509.
1) The AAA server sends WMN an EAP-Request.
2) WMN acknowledged the AAA server's EAP-Response.
3) EAP: TLC receives an EAP request.
4) EAP-Response from server to Clint.
5) EAP-Request server to TLS.
6) By sending EAP-Response the connection is over.

Successful Identification and certification is completed by the server.Any neighbor MBS that receives the notify message decrypts it and store the information in the table.If any MSK has a counter over threshold, it deletes from the table because an MSK from far distance will unlikely be used.If an authenticated MBS receives an authentication request from a suspicious MBS that has not

yet been authenticated by the MBS itself, it checks the Node's ID that is transmitted. If the Node's Id matches an entry in the table, this means that the suspicious MBS has been previously authenticated by another trusted MBS. The whole authentication process is reduced and the authenticated MBS will only initiate the MSK handshake process to match the key between each other. In the case of MBS has more than one MSK to the same suspicious MBS, the authenticated MBS will randomly select one MSK and use it to establish secure data connection. If the Node's Id does not match any entry in the table, then the full authentication process is initiated. The advantage of using this proposed cooperated mutual authentication method is that each mobile base station can manage its own AAA server, considerably reducing overhead that may occur in multi-hop authentication. Also, since the MSKs are shared between trusted and authenticated MBSs, the whole authentication process can be simplified to further reduce the overhead at the expense of small key sharing overhead.

5.SSL (Sharing Authorization Data) The first stage :
The workstations are able to detect Distributed Denial of Service (DDoS) assaults through the SA mechanism. When the MS goes into idle mode, the SA is shared between the PC and MS [11]. The MS is required to submit SA to the PC whenever it updates its location or resumes normal function. This value is compared to the original shared value by the PC. The following steps will be taken if the values are matching. Other than that, the procedures are cancelled. After a successful secure LU (location update), the next step is to perform a SA update. Threat actors launching distributed denial of service (DDoS) attacks put a strain on BS, PC, and Authenticator, which must independently verify CMAC values, determine if the requesting MSs are idle, and generate AK contexts for MSs. If we use SA during a DDoS assault, we won't have to do these pointless operations. See Figure 4 for an explanation of the Secure LU procedure. Initially, when the MS goes into idle mode, PC and MS share SA. A subsequent submission of SA to the PC is required whenever the MS updates its location or resumes normal function. The personal computer then checks this number against the initial shared value. Once they've been matched, the following steps will be taken. Otherwise, none of the other operations will proceed. As soon as Secure LU is successful, the SA update should be executed for the next Secure LU. In the subsection that follows, we go into the specific steps.

Fig-4 phases of SA algorithm

5.1 Steps for Implementing SAI :
1) SA is initialized by using the DREG-REQ and DREG-CMD messages for deregistration request and command, respectively. For the sake of illustration, this work employs DRE-GREQ. Before sending DREG-REQ to the BS, an idle MS will determine the CMAC value of DREG-REQ, extract SAI from it, and store SA. If the CMAC is genuine, the BS will extract and store SA after receiving the request (DREG-REQ). An MS-info Request message is sent by the BS to the PC along with the

MS's identity and SA. Following SA processing, the PC validates the outcome with an MS-info Response message.
2) Ensuring the accuracy and transmission of SA: When a mobile station performs Secure LU or Idle Mode Re-entry, it is given a range allocation and is tasked with sending a ranging request, which includes the Type, Length, and Value (TLV) field for SAI. The SA is already part of the TLV, hence the Mobile WiMAX standard and 802.16e don't need any updates. It is provided below the TLV for SAI.
1. When the BS receives a RNG-REQ, it uses the LU REQ message to transmit SAI TLV to the PC. The SA is confirmed by the PC. The PC will send a Context REQ message to the Authenticator requesting the MS AK context if the two values are equal. The AK context is created by the Authenticator and sent to the PC via the Context RSP message.
There is no communication between the PC and the Authenticator when they are in the same entity. The LU RSP message is used by the PC to return the AK context to the BS.
3. The BS then uses the MS's CMAC key to determine the RNG-CMAC REQ's value; if the value is valid, the BS sends RNG-RSP to the MS.
4. The RNG-REQ message is ignored by the BS once the PC tells them of the LU failure if the two SAs are not matched. Neglecting to exchange Context REQ and Context RSP messages, verify CMAC, and generate AK contexts reduces the efficacy of a DDoS attack.
• Type = Not Determinated (TBD)
Depending on the level of security needed, the length can range from 1 to 64 bits.
• The high-order 64 bits of the CMAC value are assigned to the value.
3) SA Update: Since the SA is submitted to the PC in clear text, an MS is required to update the SA once SA is used. It returns to its usual state when the MS performs IM Re-entry. Thus, the MS can de-register and update SAI when returning to idle mode. Consequently, the IM Re-entry situation does not necessitate any explicit methods for updates. After secure LU, an MS goes back to idle mode in the opposite scenario. Throughout Secure LU, the MS and BS communicate using RNG-REQ and RNG-RSP signals. Whether RNG-REQ or RNG-RSP is used to update SAI determines the specific steps to follow. To show how the update mechanisms work, this study use RNG-RSP messages. The PC verifies the MS's SA by communicating with the BS via LU REQ and LU RSP messages. The BS then changes SA with the CMAC value from the RNGRSP message, produces a RNG-RSP message, and transmits it to the MS. To let the PC know about the revised SA, the BS sends a LU confirm message. In the instance of Secure LU, the procedure for storing, checking, and updating SA is demonstrated by the PC and MS using the same new SA.

6. Model and Parameters for Simulation
The suggested approach is tested using the network simulator (NS2) [14]. Over the IEEE 802.16 MAC protocol, the suggested technique has been put into action. The simulation runs for 50 seconds and involves the deployment of clients (SS) and the base station (BS) in a 1100 m × 1100 m area. The 250-meter transmission range is the same for all nodes. Table 1 provides a summary of the simulation's settings and parameters.
6.1.Measures of Performance :

We evaluate the EAP approach (Base Station without Security) against our Protecting Base stations and Mobile stations in WiMAX networks (PBM) method.

The following metrics form the basis of our performance evaluations:

a. The total number of packets received divided by the number of packets sent is the delivery ratio.
(b) Drop: The total number of data packets that were dropped while transmission was underway. The outcomes of the performance are detailed in the section that follows.

Table 1.Simulation Parameters

Area Size	1200 X 1200
Mac	802.16
No. of mobile Nodes	75,125,175,225 and 275
Radio Range	250m
Simulation Time	50 sec
Physical Layer	OFDM
Packet Size	500 bytes
Frame Duration	0.005
Rate	1Mb
No. of Attackers	2

6.1 Measures of Performance

We evaluate the EAP approach (Base Station without Security) against our Protecting Base stations and Mobile stations in WiMAX networks (PBM) method(Base Station with Security). The following metrics form the basis of our performance evaluations:

(a) The total number of packets received divided by the number of packets sent is the delivery ratio. (b) Drop: The total number of data packets that were dropped while transmission was underway. The outcomes of the performance are detailed in the section that follows.

Scene 1: the BS Attack

A. Node-Based: We include 5, 10, 15, 20, and 25 nodes in this experiment. For various scenarios involving different numbers of nodes, Fig. 5 displays the delivery ratio of PBM and EAP approaches. Our proposed PBM method outperforms the EAP method by 85 percent in terms of delivery ratio.
B. For a variety of node densities, Fig. 6 displays the delay of PBM and EAP methods. The decline of our suggested PBM method is 45 percent lower than that of the EAP method.

Scene 2: Attack on the Client

A. Node-Based: In the first trial, we tried out 5, 10, 15, 20, and 25 nodes. For various scenarios involving different numbers of nodes, Fig. 7 displays the delivery ratio of PBM and EAP approaches. Our proposed PBM method outperforms the EAP method by an 80% margin in terms of delivery ratio.

B.For a variety of node densities, Fig. 8 displays the decline of PBM and EAP methods. Our suggested PBM strategy has a 58% lower decline than the EAP approach, as can be seen.

Table 2. Packet Delivery Ratio(PDR)
Base Station without Security Vs Base Station with Security

NO. OF .NODES	PDR (BS WITHOUT SECURITY)	PDR (BS WITH SECURITY)
75	0.949	0.951
125	0.919	0.921
175	0.915	0.899
225	0.859	0.857
275	0.802	0.798

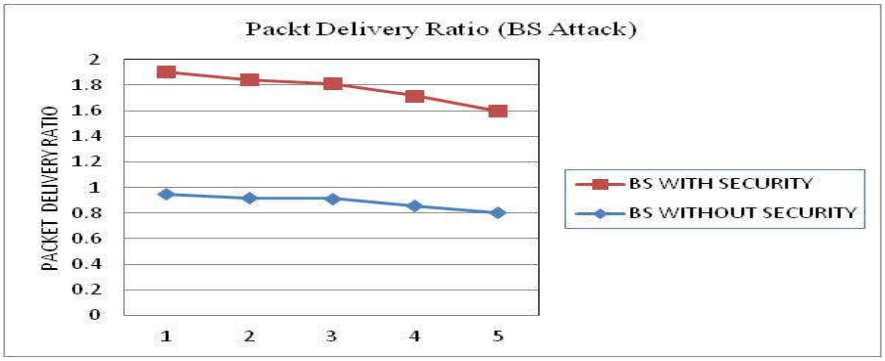

Fig5. Packet Delivery Ratio(PDR) vs No.of Nodes

Table 3. Packet Delay
(Base Station without Security Vs Base Station with Security)

NUMBER OF NODES	Packet Delay (BS with security)	Packet Delay (BS without security)
75	10	10
125	14	14
175	22	23
225	24	25
275	24	28

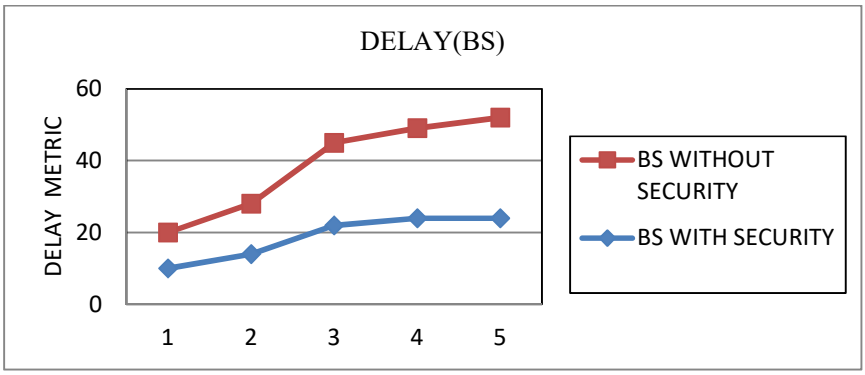

Fig6. Packet Delay VS No.of. Nodes

Table 4. Packet Delivery Ratio
(Client Station without Security Vs Client Station with Security)

NUMBER OF NODES	CLIENT STATION WITHOUT SECURITY	CLIENT STATION WITH SECURITY
75	0.94	0.949
125	0.908	0.919
175	0.891	0.915
225	0.846	0.859
275	0.785	0.802

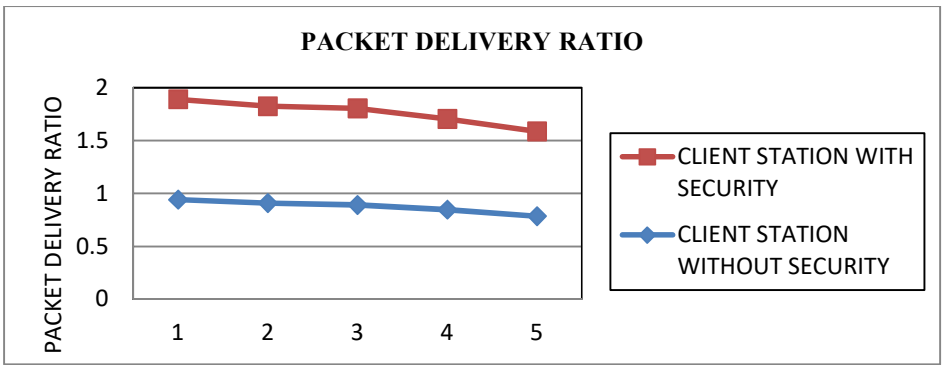

Fig7. PDR vs No. of. Nodes

Table 5. Packet Delay
(Client Station without Security Vs Client Station with Security)

Number of nodes	CLIENT STATION WITH SECURITY	CLIENT STATION WITHOUT SECURITY
75	0.984	1.007
125	1.228	1.004
175	11.25	9.885
225	14.174	16.423
275	31.399	36.422

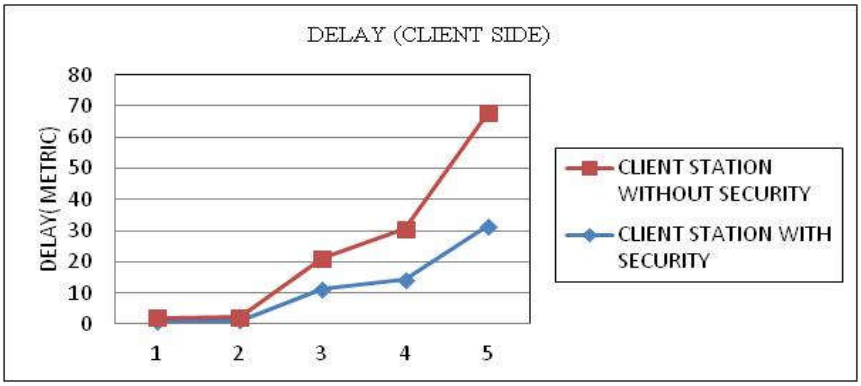

Fig8. Delay vs No. of. Nodes

7. Conclusion:

A technique to identify malicious base stations and protect against distributed denial of service attacks is demonstrated in the aforementioned descriptive paper. A tripartite explanation of the solution is provided. The sensitivity algorithm in the first section allows it to deliver rouge-based detection. Authentication via the Extensible Authentication protocol—Transport Layer Security is possible in the second stage. In order to overcome DDoS attacks, the third phase involves carrying the SA algorithm.

References :

1. Lukasz Kucharzewski and Zbigniew Kotulski: “WiMAX Networks-Architecture and data security”2010, AnnalesUMCS Informatica (AIX)
2. Farrukh Ethisham, Emmanouil A.Panaousis and Christos Politis: “Performance Evaluation of Secure Video transmission over WIMAX”2011 international journal of computer networks and communications.Vol.3 and No.6
3. Sanjay P.Ahuja and Nicole Collier: “An assessment of WiMAX security”2010 scientific research
4. Nithya Bondalapati, “Research on Security Considerations for Mobile WiMAX”, 2004
5. Deepak Kumar Mehto and Rajesh Srivastava: “An Enhanced Authentication Mechanisms for IEEE 802.16(e) Mobile Wimax”2011 International journal of soft computing and engineering (IJSCE) Vol.1 Issue 4
6. Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara and Toshiaki Tanaka, “Security Vulnerabilities and Solutions in Mobile WiMAX”, 2007 IJCSNS International Journal of Computer Science and Network Security, Vol.7 No.11
7. Ramanpreet singh and Sukhwinder singh: “Detection of Rogue Base station using MATLAB” International journalof soft computing and engineering (IJSCE) Vol.1, Issue 5
8. Michel Barbeau and Jean-Marc Robert: “Rogue-Base station Detection in WiMAX/802.16 Wireless Access Networks” 2006 Annales Des Telecommunications Vol 6, Issue 11-12
9. Deepti and Deepika Khokhar: “Detection of Rogue Base stations in WiMAX/IEEE802.16 using sensors”2012 Int.J.Computer Techonology and applications, Vol. 3
10. Liango Xiao, Lary J.Greenstein, Narayan B.Mandayam and Wade Trappe: “Channel-Based detection of Sybil attacksin Wireless Networks”2009 IEEE Transactions on information forensics and security, Vol. 4, No.3
11. Youngwook Kim, Hyoung-Kyu Lim, Saewoong Bahk: “Shared Authentication Information for preventing DDOS attacks in Mobile WiMAX Networks”2008 Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE at Las Vegas, NV
12. Patrick P.C.Lee, Tian Bu and Thomas Woo: “On the Detection of signaling Dos attacks on 3G/WiMAX WirelessNetworks”2009 Elsevier volume 53 and Issue 15
13. Yu-Jin Son, Keun-Woo Lim, TaeShik shon, Young-Bae Ko: “Cooperated Mutual Authentication between Mobilestations in Tactical Networks”2012 Online present.org/proceedings/ Vol. 3
14. Network Simulator: http:///www.isi.edu/nsnam/ns
15. B.Chandran Mahesh, Dr. B. Prabhakara Rao: Protecting Base Stations and Mobile Stations of WiMAX Network Using EAP and SAI Algorithm to Over-Come DDoS Attacks, Volume 3, Issue 3, March 2014 ISSN 2319 – 4847,International Journal of Application or Innovation in Engineering & Management (IJAIEM),Web Site: www.ijaiem.org Email: editor@ijaiem.org.