PUZZLE BASED APPROACH FOR SOLVING DENIAL OF SERVICE ATTACK IN MOBILE WIMAX

Dr. Reena Dadhich[1], Ms.Geetika Narang[2] and Dr. D.M.Yadav[3]

[1]Associate Prof. & Head, Department of MCA, Government Engg. College, Ajmer

reena.dadhich@gmail.com

[2]Asst. Prof, Sinhgad Institute of Technology, Lonavala

geetika.narang@gmail.com

[3]Principal of JSPM'S Bhivarabai Sawant Institute of Technology

dineshyadav8@yahoo.com

ABSTRACT

Mobile WiMAX or IEEE 802.16e gives the access of Broadband Wireless even when the station is moving. But, as always Wireless environment is more open to threats; various threats exist over Mobile WiMAX like "Downgrade Attack", "Key Space Vulnerability" and "Initial Network Vulnerability", and "Denial of Service (DoS)". In this paper we are proposing solution for one of the main Threat which is Denial of Service attack. Proposed solution is based on Puzzle approach. As, of more critical environment of Mobile-WiMAX we have Proposed use of Time Stamp and Nonce Variable for providing the more secure environment prone to DoS. As, DoS mainly exist in two forms which have been mentioned further, proposed work in Literature provides the solution for either of these but our proposed solution will be an attempt to overcome from

THE PHYSICAL INFRASTRUCTURE. WIRELESS NETWORKS REPRESENT AN IMPORTANT EXAMPLE OF SUCH SCENARIOS WHERE CAPTURING AND FORGING PACKETS ARE RELATIVELY EASY. ATTACKS AGAINST NETWORKED SYSTEMS ARE BECOMING MORE COMPLEX AND FOR MOBILE WIMAX IT IS MORE CRITICAL AS WELL AS MORE IMPORTANT TO HANDLE BECAUSE IT SUPPORTS SUBSCRIBER STATIONS MOVING AT VEHICULAR SPEEDS AND THEREBY SPECIFIES A SYSTEM FOR COMBINED FIXED AND MOBILE BROADBAND WIRELESS ACCESS.

1.2 Features of Mobile WiMAX

• **High Data Rates:** The inclusion of MIMO antenna techniques along with flexible sub channelization schemes, Advanced Coding and Modulation all enable the Mobile WiMAX technology to support peak data rates up to 63 Mbps per sector and peak UL (Uplink) data rates up to 28 Mbps per sector in a 10 MHz channel [3].

DOI : 10.5121/ijans.2012.2203

• **Quality of Service (QoS):** The fundamental premise of the IEEE 802.16 MAC architecture is QoS. It defines Service Flows which can map to Different Service code points or MPLS (Multiprotocol Label Switching) flow labels that enable end to end IP based QoS. Additionally, sub channelization and MAP based signalling schemes provide a flexible mechanism for optimal scheduling of space, frequency and time resources over the air interface on a frame by frame basis.

• **Scalability:** Despite an increasingly globalized economy, spectrum resources for wireless broadband worldwide are still quite disparate in its allocations. Mobile WiMAX technology therefore, is designed to be able to scale to work in different channelization from 1.25 to 20 MHz to comply with varied worldwide requirements as efforts proceed to achieve spectrum harmonization in the longer term as mentioned in [12]. This also allows diverse economies to realize the multi-faceted benefits of the Mobile WiMAX technology for their specific geographic needs such as providing affordable internet access in rural settings versus enhancing the capacity of mobile broadband access in metro and suburban areas.

2. SECURITY

As, Protocol Architecture of IEEE 802.16e consists of two layers MAC (Medium Access Control) and PHY (Physical). Security issues also occur at both levels as discussed in [2].
The usage aspect of security features are as following:-

Key Management Protocol: Privacy and Key Management Protocol Version 2 (PKMv2) which is the basis of Mobile WiMAX security as defined in 802.16e. This protocol [6] manages the MAC security using PKM-REQ (Request) / RSP (Response) messages.

Device/User Authentication: Mobile WiMAX supports Device and User Authentication by providing support for credentials that are SIM-based, Digital Certificate or Username/Password-based [7].

Traffic Encryption: Advanced Encryption Standard (AES) cipher used for protecting all the user data over the Mobile WiMAX MAC interface. The keys used for driving the cipher are generated from the EAP authentication [14]. A Traffic Encryption State machine that has a periodic key (TEK) refresh mechanism enables sustained transition of keys to further improve protection.

Fast Handover Support: A 3-way Handshake scheme is supported by Mobile WiMAX to optimize the re-authentication mechanisms for supporting fast handovers. This mechanism is also useful to prevent any man-in-the-middle-attacks [17].

3. PROPOSED WORK

Proposed work in this paper is related to PKM protocol and its shortcoming and then leads towards solution of one of major threat in Mobile-WiMAX called as DoS (Denial of Service). PKM Protocol manages the key distribution and exchange between MS (Mobile Station) and BS (Base Station). For this purpose, X.509 as given in [4], [5] digital certificates and RSA public-key encryption algorithm are utilized. The keys include Authorization Key (AK), Key Encryption Keys (KEKs) and Traffic Encryption Keys (TEKs). AK (Authentication Key) which is shared between MS and BS and the remaining keys are derived from the AK. First, version of PKM, PKM v1 provided one – way Authentication for 802.16d. But that was exposed to various threats

as discussed in [1] like rouge BS threat, replay attack and DoS, after that PKM v2 came and tried to solve some of the issues of PKM v1 but still was having threats like Interleaving, DoS attack and replay attack. (PKMv1 and v2 have been discussed more in detail in the next section), authors in [1] have given a Solution with Hybrid approach for resolving these issues but it also brought some more problems related to complexity of computation involved in procedure.
As, mentioned proposed work is related to solution of DoS attack, which broadly occurs in following two forms like in the first form as shown by [7],[15] **a)** If a MS sends a lot of false authorization requests to a BS, the BS will use all its resources to calculate whether the certificate is right. This will cause DoS, because BS will not be able to serve any MSs anymore [16]. **b)** Another DoS attack, where adversary eavesdrops the authentication message from a MS to a BS then he replays this message multiple times to the BS, which will make the BS ignore the MS and thus creating a Denial of Service.

Here we have Proposed a Solution with the help of timestamp, nonce[8] and client puzzle approach[10] which will be able to give the solution for both of these type of problems, under this when a MS wants to set up communication with BS, then MS will send its timestamp, nonce (random unique value) to BS. At the base station validity of its Timestamp and nonce will be evaluated and if it is found to be correct then BS will send a puzzle. Puzzle will be based on a Hash function like in the following format.

Puzzle= Hash ($X||MS_{NS}||BS_{NS}||MS_{TS}||$ BS_{TS} $||BS_{MAC\text{-}ADDR}$). Where X is solution of Puzzle, MS_{NS}, BS_{NS} represents nonce of Mobile and Base Station and similarly MS_{TS}, BS_{TS} represent time stamp for both and last parameter is $BS_{MAC\text{-}ADDR}$ which represent MAC- Address of Base Station. Legitimate MS will be supposed to evaluate puzzle but not by spurious MS. So, if a MS is able to solve the puzzle only then it will get the authentication. Now, if a MS sends a lot of false authorization request to BS then BS will not go for the validity of its certificate instead of that it will send the puzzle which is supposed to be not solved by spurious MS and hence by this first type of DoS will be overcome. And if adversary eavesdrop the authentication message again and again then it can be caught by nonce and Timestamp, because as mentioned earlier nonce is a unique variable so if the same value comes again and again then just by checking the nonce and validity of Timestamp, BS will come to know that it is a fake request, will ignore it and will continue to work with earlier processing stage. Hence implementation of Proposed Solution will be expected to give solution for both type of DoS attack.

4. SURVEY AND PROBLEM IDENTIFICATION

We have analysed the solution found in Literature for Denial of Service attack. As, mentioned earlier DoS is one of the major threat [15] not for only Wireless environment but also for Wired too [14]. In paper [8], authors have recommended Hybrid approach for the DoS attack. They have mentioned the need of nonce for uniqueness and Timestamp for Synchronization. They have proposed the following model:

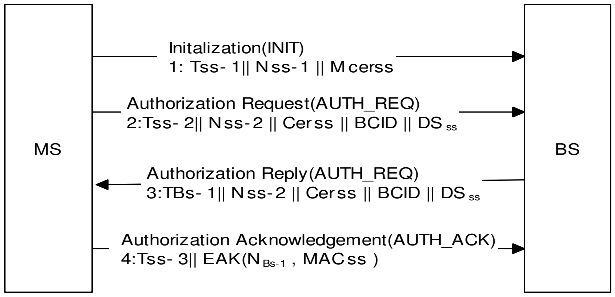

MS
BS
Initalization(INIT)
1: Tss- 1|| Nss- 1 || Mcerss
Authorization Request(AUTH_REQ)
2:Tss- 2|| Nss- 2 || Cerss || BCID || DS ss
Authorization Reply(AUTH_REQ)
3:TBs- 1|| Nss- 2 || Cerss || BCID || DS ss
Authorization Acknowledgement(AUTH_ACK)
4:Tss- 3|| EAK(N Bs-1 , MACss)

Figure 1:- Improve Secure Network Authentication Protocol [8].

Although ISNAP able to indicates the freshness of message by indication of Timestamp, but was not able to solve the first type of DoS attack as mentioned earlier. According to that attack, an attacker will send number of false authorization request by which BS will be busy in attending the request, and will not be able to attend legitimate SS. But with ISNAP too if Timestamp is fresh and nonce is unrepeatable [11] then BS will spend its time on the evaluation of its Certificate and which will again leads toward DoS.

Another problem which is present in ISNAP is the overhead for considering the value of γ as per the following equation.

$$T_{prop-1} = T_{present} - T_{ss-1}$$

$$|T_{prop-1}-T_{prop-2}| <= \gamma$$

Where γ is the auxiliary parameter introduced to consider the fluctuation in propagation time which occurs due to multipath and environmental effects [13] and in the optimum environmental conditions, if the whole process of Authentication has been taken place without any external intrusion then where value of γ must not exceed 3% of total Propagation Time as discussed by Hashmi et al. [8].

First problem can be solved by proposed solution, in which puzzle will be used. Even if the timestamp and nonce are fresh, still BS will not firstly check its Certificate instead of that Base Station will send a puzzle to solve, if the MS is legitimate then it will be able to send the solution otherwise not. So, by this BS will not waste its time in checking the certificate of MS unless and until it has not solved the puzzle.

Second problem can be solved by the use of Timer and comparison of MS timestamp with BS current Time. For example when a MS will send the request first time to BS with its nonce and timestamp then BS will compare MS Timestamp with its current timestamp, and then always MS_{ts} should be always less than BS current Timestamp. Also we can use a minimum time difference if MS_{ts} is much less than BS_{ts}, then it indicates two things either both clocks are not synchronized or the request is very obsolete. So, in that condition BS will send its Timestamp, and if the MS is legitimate and wants to send the request then will resynchronize its clock and will send the new request with fresh time stamp and if MS satisfy the timestamp condition first time then at the second time again MS_{ts} will compare by BS_{ts}. These steps are more clearly defined in proposed Algorithm. Computation overhead is supposed to be much less in this case as compare to ISNAP.

In paper [9] authors have used Client puzzle approach for 802.11. They have used Beacon Frame for Puzzle Parameters; Beacon Frames are broadcast by Access Point. Then Mobile Station which wants to send the request will solve the puzzle and along with Authentication Request.

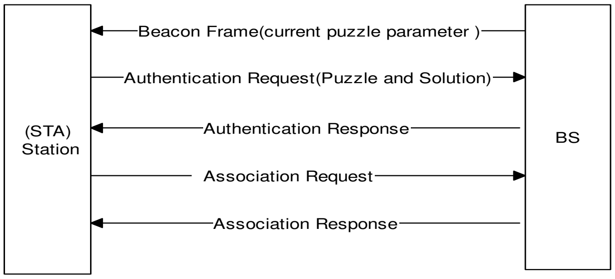
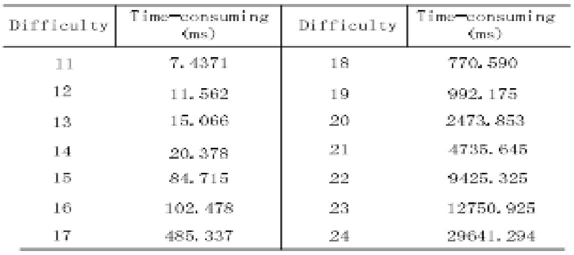

(STA)
Station
BS
Beacon Frame(current puzzle parameter)
Authentication Request(Puzzle and Solution)
Authentication Response
Association Request
Association Response

Figure 2:- Client Puzzle Approach for 802.11[9]

To avoid the potential memory-exhausting DoS attack, authors have proposed to make AP(Access Point) store the information about the puzzle as little as possible. They have chosen CPU resource-exhausting type puzzle and constructed puzzle as Hash (X||r||Ni||mac_add||L) [9]. Where X is the solution to puzzle, r represents a random nonce generated by the station, Ni represents a random nonce generated by AP, mac_add is the MAC address of AP, and L is the difficulty of the puzzle. The station needs to find a solution which makes the first L bits of puzzle all zero. Hash is a hash function decided by AP. Authors have claimed to simulate their scheme on the NS-2(Network Simulator) platform with Duo CPU 2.53GHz/1G Windows XP system. They have focused on time consumed on solving and verifying the puzzle. In simulation, they have used MD5 (Message Digest) hash function and solution X, two nonces Ni and r are all 32 bits and have got the table 1 and Fig.3, showing the relationship between difficulties and time consuming on solving puzzle. From the simulation results, they have found that with the difficulty increasing, the time spent on solving puzzle increase quickly, nearly exponent growth. On average, when difficulty increases 1, brute-force computation time doubles. If AP is not under the DoS attack, AP can set a low difficulty, even zero, so that stations can complete the access as soon as possible. When AP is under the attack, a proper difficulty is needed. In general, station can tolerate the extra time in access procedure. The extra time spent on solving puzzle influences legitimate users little. Comparing with the time consumed on solving puzzle, the time on Verification is too small to compute in simulation. Authors have argued that Verification work is trifling to AP proves that their scheme makes much more resource consumed on STA(Station) sides, but as little as possible on AP sides.



Difficulty	Time—consuming (ms)	Difficulty	Time—consuming (ms)
11	7.4371	18	770.590
12	11.562	19	992.175
13	15.066	20	2473.853
14	20.378	21	4735.645
15	84.715	22	9425.325
16	102.478	23	12750.925
17	485.337	24	29641.294

Table 1:- Time consumed on solving different difficulty puzzles [9]

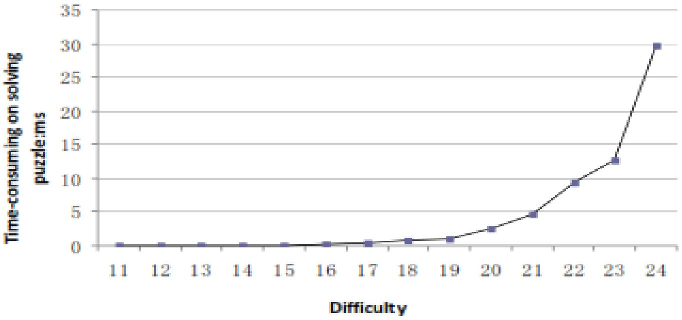


Figure 3:- The Curve Relationship between Difficulties and Time- Consuming on solving puzzle [9]

The very first problem in the proposed model of Figure 2 is the use of Beacon Frame, which increases the Access Point load for self-initiating the communication and also if not more STA (Station) are interested then these will increase the load. **The Second weakness** which is present in [9] ("Anti-DoS Attack scheme") is of no use of Timer, which can defined how much time will be allotted to solve a puzzle or we can say life time of one Beacon frame.
In the Proposed Solution beacon frames will not be present so the first problem of traffic load will be able to resolve by this. If MS will send the authentication request then in acknowledgment to that BS will send the puzzle and will start a timer at its end, if BS receives the valid answer of puzzle from MS before time out, then only BS will do further communication. Also the protocol Proposed by authors in their research paper [9] was for 802.11, but the proposed solution will be for IEEE802.16e.

5. METHODOLOGY

5.1 Proposed Algorithm

I. MS sends INIT (Initialization Request), MS_{TS} and MS_{NS} to BS.
II. BS checks the validity of MS_{TS} and MS_{NS}. If found valid then GO TO step III.
Else GO TO step XI.
III. BS sends the Puzzle (PZ), BS_{TS} and BS_{NS} to MS.
IV. MS solves the puzzle and then send Puzzle Solution (PZS), $MS_{MAC-ADDR}$, MS_{BCID} and MS_{cap}, DS_{MS}, MS_{TS} and $MS_{NS+1}$to BS.
V. BS checks PZS, if valid then GO TO step VI Else GO TO step XII
VI. BS sends the, DS_{MS}, $MS_{MAC-ADDR}$ to Certify authority (CA).
VII. CA verifies $MS_{MAC-ADDR}$ and DS_{MS} and sends the result to BS.
VIII. BS receives the Result if correct then GO TO step IX. Else GO TO step XII
IX. BS sends the Sequence Number, Life time, SAIDL, MS_{BCID}, Cer_{BS}, DS_{BS}, BS_{TS+1}
and BS_{NS+1}, MS_{TS+1}, $MS_{MAC-ADDR}$, and EPUMS $_{(AK, SSID)}$ to MS.
X. In return MS send Authorization Acknowledgment (MS_{TS+2}, EAK (BS_{NS+1}, $MS_{MAC-ADDR}$)) to BS.
XI. Communication will occur.
XII. BS Terminate the Request.

Figure 3 shows a Sequence Diagram for proposed Algorithm; explain step by step execution of proposed work. We have shown three entities in Figure3. Mobile Station (MS), Base Station (BS), and Certificate Authority (CA). Communication will be initiated by Mobile Station as per following Steps.

Step1 Communication will be started by Mobile Station (MS), It will send the initialization request called as INIT, its timestamp called as Mobile Station Time Stamp(MS_{TS}), Mobile Station Nonce sequence (MS_{NS}). It will start its Timer which can be called as (MS_{TR}).With its timer it will wait for specified amount of time and if it does not get the response from BS then it will resend the request.

Step 2 BS will receive this message it will firstly check MS_{TS}, MS_{NS}.BS will match the MS_{TS} with its current Timestamp. If it is much smaller than that (minimum value can be proposed) then BS will not respond to this because that must be obsolete request and may be intruder taking the benefit of that. Also it will check the validity of Nonce.

Step 3 After doing verification at step2, BS will send its Nonce, its Timestamp, and puzzle which will be created with number of parameters like Last Timestamp and nonce of MS, MAC_addr of BS, nonce and timestamp of BS. For creating the puzzle Hash Function will be used, and MS will use brute force computation

Step 4 and Step 5 After solving the puzzle at Step 4, MS will send solution to BS, along with solution it will send its MAC Address($MS_{MAC-ADDR}$), Digital signature (DS_{MS}) and Capb(MS_{cap}) which indicates Crypto capability of MS and BCID(Basic Connection Identity) or MS_{BCID} along with these MS_{TS+1} and MS_{NS+1} will also be send.

Step 6 and Step 7 Now Base Station will check the puzzle solution at step 6 and if it is correct only then it will send MS's MAC address and its Digital Signature to Certify Authority otherwise request will be discarded.

Step 8 Certify Authority will check certification and accordingly will reply to BS.

Step 9 and Step 10 CA will send the response for MAC address and Digital Signature, once BS has been verified about MS, It will send Authorization reply by sending AK (Authentication Key) encrypted with MS public key and MSID (Mobile Station identifier) unique for each Mobile Station in network, Digital Signature of BS(DS_{BS}), Sequence Number(Seq No), Authorized Association Identifier (AAID) which determines the selected security Association, Security Association Identify list(SAIDL), Life-Time, MS_{NS+1}, BS_{NS+2}, MS_{NS+2}.

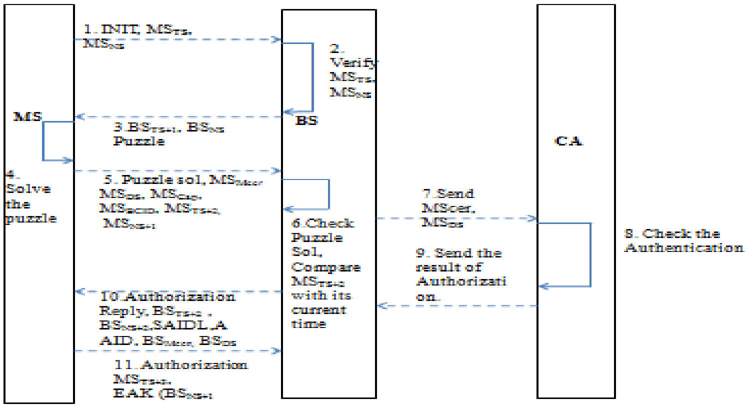

MS
BS
CA
1. INIT, MSTS, MSNS
2. Verify MSTS, MSNS
3.BSTS+1, BSNS Puzzle
4. Solve the puzzle
5. Puzzle sol, MSMacr MSDS, MSCap, MSBCID, MSTS+2, MSNS+1
6.Check Puzzle Sol, Compare MSTS+2 with its current time
7.Send MScer, MSDS
8. Check the Authentication
9. Send the result of Authorizati on.
10.Authorization Reply, BSTS+2 , BSNS+2,SAIDL,A AID, BSMacr, BSDS
11.Authorization MSTS+3, EAK (BSNS+1

Figure 4. Sequence Diagram for Proposed Authentication Framework.

Step 11 Now MS sends Authorization Acknowledgement with EAK (BS_{NS+2}, $MS_{MAC\text{-}ADDR}$), MS_{TS+3}.

5.2 Flow Chart

To explain the working of Algorithm in more detailed way, Figure 4 the Flow Chart for Proposed Authentication Frame work which shows detail of picture of Proposed Authentication Frame Work. There are three entities present in the diagram MS (Mobile Station), BS (Base Station), CA (Certificate Authority). As, shown in the diagram communication will be initiated by MS by sending its First Time Stamp, nonce variable, and its MAC address and a timer will be initialize, this timer will decide for how much time MS will wait for the response of BS. If MS does not receive the response from Base Station before Timeout then it resends the Request. On the other when BS receives this message, it evaluates Mobile Station Time Stamp with its current time as mentioned in step 2 of Figure 3 and after the verification of MS, BS sends the puzzle along with its Timestamp and Nonce to MS and starts its timer if before the Timeout MS sends the correct solution only the it verifies the solution of Puzzle otherwise request to get terminated as shown in the Figure 4. Also when MS sent the solution of puzzle it also send important information like its Digital Signature, its crypto capability, its Basic Connection Identity (BCID), and its current time stamp. Now, if BS found that puzzle solution is correct then it sends the MS_{DS}, $MS_{Mac\text{-}Addr}$, to CA. And before sending these to CA, BS again compares the Timestamp of MS with its current Timestamp and if found valid only then proceed for signature verification. CA does the verification and sends back the result to Base Station. If Base Station found the result positive then it sends the Authorization Reply to the MS as mentioned in step 9 and 10 of Figure 4 and reply to that MS sends the Authentication Acknowledgment to the Base Station.

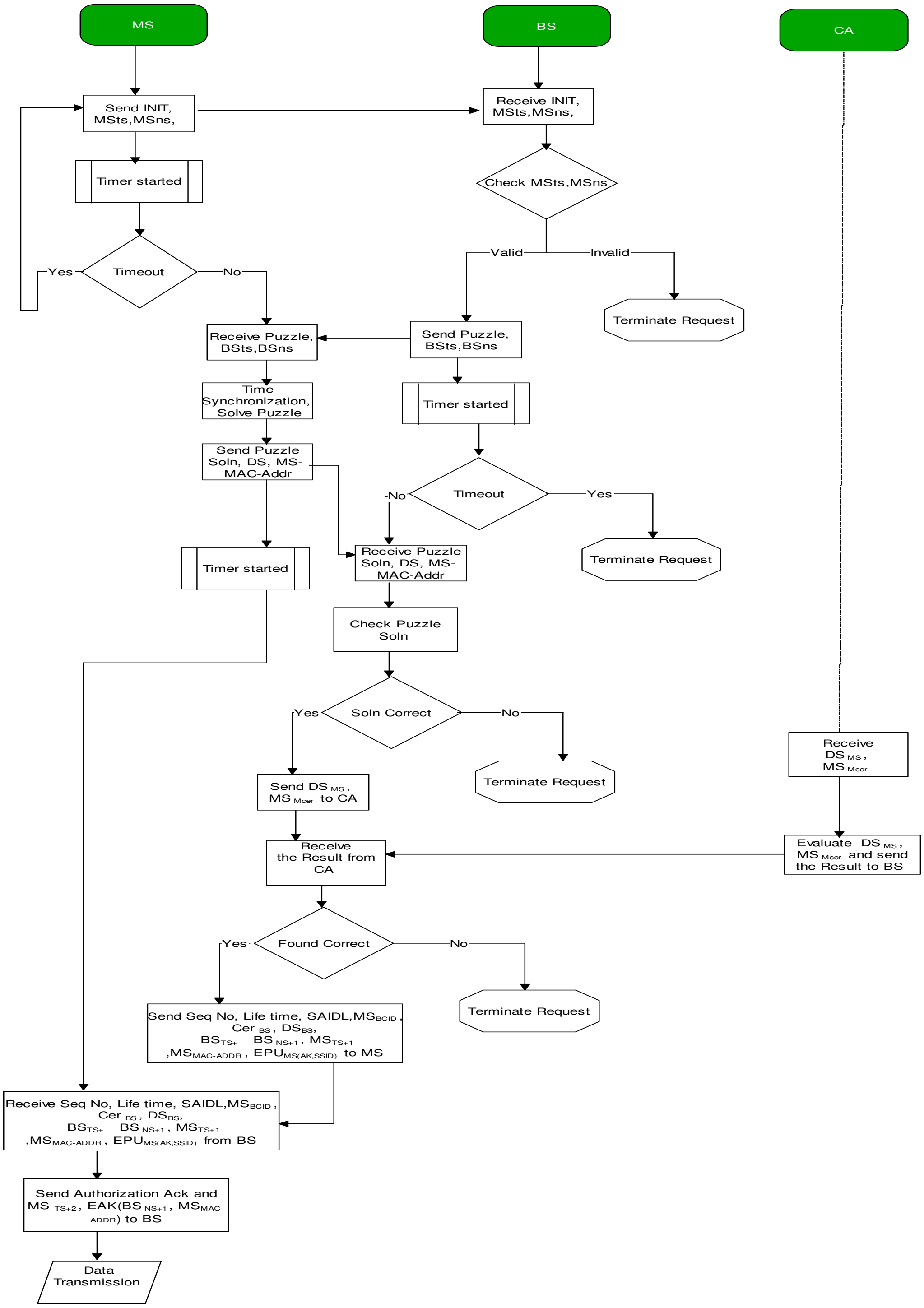

MS
BS
CA
Send INIT, MSts,MSns,
Receive INIT, MSts,MSns,
Timer started
Check MSts,MSns
Valid
Invalid
Yes
Timeout
No
Terminate Request
Receive Puzzle, BSts,BSns
Send Puzzle, BSts,BSns
Time Synchronization, Solve Puzzle
Timer started
Send Puzzle Soln, DS, MS-MAC-Addr
No
Timeout
Yes
Timer started
Receive Puzzle Soln, DS, MS-MAC-Addr
Terminate Request
Check Puzzle Soln
Yes
Soln Correct
No
Receive DS_{MS}, MS_{Mcer}
Send DS_{MS}, MS_{Mcer} to CA
Terminate Request
Receive the Result from CA
Evaluate DS_{MS}, MS_{Mcer} and send the Result to BS
Yes
Found Correct
No
Terminate Request
Send Seq No, Life time, SAIDL,MS_{BCID}, Cer_{BS}, DS_{BS}, BS_{TS+} BS_{NS+1}, MS_{TS+1} ,$MS_{MAC-ADDR}$, $EPU_{MS(AK,SSID)}$ to MS
Receive Seq No, Life time, SAIDL,MS_{BCID}, Cer_{BS}, DS_{BS}, BS_{TS+} BS_{NS+1}, MS_{TS+1} ,$MS_{MAC-ADDR}$, $EPU_{MS(AK,SSID)}$ from BS
Send Authorization Ack and MS_{TS+2}, EAK(BS_{NS+1}, $MS_{MAC-ADDR}$) to BS
Data Transmission

Figure 5. Proposed Flow Chart for Secured Authentication Framework in Mobile-WiMAX.

6. CONCLUSION AND PROPOSED WORK

Mobile WiMAX requires a highly secure Authentication Framework, in previous research work various methods like PKMv1, PKMv2, have been used and then ISNAP have been proposed with addition of Time Stamp and Nonce to ensure the freshness of protocol initiation certificate which was not present in PKMv1 and PKMv2. But as the security is more crucial in case of Mobile-WiMAX due to its open working environment, only Timestamp and Nonce addition cannot assure whether the MS is an intruder or not and verification of Digital Signature of MS makes BS too busy and leads toward DoS for others. So, to provide more reliability and to overcome or reduce the problem of DoS attack we have proposed a solution with puzzle approach, in which unless and until a MS will not solve the puzzle (which is sent by BS) will not be able to set up the communication. As, discussed in the paper there are two type of DoS attack and proposed work will be able to solve both of these. In our future work we will implement proposed puzzle based approach authentication results by simulating using NS-2.

REFERENCES

[1] Fuden T Shering, Anjali Sardana Dept. of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, “A Review of Privacy and Key Management Protocol in IEEE 802.16e”, International Journal of Computer Applications (0975 – 8887) Volume 20– No.2, April 2011

[2] Bart Sikkens, Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, the Netherlands ,sikkensb@cs.utwente.nl , “Security issues and (IEEE 802.16e)” proposed solutions concerning authentication and authorization for WiMAX8thTwente Student Conference on IT, Enschede, January 25 , 2008 Copyright 2008, University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science.

[3] Dr. Jacob Sharony, Director, Network Technologies Division. Centre of Excellence in Wireless & IT Stony Brook University, “Introduction to Wireless MIMO – Theory and Applications” IEEE LI, November 15, 2006.

[4] Frank Chee-Da Tsai, Jenhui Chen, Chiang-Wei Chang, Wei-Jen Lien, Chih-Hsin Hung, Jui-Hsiang Sum, “The Design and Implementation of WiMAX Module for ns-2 Simulator”, Network and Multimedia Institute, Institute of Information Industry, Department of Computer Science and Information Engineering, Chang Gung University, Kweishan, Taoyuan, Taiwan, R.O.C

[5] Michel Barbeau, “WiMax/802.16 Threat Analysis”, School of Computer Science Carleton University, Ontario, Canada, October, 2005

[6] Ayesha Altaf, College of Signals, NUST, ayeshaaltaf@mcs.edu.pk, M.Younus Javed College 0f E&ME, NUST, myjaved@ceme.edu.pk, Attiq Ahmed, College of Signals, NUSTattiq-mcs@nust.edu.pk “Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005”.

[7] Leonardo Maccari, Matteo Paoli, Romano Fantacci, Department of Electronics and Telecommunications- University of Florence Telecommunication Network Lab tel.: +390554796467- fax: +390554796485 Florence, Italy Email maccari, Paoli, fantacci @lart.det.unifi.it “Security analysis of IEEE 802.16”.

[8] Raheel M. Hashmi, Arooj M. Siddiqui, M. Jabeen, K. Shehzad, A. Zubair, K. S. Alimgeer,” “Improved Secure Network Authentication Protocol (ISNAP) for IEEE 802.16” Information and Communication Technologies, 2009. ICICT '09. International Conference.

[9] Qingkuan Dong, Lin Gao , State Key Lab. Of Integrated Services Networks, Xidian University Xi’an, 710071, China, qkdong@mail.xidian.edu.cn, Xiaoping Li, The School of meno- electronic engineering, Xidian University, Xi’an, 710071, China, xpli@xidian.edu.cn.”A New Client-Puzzle Based DoS-Resistant Scheme of IEEE 802.11i Wireless Authentication Protocol” 2010 3rd International Conference on Biomedical Engineering and Informatics (BMEI 2010).

[10] Sen Xu, Chin-Tser Huang, “Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions”, Computer Science and Engineering Department, University of South Carolina, Columbia, September, 2006.

[11] GauravSoni, Assistant Professor, Department of Electronics and Communication Engineering, Sandeep Kaushal Amritsar College of Engineering and Technology, Amritsar, India, Sandeep Kaushal "Analysis of security issues of mobile WiMAX 802.16e and their solutions" volume 1 issue 3 manuscript 3 November 2011. International journal of Computing and Corporate Research. ISSN 2245 054X.

[12] David Halliday, Robert Resnick, Jearl Walker, "Fundamentals of Physics", Chapter 33: Electromagnetic Waves, p. 893, Jhon Wiley & Sons Inc., June 2004. ISBN 9780471232315.

[13] Michel Barbeau, "Rogue-Base Station Detection in WiMAX/802.16, Wireless Access Networks", School of Computer Science, Carleton University, Ottawa, Canada

[14] Prof. Pranita K. Gandhewar Computer Science & Engineering Department NYSS College of Engineering & Research Nagpur, India E-mail: pranita.gandhewar@gmail.com, Prof. Prasad P. Lokulwar Computer Science & Engineering Department, J.D Institute of Engineering & Technology Yavatmal, India. E-mail: prasadengg16@gmail.com. "Improving Security in Initial network entry process of IEEE 802.16 e".

[15] Anjani K.Raietal. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 08, 2010, 2736-2741."Strong Password Based EAP-TLS Authentication Protocol for WiMAX".

[16] Guide to Securing WiMAX Wireless Communications, Recommendations of the National Institute of Standards and Technology, Karen Scarfone, Cyrus Tibbs, Matthew Sexton, NIST (National Institute of Standard and Technology), US Department of Commerce.

[17] Federal Information Processing Standards Publication November 26, 2001, announcing the Advanced Encryption Standard (AES).

Authors

Dr.Reena Dadhich
Associate Prof. & Head, Dept. Of MCA, Govt.Engg.College, Ajmer

Ms.Geetika Narang
Asst. Prof. Sinhgad Institute of Technology, Lonavala

Dr.D.M.Yadav
Principal of JSPM'S, Bhivarabai Sawant Institute of Technology