A Review of Privacy and Key Management Protocol in IEEE 802.16e

Fuden Tshering
Dept. of Electronics and Computer Engineering,
Indian Institute of Technology Roorkee,
Roorkee, India

Anjali Sardana
Dept. of Electronics and Computer Engineering,
Indian Institute of Technology Roorkee,
Roorkee, India

ABSTRACT
WiMAX is the next generation technology that offers broadband wireless access over long distances. As WiMAX standards expand from considering a fixed line-of-sight propagation and point-to-multipoint infrastructure high frequency system to a lower frequency non-line-of-sight mobile system, WiMAX is open to more security threats than other wireless systems. This paper presents the different security issues present in Privacy and Key Management Protocol along with the proposed solutions.

General Terms
WiMAX; Security

Keywords
WiMAX; security; privacy and key management protocol; authentication; authorization.

1. INTRODUCTION
The IEEE 802.16 is the standard for the Wireless Metropolitan Area Network (WMAN), better known as WiMAX (Worldwide Interoperability Microwave Access). WiMAX Forum is on a mission to advance and certify compatibility and interoperability of broadband wireless products based on IEEE 802.16 family standards. The standard IEEE 802.16 gives the specifications for the air interface allowing point-to-point and PMP BWA in the 10-66 GHz frequency band under line-of-sight (LOS) conditions. In 2004, IEEE 802.16d [1] was published to address the requirements of fixed BWA under nonline-of-sight (NLOS) conditions. An amendment to IEEE 802.16d was drafted in 2005 as IEEE 802.16e [2] to increase the scope of WiMAX which provide support for mobility of mobile subscriber stations (MS) moving at a vehicular speed up to 150km/h.

The key feature of WiMAX networks is that the security layer is built into the protocol stack instead of being added on later. The messages for authentication and key exchange are defined as part of the medium access control (MAC) layer. The MAC layer performs encryption based on the keys negotiated during the key exchange phase. The IEEE 802.16d standard defines the security mechanisms for fixed network. The security architecture of the IEEE 802.16d standard is based on PKMv1 (Privacy and Key Management) protocol. The IEEE 802.16e standard defines the enhanced security mechanisms for the mobile network. The security architecture of the IEEE 802.16e is based on PKMv2 protocol which resolved most of the issues present in the IEEE 802.16d, with a major improvement in mutual authentication.

Many methods have been proposed to address some of the security issues in WiMAX while some others are still untouched. The objective of this paper is to present a literature survey on existing security issues and its various solutions. Section 2 will briefly give an overview of the architecture and security mechanisms of IEEE 802.16. Section 3 discusses the security issues and its counter measures from existing research efforts. Finally, section 4 will provide the conclusions and the future work activities.

2. BACKGROUND STUDY

2.1 Protocol Layer
The protocol architecture of IEEE 802.16 is structured into two main layers: the MAC layer and PHY (physical) layer (see Figure 1).

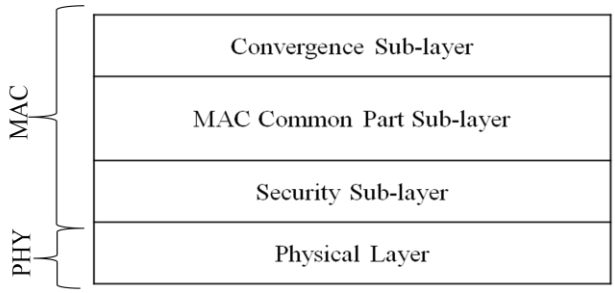

Fig 1: Protocol Architecture of IEEE 802.16.

The MAC layer is divided into three sublayers: Convergence Sublayer (CS), Common Part Sublayer (CPS) and Security Sublayer [3]. The CS sublayer is to converse with higher layers and transform upper-level data services to MAC layer flows and associations. The function of CS sublayer is to receive data from higher layers and to classify them as ATM cell or packet and forward frames to CPS sublayer [4]. In CPS sublayer, the rules for system access, bandwidth allocation and connection management are defined. Functions like scheduling, connection control and automatic repeat request is defined here. Security sublayer provides secure key exchange and encryption. Security sublayer has two main protocols: (a) encapsulation protocol for encrypting packet data across the 802.16 network. (b) PKM protocol for secure distribution of the key negotiations from the Base Station (BS) to the Subscriber Station (SS). The PHY layer is responsible for receiving MAC frames and transmitting them through coding and modulation of radio frequency signals, providing a two-way mapping.

2.2 WiMAX Security Mechanisms
The security protocol provides mechanisms to ensure confidentiality, integrity and client authentication with the implementation of a PKM. PKM provides secure key distribution between BS and SS. The PKM uses security

associations (SAs) of which there are two types [5]: (a) Data SA specifies the messages encryption algorithm and the keys to be used and related information. Each data SA includes an ID (SAID), an encryption algorithm to protect the confidentiality of messages, traffic-encryption key (TEK), and a TEK identifier, a TEK lifetime, an initialization vector for every TEK, and an indication of the type of data SA (primary or dynamic); (b) Authorization SA includes a credential, an authorization key (AK) to authorize the use of the links, an identifier for the AK, a lifetime for the AK, a key-encryption key (KEK), a downlink hash-based message authentication code(DHMAC),an uplink hash code(UHMAC), and a list of authorized data SAs.

The WiMAX communications follow the security procedure in phases to ensure secure access of a connection [6].

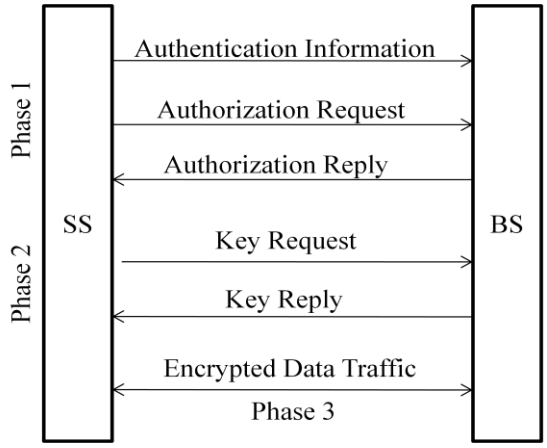

Fig 2: Phases in PKM protocol.

Phase 1 (SS Authentication and Authorization): To establish the genuine identity of the SS wishing to join BS, the SS sends Authentication Information message containing the X.509 certificate to BS. The X.509 is used in the public key cryptography and the digital signatures. The certificate contains information like version, a serial number, the certificate issuer, validity period, public key of SS etcetera. The BS may choose to ignore this message. Then SS sends authorization request to BS. It contains the X.509 certificate, the description of the requesting SS's cryptographic capabilities that SS supports and the SS's Basic CID (connection ID), which is the first static CID assigned by the BS to SS during initial ranging. After receiving this message, BS authorizes the SS via X.509 certificate and sends authorization reply message back containing AK (authorization key), AK sequence number, AK lifetime and SA descriptors.

Phase 2 (TEK exchange): After AK exchange the SS derives three keys. (a)KEK for the encryption of the TEK, that BS sends to each SS. TEKs are used for the data encryption to ensure confidentiality. (b)DHMAC key for derivation of the HMAC digest of the management messages sent by the BS to the SS and the SS uses this key to verify the HMAC Digest of the messages received from BS. (c)UHMAC key for derivation of the HMAC digest of the management messages sent by the SS to the BS and the BS uses this key to verify the HMAC Digest of the messages received from SS. For each SAID, the authenticated SS starts a separate TEK process. The TEK process periodically (TEK's lifetime varies between 30 minutes and 7 days) sends TEK key request messages to the BS, requesting a refresh of keying material. The BS responds to the key request message with a key reply message which contains TEK sequence number, TEK's SAID, the old and new TEK encrypted with KEK and the digest of the message with the UHMAC key.

Phase 3 (Encrypted Data Traffic): After the completion of authorization and initial key exchange, data transmission between the BS and the SS starts by using the TEK for encryption. The data encryption [7] is done based on the TEK length, DES in Cipher Block Chaining (CBC) mode using a 56-bit key with 64-bit block encryption along with the 64-bit IV (initialization vector), AES in CCM mode with 128-bit key and 128-bit block size and AES in CBC mode with 128-bit TEK key and 128-bit block size.

3. SECURITY ISSUES AND SOLUTIONS

3.1 Denial of Service (DoS)

The attacker can easily intercept an authorization request message from a legitimate SS to a BS. Then it replays this message multiple times to the BS, burdening the BS with effect that this declines the legitimate SS. This is a Denial-of-Service attack.

Message 1. SS → BS : Cert(SS.Manufacturer)

Message 2. SS → BS : Cert(SS) | Capabilities | BCID

Message 3. BS → SS : KU_{SS} (AK) | SeqNo | Lifetime | SAIDList

Fig 3: Basic PKM authentication protocol

Solution: In [8], the authors have proposed a solution by adding a timestamps in message 2 of basic PKM authentication protocol (Figure 3), together with a digital signature by SS. The revised protocol is shown be seen in Figure 4.

In Figure 3 and 4, Cert(SS.Manufacturer) is the X.509 certificate of SS's manufacture, Cert(SS) is SS's X.509 certificate, BCID of SS equals its primary SAID. KU_{SS}(AK) is the Authorization key encrypted by public key of SS. Lifetime and SeqNo are the lifetime and a sequence number for the AK. SAIDList describes the identities and the properties of the SAs. $T_{S \text{ and }} T_B$ are the timestamps of SS and BS respectively. $SIG_{SS}(2)$ and $SIG_{BS}(3)$ are the signatures of SS over message 2 and BS over message 3 respectively. By adding the timestamps and signatures, freshness can be guaranteed for both messages. By adding Cert(BS), mutual authentication is achieved which prevents replay attack from malicious BS. Thus, both the SS and the BS know that the message is fresh and not replayed.

Message 1. SS → BS : Cert(SS.Manufacturer)

Message 2. SS → BS : T_S | Cert(SS) | Capabilities | SAID | SIG_{SS} (2)

Message 3. BS → SS : T_S | T_B | KU_{SS} (AK) | Lifetime | SeqNo | SAIDList | Cert (BS) | SIG_{BS} (3)

Fig 4: Revised authentication protocol [8]

The IEEE 802.16e proposes PKMv2 authentication protocol, in which one additional message is added at the end of the PKMv1 protocol as shown in Figure 5. It is a 3-way authentication protocol, with a confirmation message from SS to BS. SSID is SS's identifier from Cert(SS); AAID is the ID of Authorized Association (AA); SSAddr is the ID of SS. PKMv2 is based on alternating nonce. The addition of a nonce assures SS that the subsequent message is the reply to its request.

Message 1. SS → BS : Cert(SS.Manufacturer)

Message 2. SS → BS : N_S | Cert(SS) | Capabilities | BCID

Message 3. BS → SS : N_S | N_B | KU_{SS} (PAK, SSID) |
Lifetime | SeqNo | SAIDList | AAID | Cert (BS) | SIG_{BS} (3)

Message 4. SS → BS : N_B | SSAddr | EAK(N_B, SSAddr)

Fig 5: PKMv2 Authentication Protocol

Without the signature by SS, the message 2 is vulnerable to replay attack. Even with the signature from SS which serve as message authentication, the interleaving attack still exists. In this type of attack, the intruder stands in between the SS and the BS, impersonating itself as a SS to the BS and vice versa. The intruder uses SS as an oracle to answer the nonce challenges.

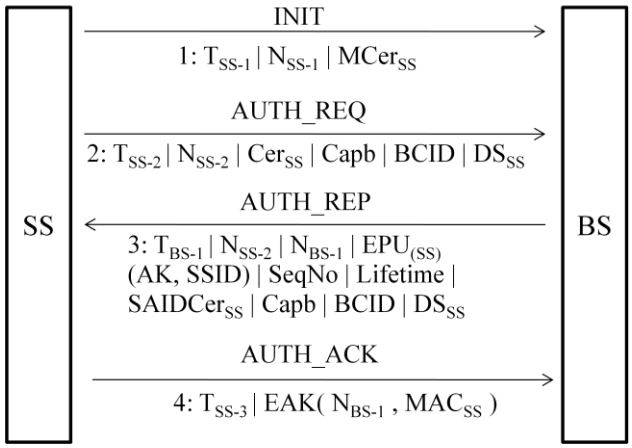

Fig 6: ISNAP [9]

Therefore, the author in [9] proposed a model called Improved Secure Network Authentication Protocol (ISNAP) shown in Figure 6.

The ISNAP authentication protocol is an extension of the hybrid approach using timestamps together with nonce. The message 1 consists of timestamp (T_{SS-1}), nonce (N_{SS-1}) and $MCer_{SS}$. BS receives the INIT (initialization) message and calculates the trip time as:

$$T_{PROP-1} = T_{PRESENT} - T_{SS-1}$$

where $T_{PRESENT}$ is the time at which INIT is received. Following INIT message, the AUTH_REQ (authorization request) and AUTH_REP (authorization reply) messages are exchanged between SS and BS with validation of their respective credentials. After receiving AUTH_ACK (authorization acknowledgment) message, BS calculates the second propagation delay (T_{PROP-2}) as:

$$T_{PROP-2} = T_{PRESENT} - T_{SS-3}$$

If the whole authentication process took place without any external intrusion under optimal environmental conditions, then:

$$|T_{PROP-1} - T_{PROP-2}| \leq \gamma$$

where γ is the auxiliary parameter introduced to consider the fluctuations in propagation time which occurs due to environmental and multi-path effects [9]. The value of γ must not exceed 3% of the total propagation time (T_{PROP-1} or T_{PROP-2}), based on empirical analysis considering a Quasi-static Rayleigh Channel. The ISNAP model is robust against the replay attack, DoS attack, interleaving attack, multiplicity attack and man-in –the-middle attack.

In [10], the authors have proposed a technique to counter DoS attacks that uses visual authentication principles. In this proposed technique, the SS has to qualify pre-authentication process based on visual authentication principles before it is considered for the authentication process. This technique considers that the subject unique identifier attribute of the digital X.509 certificate is mandatory. The value of this attribute is the binary images shared between the SS and BS and registered with Trusted Third Party (TTP) server. With the help of TTP server, both the SS and the BS validate each other. If an SS fails the pre-authentication process, the BS does not have to process authorization, this saves the computational power and resources. If the identity of the SS is validated, the BS continues with the regular authentication process. This pre-authentication technique provides an effective means to counter DoS attacks.

A neural network based authentication method has been suggested for the generation of secret key keys in [11], which is based on synchronization of the neural network by mutual learning. The secret key generation process is triggered by the competition between stochastic attractive and repulsive forces which act on the weights of the two neural networks. These dynamical systems, synchronized by mutual signals, can prevent the attack as an attacker can only listen to exchanged signals and cannot influence the dynamics of the weights of two nodes' neural networks. Finally the key is securely established as the synchronized weights of the two networks. This technique is effective for generating shared secret key and requires major amendments in the standard.

3.2 Key Space Vulnerability

In 802.16e, 4-bit key and 2-bit key sequence numbers are used to distinguish between successive generations of AKs and TEKs respectively. The key reply message sent by BS contains the sequence number as a part of the TEK parameters. The standard treats the 2-bit key sequence number as a circular buffer, allowing an attacker to interject reused TEKs [12]. An attacker can capture key exchange messages and replay them to gain information needed and decrypt the data traffic.

Solution: As proposed in [13], the problem can easily be solved by increasing the number of bits for both keys. As a result, keys can be generated and used for long validity duration securely. The size of sequence number can be increased to 8 bits. This increase in size may lead to trade off with the performance. This

solution requires amendments in the standard encryption and decryption algorithms.

3.3 Downgrade Attack

In the authorization phase, the authorization request message sent by the SS to BS is an unsecured message which describes the security capabilities required by SS. To make the encrypted communication between BS and attacked SS vulnerable, an attacker can send a spoofed message to BS containing weaker capabilities.

Solution: As proposed in [13], a possible solution for downgrade attack is that the BS could ignore messages with security capabilities under a certain limit. But this solution can lead to DoS for SSs that have low required cryptographic capabilities.

3.4 Cryptographic Algorithm Computational Efficiency

In the authorization phase, the standard model uses RSA encryption algorithm for encryption which is having a key size of 1024 bits. But RSA is less efficient than ECC as it uses stronger keys (1024 bits) at more cost and ECC is much faster than RSA.

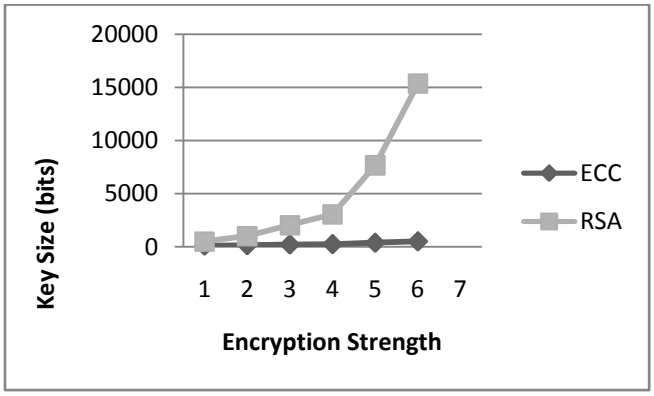

Fig 7: Key Size vs. Encryption Strength of RSA and ECC [15]

Solution: The RSA-based public key cryptography can be replaced with ECC as it is more efficient [14, 15]. ECC can provide the same level of security as RSA with smaller key sizes. For example, 160-bit ECC provides comparable security to 1024-bit RSA. ECC provides faster computational efficiency. Since ECC key size is relatively smaller than RSA key size, thus encrypted message in ECC is smaller, energy and bandwidth efficient. Figure 7 provides additional information to describe the security level desired.

3.5 Initial Network Entry Vulnerability

The initial network entry process is the first step to establish a connection to Mobile WiMAX. When SS first tries to join WiMAX network, it sends a Ranging Request (RNG-REQ). BS sends a Ranging Response (RNG-RSP) to SS to change Timing, Power Level, Offset Frequency, Ranging Status, and other Ranging parameters. The attacker can intercept this RNG-RSP message and send the spoofed RNG-RSP message by setting the RANGING_STATUS value to 2 which means "abort". This leads to a DoS attack.

Solution: To resolve this problem, [16] applies Diffie-Hellman (DH) key agreement scheme to initial ranging procedure as shown in figure 8. DH key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel with global variables known as prime number 'p' and 'q' a primitive root of 'p'. After choosing ranging code, SS generates 'p' and 'q'. Then SS sends the global variables along with the ranging code to the BS. After verifying the received key and variables, BS also sends its public key to SS. If the received key and variables are verified, BS also sends its public key to SS. Thus, BS and SS can share global variables and public key with which they generate secret key and establish secret communication channels. However the original DH key exchange protocol cannot prevent man-in-the-middle attacks [17] since it provides no identity authentication.

To resist man-in-the-middle attacks in this procedure, the authors in [17] have enhanced the DH key exchange protocol by introducing identity authentication. In [17], the author assumes that every SS has its own International Subscriber Station Identity (ISSI) and using this ISSI, SS can generate Temporary Subscriber Station Identity (TSSI). This TSSI is used as SS's identity. The author also assumes that legitimate BS has the hash value, H(TSSI). The author uses H(TSSI) as an input parameter of hash authentication function instead of direct usage of TSSI, because in certain situation, one of the legitimate BSs may be captured by attackers, storing H(TSSI) in BS prevents attackers to achieve the SS's TSSI. In this protocol, along with the DH key exchange, the SS and BS sends the challenge to each other. The BS sends a challenge R_{BS} to SS, in turn SS generates hash value using cascade of H(TSSI), R_{BS} and its public key PK_{SS} as input. This Hash value is send to BS along with its public key PK_{SS} and challenge R_{BS}. Then, the BS calculates the hash value using same inputs and compares it with the SS's response to check identity of SS. If SS is legitimate, BS calculates hash value using the cascade of H(TSSI), R_{SS} and its public key PK_{BS} as input and sends it to SS. The SS checks BS's identity using the response that it receives, if the BS is legitimate, the shared key is established and SS continues to communicate with BS; otherwise, SS ceases the communication. The secure initial network entry is shown in Figure 9.

4. CONCLUSIONS & FUTURE WORKS

4.1 Conclusion

This paper described the security mechanisms present in the WiMAX. Then it described the different security issues in PKM protocol and the various solutions proposed in literature. The table 1 gives the brief analysis of the different proposed solutions. The authors in [8, 9, 10, 11] solve the DoS/Reply attacks. They require a reasonable modification to the standards. In [9], computing and analyzing the value of γ increases the complexity. Although [10] counters DoS effectively, it has increased the number of message exchanged thus affecting the performance. In [11], the authors proposed completely new protocol for authentication and authorization process which requires complete modification to the standard. In [13], the author solves the key space vulnerability issue. However experiments are needed to validate the behaviour and performance of this solution. Also, the author [13] solves the downgrade attack but it may create another issue, so this solution cannot be considered to operate satisfactorily. The

author in [14] described that ECC is better than RSA but are inappropriate from the point of authentication and authorization improvement. In [16, 17], the authors solve the initial network entry vulnerability issue but still it is prone to other attacks. These solutions can be further enhanced to develop a robust WiMAX network.

4.2 Future Works

In future, the listed solutions need to be implemented and tested to improve their performance and scalability. More research is required for achieving high performance and security in WiMAX network.

5. REFERENCES

[1] IEEE 802.16-2004. IEEE standard for Local and Metropolitan Area networks-Part 16: Air Interface for Fixed Broadband Wireless Access Systems. IEEE Press.

[2] IEEE 802.16-2005, IEEE standard for Local and Metropolitan Area networks- Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. IEEE Press.

[3] Ahson, S. and Ilyas, M. 2008. WiMAX: Standards and Security: CRC Press, Inc. Boca Raton, FL, USA.

[4] Hasan, J. 2006. Security Issues of IEEE 802.16 (WiMAX). In School of Computer and Information Science, Edith Cowan University, Australia.

[5] Eren, E. 2007. WiMAX Security Architecture - Analysis and Assessment. In 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. IDAACS 2007, pp. 673-677.

[6] Panagiotis, T. and George, G. 2010. WiFi and WiMAX Secure Deployments," Journal of Computer Systems, Networks, and Communications, vol. 2010.

[7] Luo, C. 2009. A Simple Encryption Scheme Based on WiMAX. In International Conference on E-Business and Information System Security, 2009. EBISS '09. pp. 1-4.

[8] Xu, S., Matthews, M. and Huang, C. 2006. Security issues in privacy and key management protocols of IEEE 802.16. In 44th Annual South-east regional conference, Melbourne, Florida. pp. 113-118.

[9] Hashmi, R.M., Siddiqui, A.M., Jabeen, M., Shehzad, K., Zubair, A., and Alimgeer, K.S. 2009. Improved Secure Network Authentication Protocol (ISNAP) for IEEE 802.16. In Information and Communication Technologies, 2009. ICICT '09. Doha, Qatar. pp.101-105.

[10] Altaf, A., Sirhindi, R., and Ahmed, A. 2008. A Novel Approach against DoS Attacks in WiMAX Authentication using Visual Cryptography, In Proc. of Int'l conference on Emerging Security Information, System and Technologies, Securware, France

[11] Dong, H., and Yan, W. 2008. Secure Authentication on WiMAX with Neural Cryptography. In International Conference on Information Security and Assurance, 2008. ISA 2008, pp. 366-369**.**

[12] Yang, Y., and Li, R. 2009. Toward Wimax Security. In Proceedings of Computational Intelligence and Software Engineering, Wuhan, China, pp. 1-5.

[13] Sikkens, B., 2008. Security Issues and Proposed Solutions Concerning Authentication and Authorization for WiMAX. In Proceedings of 8th Twente Student Confereence on IT, Enschede.

[14] Liu, F., and Lu, L. 2006. A WPKI-based Security Mechanism for IEEE 802.16e. In Proc. of Int'l Conference on WirelessComm., Networking and Mobile Computing, pp. 1–4.

[15] Habib, M., Mehmood, T., Ullah, F., and Ibrahim, M. 2009. Performance of WiMAX Security Algorithm (The Comparative Study of RSA Encryption Algorithm with ECC Encryption Algorithm). In Proc. of International Conference on Computer Technology and Development. ICCTD '09, Kota Kinabalu, Malaysia, pp. 108-112.

[16] Shon, T., and Choi, W. 2007. An analysis of mobile WiMAX security: vulnerabilities and solutions. In Proc. of the 1st International Conference on Network-based information systems, Regensburg, Germany, pp. 88-97.

[17] Han, T., Zhang, N., Liu, K., and Tang, B. 2008. Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions. In Proc. of 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems,'08. Atlanta, GA, pp. 828 - 833.

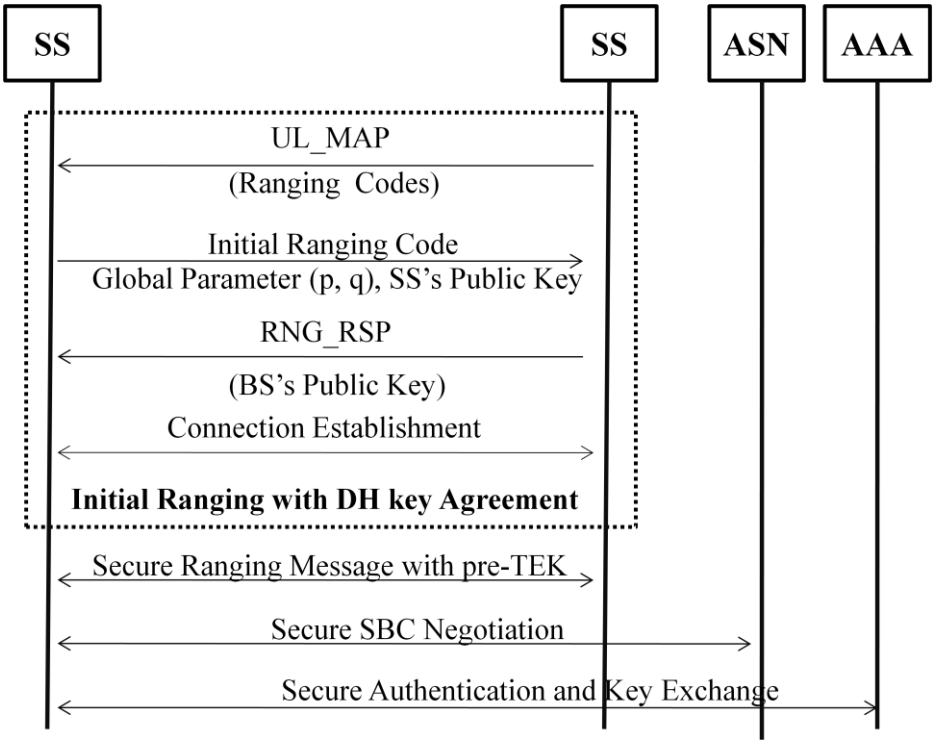

Fig 8: Initial Network Entry with DH Key Agreement [16]

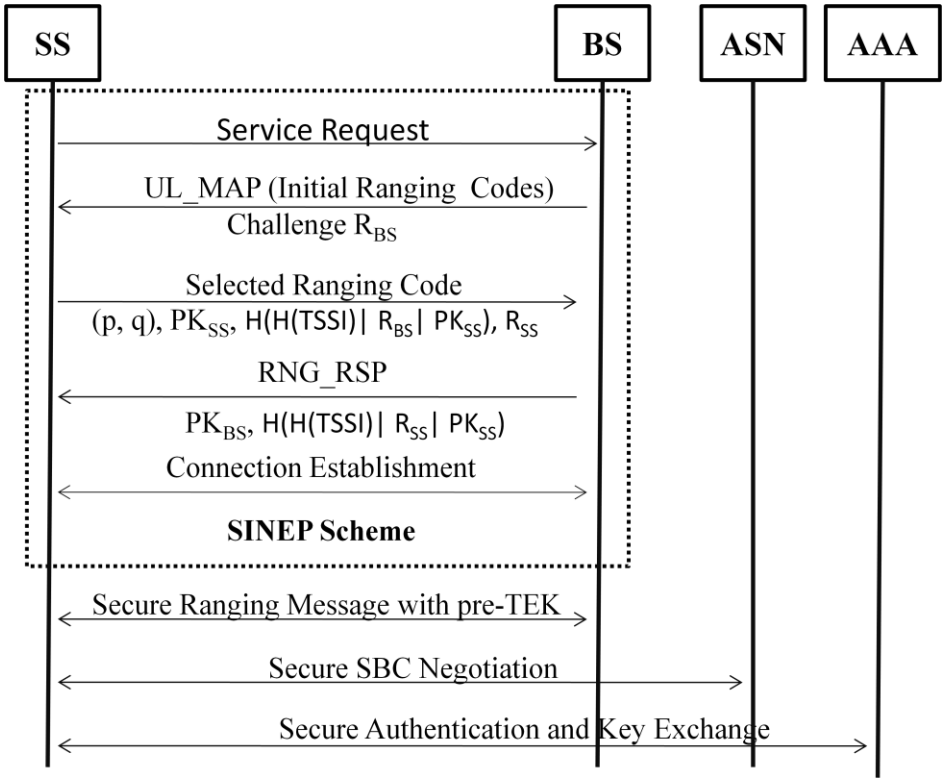

Fig 9: SINEP Scheme [17]

Table 1. Analysis of Solutions

S. No.	Solution	Issue addressed	Advantages	Disadvantages
1.	Nonce [8]	Denial-of-Service	synchronization not required	unable to check the freshness of the message
2.	Timestamp [8]		prevents simple replay attack.	requires the time synchronization
3.	timestamp together with nonce [9]		prevents interleaving attack.	difficult to consider the value of γ
4.	Visual cryptography for pre-authentication [10]		successfully avoids the request from rogue SS	increases the computational overhead by introducing TTP server
5.	Neural cryptography [11]		very secure key exchange	requires complete change in the authentication standards
6.	increase the size of key space [13]	Key Space vulnerability	prevents the circular key space attack	requires modification in the authentication standard and hardware update.
7.	Ignore the cryptographic capabilities beyond certain limit [13]	Downgrade Attack	prevents downgrade attack	vulnerable to DoS
9.	ECC [14,15]	Cryptographic algorithm computational efficiency	ECC requires less key size and computation.	requires modification in the standards.
10.	Diffie-Hellman key exchange [16]	Initial Network Entry	provides key to secure the messages	vulnerable to man-in-the-middle attack
11.	SINEP Scheme [17]		Prevents man-in-the-middle attack	many assumptions and increase in computation cost