International Journal of Management, IT & Engineering
(ISSN: 2249-0558)

CONTENTS

Editorial Board

Editorial Advisory Board

Title

ENHANCEMENT OF SECURITY FOR INITIAL NETWORK ENTRY OF SS IN IEEE 802.16E

Author(s)

AHMAD ADNAN
Department of Computer Science,
University of Agriculture, Faisalabad-38040, Pakistan

FAHAD JAN
Department of Computer Science,
University of Agriculture, Faisalabad-38040, Pakistan

AHSAN RAZA SATTAR
Department of Computer Science,
University of Agriculture, Faisalabad-38040, Pakistan

MUHAMMAD ASHRAF
Department of Computer Science,
University of Agriculture, Faisalabad-38040, Pakistan

INAAM SHEHZAD
Department of Computer Science,
University of Agriculture, Faisalabad-38040, Pakistan

ABSTRACT:

Security is the main concern in these days and everyone want to secure his communication. IEEE 802.16e is a new broadband technology that is used to provide secure wireless access to thousands of users in a city at high data rate. This research paper examines the security for initial network entry of mobile stations and subscriber stations for IEEE 802.16e network. Some threats like denial of service (DoS) attacks were most common in the IEEE 802.16e network, the reason is; it is a new standard and need some security measurements. DoS attacks occur when the SS wants to communicate with base station (BS) and range request message (RNG_REQ) has been sent to BS. BS responds with range response (RNG_RSP) message to SS. Here occurs the DoS attack and this attack denied all communications between BS and SS. In this research paper we have discussed some security countermeasures that control the DoS attacks that occurred at the time of initial network entry of SS.

Key Words: Security, Communication, Threats

INTRODUCTION:

This paper is about the security of WiMAX technology. WiMAX is an emerging standard by the IEEE and WiMAX Forum. This technology has been designed to give network access at high data rate with security, but being a new technology it has been attacked by different attackers and threats at different time. WiMAX working is on two layers and these layers are physical layer and MAC layer. The endeavor of these two layers is that, to support the internet services over wireless metropolitan area networks (WMAN). WMAN is used at the place of wired system such as Digital Subscriber Line (DSL). The current version is IEEE 802.16-2009 can also be shown as, 802.16 j-2009. As it is used to provide wireless access in a city, but when we see security then so many threats have been found on both layers. PHY layer threats are jamming and scrambling (Jamshed, 2005).

On the other hand MAC layer threats are related to authentication and authorization (Fernandez, and Michel, 2008). Reviewing these threats many solutions have been designed to provide security but they were not sufficient in providing security. These solutions use the key protocol and that protocol is Privacy and key management protocol. There are two versions of

PKM and that are PKM v1 and PKM v 2. Privacy and key management protocol version 1 has been used in developing the solutions and this protocol was the key protocol in WiMAX. Although they successfully design the solutions for providing security but after some time that solutions were also attacked by some attacker. They found some new threats that attack on protocol and cause diminish of communication. The threats that attacked the privacy and key management protocol version 1 were replay attack, man in the middle attack and denial of service attack. In them denial of service attack is the most dangerous attack because it completely demolish the communication between the base station and the subscriber station (IEEE Press, 2009).

PKM v 2 has been developed to overcome the threats of last protocol. It provides some extra features for security. In this version of PKM two algorithms are used to design security and they are RSA and EAP. They can be used in many ways such as RSA, RSA + EAP, EAP and EAP + EAP (IEEE Press, 2009).

METHDOLOGY:

There are some methods that were proposed and some are under development. The reason is it is a new standard. The research has done in this paper based on the published materials, journals and literature review. Some materials also get from IEEE publications and websites. Our method that is proposed in the research based on the study of research papers of Shon, T. *et al.*, **S. Maru *et al.* and** Altaf *et. al.* They discussed some methodologies in their papers. They proposed different schemes for initial network entry adversary. Shon, T. *et. al.* proposed that prime numbers should be generated at the time of initial network entry and they devised the use of diffie hellman key agreement scheme. Some limitations found in their proposed solution and that was they devised the use of prime numbers but they could not mentioned that BS will generate that prime number or SS. The other limitation was that they have not given any mechanism to generate the prime numbers**.** S. Maru *et al.* proposed that the use the public key cryptography (PKC) to transmit the initial ranging messages. They also said that the digital certificate should be used at the time of initial ranging process. Some limitations were found and that were; if we use the digital certificates then there was a fundamental change require in protocol. That is not possible. Altaf *et. al.* proposed the visual cryptography scheme to

extend initial network entry mechanism and they also devised the use of digital certificates. By using this scheme some limitations were found and that were; if we use the visual cryptography scheme then a trusted third party server should be needed for end to end communication that is not good for the network. The other one was that they devised the use of digital certificates but it requires a fundamental change in algorithm.

Our research depends upon their literature. We proposed a scheme and that scheme is; prime numbers should be known at the time of initial network entry by base station and the subscriber station. Both BS and SS maintain a list of prime numbers that is denoted by "x". Values should be an 8 bit number. We have also used the deffe helman key algorithm. Algorithm for our scheme is.

1) BCID request from subscriber station to base station. The BCID value is zero.
    a. A random CDMA code obtained by the subscriber station
2) Base station reply to subscriber station with BCID. That is 16 bit long.
3) Subscriber station generates the prime-root 'x' using updated dot 16 KDF algorithm, and send this to base station.
4) Now base station reply to Prime-root after verification and sent to base station but extension of six steps include.
    a. 'x' is generated by base station using updated dot16KDF algorithm
    b. 'x' is verified by the base station that whether it is in prime root in gf (P)
        i. If it is in then send value 0 to subscriber station
        ii. otherwise send the difference of nearest (g – x)
    c. g value of prime is adjusted by the subscriber station
    d. A random number A_{BS} mod P is choose by the base station
    e. Public key $B_{BS} = g^{A_{BS}}$ mod P calculated by the base station
    f. Then this public is sent to subscriber station by the base station
5) A request is sent from subscriber station to base station that is containing public key of subscriber station.

a. A random number is choose by the subscriber station and the number is A_{ss} mod P

b. Public key $B_{ss} = g^{Ass}$ mod P is calculated by the subscriber station.

c. Then this public key of subscriber station is sent to base station

6) Now both the base station and the subscriber station calculate the session keys.

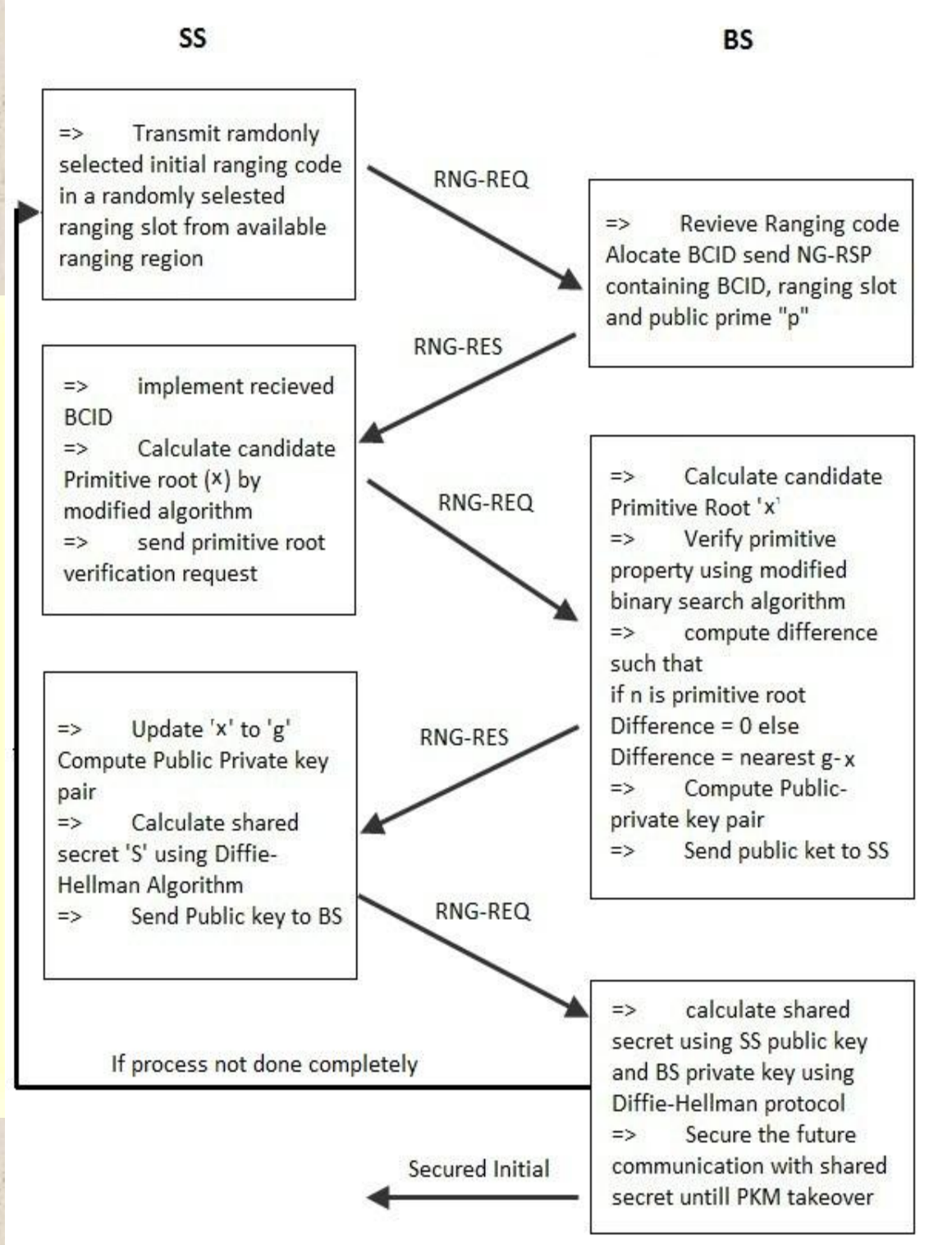
a. Session Key $_{SS} = B_{BS}^{Ass}$ mod P

b. Session Key $_{BS} = B_{SS}^{A_{BS}}$ mod P

7) If process not done clearly. Reset prime numbers list and do the all steps again.

8) From the session keys the initially network is now safe. The other initial ranging messages are encrypted. For further security hash message authentication code and cipher block chaining can be applied depending upon the network situations.

Our solution is implemented in simulation software OMNET++. Three mobile stations one base station and one attacker in scenario and results are discussed in next section.



Explanation of Algorithm

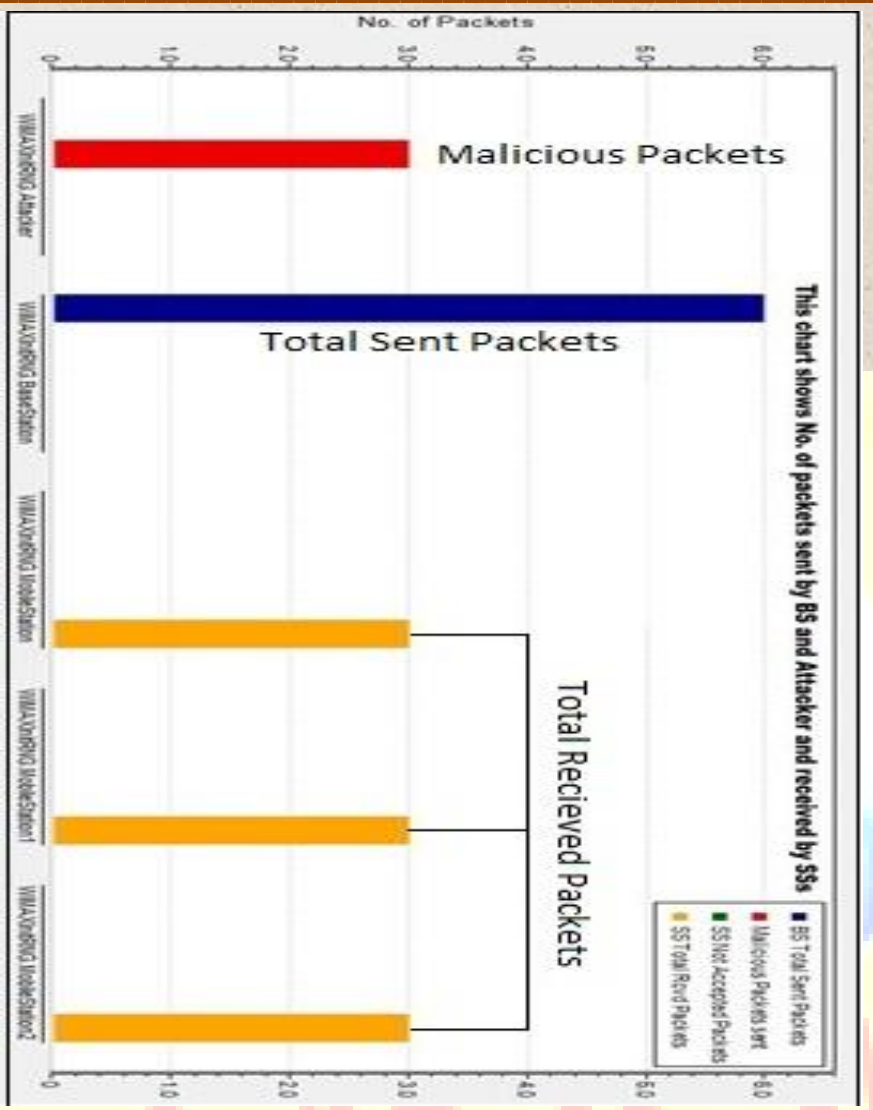
RESULTS AND DISCUSSIONS:

Results based on two scenarios and these scenarios are;

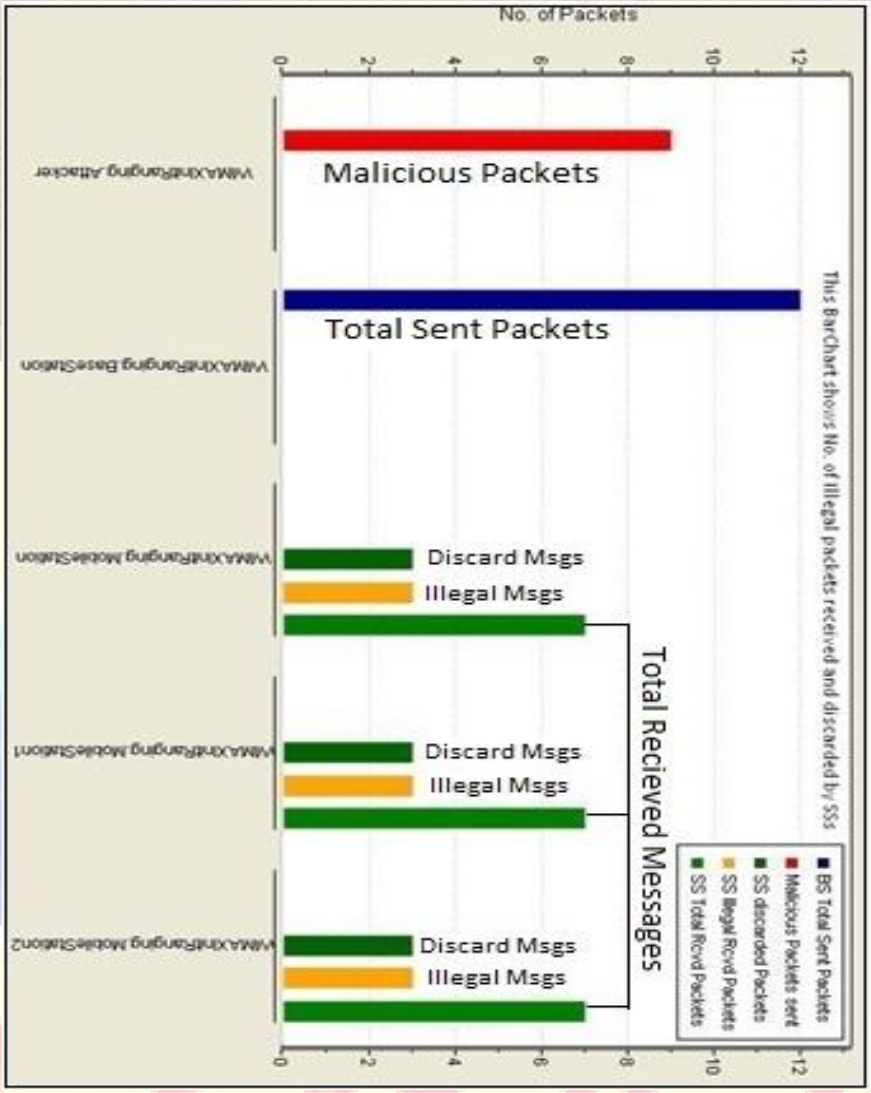
- ✓ Without proposed solution
- ✓ With proposed solution

When using without proposed solutions we found some adversaries at the time of initial network entry. Results are explained by the following graph 1. Total sent packets by base station are in blue line. Total received messages are in yellow lines and malicious packets are in red line. Malicious packets are three its mean one malicious packet sent to each mobile station and no malicious packet was removed or covered.

When using with proposed solutions we found some results and are explained by the following graph 2. Total sent packets by base station are in blue line. Total received messages are in light green lines and malicious packets are in red line. Illegal messages that were received by each mobile station are in yellow line. All three illegal messages are discarded and it shows that initial network entry is safe.



Network Conditions before proposed Solution (Graph 1)



Network Conditions after proposed solution (Graph 2)

The above graph shows that; the total discard messages are equal to the number of illegal messages that were sent using malicious packets. These results show that the initial network entry for mobile stations is safe.

CONCLUSION:

There are so many threats that are common in wireless network and WiMAX network. Security sub layer provides many security features to avoid these threats but this is not quite enough. The reason is new threats are coming by different attackers so we have to work more in

security areas to avoid these threats. So more security countermeasure should be needed and researchers have to work more in this area to defend network. Researchers have to develop stronger security measurements because it is a new standard and everyone is moving on it.

REFERENCES:

- Altaf. A., M. Younus, and A. Ahmed, 2008. "Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005," Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. 0(1):335-339
- Fernandez, E. B. and V. Michel, 2008. "An Overview of WiMAX Security" CRC Press. 978(4523):197-204
- IEEE Press, 2009. "Design of distributed Security architecture for DoS attacks in Wimax Networks". 978(3):54-61
- Jamshed, H. 2006. "Security Issues of IEEE 802.16 (WiMAX)" School of Computer and Information Science, Edith Cowan University, Australia, PP:1-10
- Maru, S. and Brown. 2004. "Denial of Service Vulnerabilities In the 802.16 Protocol". 4th International ICST Conference on Wireless Internet, 5(3):97-103.
- Shon, T. and C. Wook. 2007. "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions". First International Conference, NBIS, LNCS, 4650(1): 88-97