


Formal Verification for WiMAX Networks Using Enhanced Security Protocols

Afrizal Zein^{1*}, Julianto Lubis²

¹ Universitas Pamulang, Indoensia, ² Universitas Graha Nusantara, Indonesia

ARTICLE INFO	ABSTRACT
<p>Article history:</p> <p>Received November 22, 2023 Revised November 28, 2023 Accepted December 25, 2023</p> <hr/> <p>Keywords:</p> <p>WiMAX Security Property Protocol Verification Formal Model</p>	<p>This study discusses the formal verification of the Worldwide Interoperability for Microwave Access (WiMAX) security protocol. WiMAX security specifications are defined as a security property that must be met by the protocol in a WiMAX network. The security properties that must be met include pseudonymity, information confidentiality, anti-tapping and session key secrecy.</p> <p>Several studies have found several failures to comply with the security properties set by the WiMAX IEEE 802.16-2004 and IEEE 802.16e-2005 standards. Some of the attacks that can occur include jamming, scrambling, DoS attacks, replay attacks, modification of management messages, downgrade attacks, interleaving attacks and other types of security attacks. From some of these attacks there are several solutions to improve security protocols to overcome these attacks so that they can comply with security protocols.</p> <p>Proof of security protocols in the ability to fulfill security properties can be done either formally or informally. The security protocol operational semantic model framework developed by Cas Cremers and Sjouke Mauw is used to carry out formal verification of proposed improvements to the authentication protocol and Privacy and Key Management (PKM) protocol.</p> <p>Modeling the proposed protocol with an operational semantic framework has been able to prove the proposed improvement of the authentication protocol and PKM by using timestamps, SS/BS identity encryption and adding digital signatures or message digest values to ensure authentication is able to meet the specified security properties.</p> <p><i>This is an open access article under the CC BY-NC license.</i></p> 

Corresponding Author:

Afrizal Zein,
Universitas Pamulang,
Jl.Surya Kencana No.1, Pamulang, 15417.
Email: dosen01495@unpam.ac.id

1. INTRODUCTION

The Wireless Metropolitan Area Network (Wireless MAN) interface is defined by the IEEE 802.16 standard, which provides high transmission rates and wide bandwidth. WiMAX, a forum that supports the IEEE 802.16 standard, also known as IEEE 802.16. IEEE 802.16 is divided into three parts: the privacy sublayer, the commons sublayer, and the convergence sublayer, all of which make up the MAC layer. Privacy and Key Management Protocol Version 1 (PKMv1) is used by the privacy sublayer to securely authenticate

and distribute session key information from the authenticator (BS) to the requester (SS). In IEEE 802.16, Privacy and Key Management Protocol provides one way authentication, where BS authenticates SS using X.509 certificate from SS. This information is discussed further in paper [4], The authors improved the PKMV1 authentication protocol using random numbers, where SS authenticates BS and BS authenticates SS. S. Xu, M. Matthews, and C. T. Huang also analyzed PKMV1 and its nonce versions; they proposed a solution using [5] timestamps. Amendments to IEEE 802.16e[3] add mobility to IEEE 802.16. IEEE 802.16e defines the PKMV2 protocol by providing mutual authentication between the SS and the BS. Paper [5][6][7][8][9] publishes an attack on PKMV2 and proposes a solution.

Data security is absolutely necessary for telecommunication networks, especially wireless communication networks included in WiMAX. That's because the possibility of attack on a wireless network is more when compared to a wired network. Wireless networks have several security requirements, including being able to authenticate, namely verifying identity and checking resource access, confidentiality, namely ensuring that only those with authority can access information, and integrity, namely the ability to guarantee that information has not been changed by third parties. other.

Wireless networks have the possibility of various attacks including insertion attacks such as the presence of clients or access points (access points) that do not have authority, interception and unauthorized monitoring such as packet analysis and access point cloning, brute force attacks to break access point passwords and attacks on encryption such as attacks on the encryption method. In WiMAX there are several possible attacks, namely attacks on the physical layer level such as jamming and scrambling and attacks on the MAC layer such as eavesdropping, message modification and DoS (Denial of Service). I-2

WiMAX based on IEEE 802.16 has security standards in the form of authentication, authorization and encryption. The authentication process uses an X.509 digital certificate with an RSA public key then authorization is obtained after the authentication process is successful. WiMAX uses Privacy Key Management (PKM) which is useful for distributing keys from Base Station (BS) to Subscriber Station (SS) in which there is a re-authentication process for a certain period of time. In 802.16-2004, encryption is performed on data using 56-bit DES in Cipher Block Chaining (CBC) mode using keys that change periodically within a certain time.

WiMAX has undergone several evolutions aimed at improving features and performance. Several major evolutions have taken place, namely the IEEE 802.16-2004 standard WiMAX or better known as fixed WiMAX, then the IEEE 802.16e-2005 standard WiMAX or better known as mobile WiMAX and the most recent is the IEEE 802.16j-2009 standard WiMAX with the ability to perform multi-hop relays. From the description of possible attacks that can occur on wireless networks including IEEE 802.16/WiMAX, this thesis will discuss the analysis of various attacks that can be carried out on WiMAX and the design of solutions to overcome these attacks as well as provide formal evidence for some of these solutions. Currently there have been several discussions about WiMAX security. Therefore this thesis focuses on gathering some results analysis and solutions, then prove several proposed solutions, especially on formal authentication protocols and PKM protocols. The formal modeling of the protocol will make it easier to analyze whether the protocol is capable or not capable of fulfilling the specified security properties.

2. RESEARCH METHOD

This research describes various types of risks and design of security solutions that can occur in WiMAX, which is a compilation of various sources that have previously carried out analysis and provided solution designs for each of the risks involved.

2.1 WiMAX Security Needs

A good WiMAX or wireless network architectural design must meet the following security requirements:

1. Authentication, namely WiMAX must have a mechanism that guarantees that the connected device is the device it should be and guarantees the authenticity of the network connected to it and ensures two-way authentication.
2. Authorization, namely WiMAX must have a mechanism to verify that the connected user is a user who has the authority to receive services and ensure Data Integrity, namely WiMAX must be able to use the service.

3. Data integrity, namely WiMAX must be able to guarantee good message management and data messages are still in their original condition and not modified.
4. Confidentiality, namely WiMAX must guarantee the protection of message contents from eavesdroppers during transmission.

By looking at the security needs as mentioned above, the security risk analysis This WiMAX is an analysis to see the various possibilities that cause one or some of these security needs are not met and explain how the attack mechanism can then be used as material for consideration solution to the security problem.

2.2 Attack on WiMAX

Security risk analysis on WiMAX is an analysis of possible attacks that can happen to the 802.16 standard along with how the attack mechanism is happen. This analysis will discuss all the possibilities that can occur both in IEEE 802.16-2004, IEEE 802.16e-2005, IEEE 802.16j-2009 standards.

2.2.1 Attacks on the Physical Layer

The physical layer is the lowest layer which directly interacts with the medium the conductor in the case of a wireless network is air. On medium air wave is used. Therefore this type of attack is a disruptive attack WiMAX band. The attacks that occur on the physical layer are jamming and scrambling.

2.2.2 Denial of Service (DoS)

DoS attack is a condition where the system cannot run its services to a user. DoS can occur due to several factors including :

1. When SS sends too many authorization requests to BS so that the BS will use all the resources to perform calculations for checks whether the SS certificate is valid or invalid. Because of the process consuming all the resources, the BS cannot serve other SS so cause DoS. In this type of attack, the BS cannot serve all the SS want to connect with it. An example of this type of attack with a mechanism like this namely jamming as explained in the previous sub-chapter.
2. When the eavesdropper intercepts the authentication message from SS to BS, then the eavesdropper sends the message repeatedly to the BS that made it BS rejects SS which sends the repeated message causing DoS. In this attack, only the SS that was intercepted was affected by the attack This.

DoS attack occurs when SS performs initialization while entering the network. During SS enters the network, SS scans the downlink channel and performs sync with the downlink. On the downlink channel BS notifies

initialization code range to SS. Then SS selects one of the initialization code ranges and send to BS. After receiving the initialization code range notification from SS,

The BS notifies by sending a ranging response message with a success status. Message The ranging response from BS aims to notify SS not to re-scan so it can save SS power.

At initialization when entering the attack network can be done by modifying ranging response and sets the status to failure so that the SS receives the message it will rescan and send the initialization code range selection again. If

a ranging response message containing this failed message is sent repeatedly, it can cause SS unable to access BS.

Another possible attack is that the attacker retrieves the authentication message from the SS then sends that authentication message many times to BS thus creating BS overwhelmed with the same number of authentication requests over and over again, resulting in BS creating a response with the contents fails causing the SS to be unable to access the BS.

Jamming can be done by including very strong noise, the noise is in the form of garbage data with the same wave frequency as the WiMAX frequency so captured by the receiver and considered as traffic data. The amount of data entered and fixed receiver capabilities thereby reducing channel capacity. With reduced channel capacity, every time there is a valid connection request become unserved anymore, causing Denial of Service (DoS).

Scrambling is a kind of jamming that is done in a short time and attack a certain frame. Scrambling is easy to do for Frequency Division Duplex (FDD) where the uplink and downlink transmissions are carried out at the same time, the frequency varies different. Scrambling is difficult for Time Division Duplex (TDD) where

each packet sent according to a certain time slot. Jamming and scrambling can occur for all kinds of WiMAX variants.

2.2.3 Authorization Message Modification

WiMAX emphasizes mutual authentication to protect against attacks from data falsification (forgery attack) that is by using HMAC. Will but on the authentication protocol is not a message integrity guarantee so someone with the right radio receiver can capture the authorization message then can modify and retransmit the message. On the authorization protocol on IEEE 802.16-2004 no there is a mechanism to prove that the authorization message has not been modified by other parties.

2.2.4 Attacks on Key Management

To distinguish active and inactive AK can be done by using 2 sequence number bits, these conditions are not sufficient to keep AK confidential because AK's long lifetime and very few possible identifiers. Number The sequence can form 4 possible sequence number values, namely 0, 1, 2 and 3. The size of the key is not sufficient to keep TEK as it is by entering a number sequence 3 becomes 0 on every fourth possible repetition of the key replay attack occurs by reusing TEK.

2.2.5 Downgrade Attack

In the authorization protocol, the first time the SS sends a message to the BS. The message is wrong one of which contains information to the BS about the security capabilities of the SS. Attacker in this case it sends a message to the BS containing the security capabilities of that BS weaker than the SS's actual abilities. With the sending of messages from the attacker's BS will provide a low standard of security according to attacker requests thus lowering the security strength between SS and BS.

2.2.6 Interleaving Attack on PKMv2

The interleaving attack mechanism in accordance with Figure 3.1 shows the attack against PKMv2 which allows attackers to break into the BS network or SS will enter the attacker's network. Steps of the attack is initiated by the intruder pretend as SS and carry out steps $\alpha.1$, $\alpha.2$. After executing $\alpha.2$ intruders only get Pre-AK. Because the intruder doesn't have an AK, then the third message to complete the entire authentication process has not been carried out, then the intruder by way pretend to be BS do steps $\beta.1$, $\beta.2$, $\beta.3$. This step is for get the message on $\beta.3$ in which there is a message encrypted with use A.K. From this operation the intruder then forwards the message $\beta.3$ containing the third message authenticates to the original BS (as message $\alpha.3$ in Figure 3.1). With this authentication process successfully executed intruder.

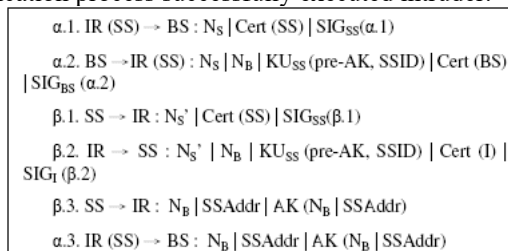


Figure 2.1 Interleaving Attack on the PKMv2 Authentication Protocol

2.2.7 Use of Large Encryption Keys

The standard algorithm used in 802.16e is RSA which uses the same key large and the certificate used is X.509. The problem that occurs is the need very large resource. Because it needs an encryption algorithm that has a need resources for computing that are not too large so that they can maintain performance WiMAX.

2.2.8 Encryption Key Interception

The encryption key on the WiMAX security mechanism is sent in one message so that if the KEK is known or the key management encryption algorithm can be uncovered then the encryption key can be easily identified by an attacker.

3. RESULTS AND DISCUSSIONS

This chapter will discuss a formal model of solution design to address the DoS problem has been discussed in chapter 3. The reason for choosing this DoS case is because in this case there is problem that includes several other problems such as attacks on message modification authorization, downgrade attack. Because of that, this DoS problem solution can also be used for solutions to the problems covered therein. In the case of DoS, proposed solutions are carried out by modifying the authentication protocol and PKM protocol. In this chapter, discussion done by defining the security properties that must be met, then model each of those security properties with a formal model and perform verification using the formal semantics of security protocols to prove whether the proposed security protocol meets the specified security properties defined.

3.1 Security Protocols and Properties

A security protocol is a procedure in the form of a sequential operation that guarantees data protection used in communication protocols. Some examples of protocols security such as Secure Socket Layer (SSL), IPSec, HTTPS, and all protocols cryptography. The purpose of a security protocol is to guarantee the security properties of the system such as authentication, key exchange, key distribution, anti-denial, authentication, message integrity, message confidentiality and anonymity. such security can be done by creating a session key between the communicating parties, authentication agents and nodes, guarantee confidentiality, integrity, and other security properties. Security properties are general properties that must be met by a security protocol so that defined security can be guaranteed. A security protocol so to speak safe or unsafe by seeing whether the security protocol is in compliance or does not meet the safety property. Because it becomes very important for specifies the security properties precisely to meet the safety standards of possibility of attack. Security properties in general must guarantee safety and liveness.

Safety is a property that defines that something bad must not be happen and a liveness property that defines something that is desired to happen.

Examples of some security properties eg confidentiality property where as an example the intruder cannot deduce anything from the conversation between the two points communicate. With that property, a security protocol can be defined is said to be secure if it satisfies the defined confidentiality property.

3.2 Formal Modeling

This section will explain how to model an abstract system built with using formal models. The general architecture of the system to be modeled can be seen in Figure 3.1

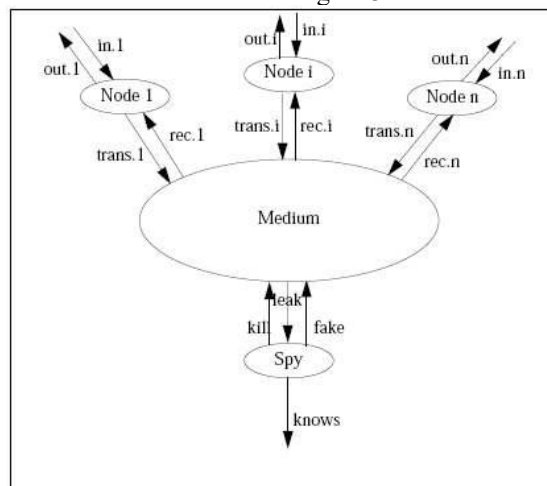


Figure 3.1 General System Architecture

In Figure 3.1 illustrates the specifications of the protocol where each agent is connected with the medium and has input and output channels for communication with other agents. The agent has 2 input and output channels, both medium and external. The protocol specification also defines the type of spy/intruder, namely the type that can perform kill actions, namely removing messages on the medium, leak, namely stealing messages on medium and fake i.e. create a fake message to the medium.

In an architecture there is a message that is something sent on the network. Message can be in the form of plaintext, ciphertext or other types such as nonce, identifier, timestamps and more. Each agent must be able to distinguish between each type of message and can process it. This formal analysis will use a black box approach in the use of cryptographic algorithms. This approach means assuming that Messages encrypted using cryptographic algorithms cannot be read by anyone except the owner of the decryption key. Thus if the message is successful taken by spy will but spy won't be able to read it if it doesn't have the key the description. Medium is something that can send messages and connect with all agents and intruders. The medium will always convey messages from the sending node to the node recipient according to the destination address of the message. However, the spy can perform the action on mediums such as removing messages, eavesdropping/tapping messages i.e. messages will get to the destination but the spy also receives the message, steals the message, namely the message not to the destination but to the spy, re-route that is the spy will change the address the destination of the message as well as the spy can be the man in the middle, namely capturing the message later change its contents and send the modified results to the recipient. By including the WiMAX architecture in the general architecture, the user agent consists of SS and BS with one spy. The medium used is air because WiMAX is a wireless system. In accordance with the proposal in chapter 4 below is message flow that occurs on a WiMAX network.

The authentication protocol is:

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

Message 2: SS BS: Ts | {Cert (SS)}PK(BS) | Capabilities | SAID | SIGSS

Message 3: BS SS: Ts | Tb | {AK}PK(SS) | Lifetime | SeqNo | SAIDList | {Cert(BS)}PK(SS) | SIGBS

In the authentication protocol, the first message is a message from SS to BS which contains a certificate manufacturing, then the second message which is also a message from SS to BS is AK request message containing SS timestamp, SS certificate encrypted with key public BS, SS security capability, SA identifier and SS signature. Third message is a reply message from BS to SS upon AK's request containing the SS timestamp sent on the second message, timestamp BS, AK encrypted with public key SS, lifetime AK, sequence number, list of SAID used in connection and BS certificate which is encrypted with SS public key and BS signature.

In the PKM protocol, namely:

Message 1: BS SS: Tb | SeqNo | SAID | HMAC

Message 2: SS BS: Tb | Ts | SeqNo | SAID | HMAC

Message 3: BS SS: Ts | Tb | SeqNo | SAID | {OldTEK}KEK | {NewTEK}KEK | HMAC

In the PKM protocol the first message is an optional message if the BS wants replace the TEK before the TEK expires. The first message contains the BS timestamp, number sequence, SA identifier and the digest value of the first message to be calculated with using hmac download key. The second message is a message from SS to BS contains the BS timestamp, SS timestamp, sequence number, SAID and the digest value of the second message which is calculated using the hmac upload key. The third message is a message from BS to SS containing SS timestamp, BS timestamp, sequence number, SAID, new TEK and The currently used TEK is encrypted using the KEK and the digest value the third message enumerated using the hmac upload key.

3.3 Formal Definition of Solution Design

In accordance with the proposal to overcome Denial of Service (DoS) caused by replays attack on the BS which consumes BS resources and guarantees message authenticity authorization. In accordance with the proposal to overcome these problems can be done by modifying the authentication protocol and key management protocol. The following is a formal definition of security requirements according to the proposal: 1. Added SS and BS timestamps and SS and BS signatures to the authentication protocol.

The security properties that must be met for the proposal are:

- a. If SS sends m messages, BS must receive m messages (liveness) The formal model for this property is according to the definition of 1L-SYNCH.

$1L-SYNCH(\alpha, k, l, rid1, rid2) \Leftrightarrow \exists i, j \in \mathbb{N}, inst1, inst2 \in Inst, m1, m2 \in MSG.$

$i < j < k \wedge \alpha_i = (inst1, sendl(m1)) \wedge runidof(inst1) = rid1 \wedge \alpha_j = (inst2, readl(m2)) \wedge runidof(inst2) = rid2 \wedge inst1(m1) = inst2(m2)$

- b. BS will only receive message m_1 if SS also sends message m_1 (safety) The formal model of this property conforms to the definition of 1L-SYNCH.
 - c. If the SS sends n messages m then the BS will only receive n messages m (safety and authenticity) The formal definition of this property conforms to the ML-SYNCH definition
2. Added SS and BS timestamps to the key management protocol. The security properties that must be met for the proposal are:
- a. If SS sends m messages, BS must receive m messages (liveness) The formal model of this property corresponds to 1L-SYNCH.
 - b. BS will only receive message m if SS also sends message m (safety) The formal model of this property corresponds to 1L-SYNCH.

3.4 Security Properties

To carry out a solution design analysis, it is necessary to define security properties. Property Security is a requirement that must be met by the system to be installed analysis. Security properties can be defined using the formal claim model (x, secret, y) . The notation means that a role x knows that only he knows the information message y . Here are the security property definitions that must be available:

1. Pseudonymity, meaning if there is an intruder who is observing communication traffic then the intruder can not associate any traffic with an SS certain. To ensure that by looking at the intruder's communication traffic, you cannot connecting it with a certain SS, the MAC address of the SS must be secret. In this case the MAC address is in the SS certificate, hence the SS certificate must be confidential. The formal definition of pseudonymity is:

Property 1: $\{\text{claim}(\text{SS}, \text{secret}, \text{sertifikat SS})\}$

2. Confidentiality of information, meaning that only authorized users can accessing information, all existing data messages on SS and BS traffic are guaranteed secrecy. The formal definition of information confidentiality is:

Property 2: $\forall m \in M \{\text{claim}(\text{BS}|\text{SS}, \text{secret}, m)\}$

That is, for each m element of M which is a message between the SS and the BS can only be known by SS and BS.

3. It is not possible to have wiretapping services, meaning that no unauthenticated users may benefit from the services provided and can trick other users. The formal definition of this third property is the same as the formal definition of the information confidentiality property where only the SS and BS know the contents of the messages exchanged.

Property 3: $\forall m \in M \{\text{claim}(\text{BS}|\text{SS}, \text{secret}, m)\}$

4. The secrecy of the session key means that the session key that is shared between the SS and the BS must be guaranteed confidentiality.

The formal definition of key secrecy is:

Property 4: $\forall \text{key} \{\text{claim}(\text{BS}|\text{SS}, \text{secret}, \text{key})\}$

3.5 Solution Design Analysis

This section is an analysis of the solution design security solutions and explain whether the design the solution meets or does not meet security requirements and security properties. In the solution design analysis, this thesis uses formal semantics of security properties where this framework model can model networks with a model formal and can prove the claims of the modeling. In accordance with the previous explanation, this formal analysis will use the approach black-box in the use of cryptographic algorithms which means encrypted messages will not can be opened by anyone except the holder of the decryption key.

3.6 Analysis of the Application of the Operational Semantic Framework

In this study the operational semantic framework developed in applied in verifying the proposed improvement of the authentication protocol and PKM on WiMAX. Following are the results of the analysis of the application of the framework on the WiMAX protocol:

1. Framework can be used to model protocols according to specifications authentication protocol and PKM on WiMAX with role modeling according to true characteristics. The role modeling here is SS and BS modeling where SS acting as initiator and BS acting as responder

as well as knowledge and functions owned by SS and BS, including intruder role modeling wherein some cases of intruders can act as BS to trick SS or intruders can act as SS tricking BS as well as explicitly describing knowledge possessed by intruders.

2. The framework allows for the definition of security properties as local claims. This local claim means a claim that applies only to the role that defines the claim and claims are viewed from the perspective of the defining role. For example claim(BS, secret, AK) which means that the claim is a confidentiality claim AK seen from BS perspective. This local claim is useful for facilitating the identification of errors or protocol weaknesses so that ultimately it facilitates repair of the protocol because the exact role is known where the error lies.
3. The framework provides facilities for checking confidentiality properties. Model checking is done by looking at all traces on send and read events which is contradicted by the knowledge possessed by the intruder. For example checking claims (BS, secret, AK). So the check is done Checks all send events. Where confidentiality is guaranteed if every event it is certain that it will not add to the intruder's knowledge about AK or with In other words, the intruder cannot learn the undisclosed value, namely AK from all over existing events.
4. The framework has limitations in modeling internal message processing roles. Processing messages on the role in question is processing messages after messages it is in roles. For example: messages can be matched against role knowledge or the message will be ignored (not processed) if it does not match the criteria determined. An example in the case of the first message of the PKM protocol where the first message sending Ts, seqno, SAID, HMAC values sent in plaintext. After sent the message is common knowledge which means that all roles (BS, SS, intruder) can know the message. Ts is the timestamp used by BS to check whether the message is fresh or not. In this case nothing modeling to check the Ts of each message with the existing Ts of BS knowledge.
5. The framework has limitations in modeling digital signatures and authentication digest value so that the proof of integrity and authenticity cannot be modeled. In relation to point 4 where a message contains a digital signature or the digest value cannot be modeled to prove the authenticity and integrity of the message.

4. CONCLUSION

This research on the Formal Verification of the WiMAX Security Protocol provides the following conclusions:

1. Operational semantic framework developed by Cas Cremers and Sjouke Mauw can formally model authentication protocols and PKM protocols where SS acts as initiator and BS acts as complete responder with modeling intruders who can act as SS or BS and exist claims that are local to each agent, namely SS and BS, where the claim is are confidentiality claims and synchronization claims.
2. Solution for DoS caused by replay attack causing BS running out of resources by adding timestamps, digital signatures, values Message digest on the authentication protocol and PKM protocol has been verified formal can comply with standard security properties such as pseudonymity, confidentiality information, anti-tapping and session key secrecy and guaranteed synchronization in exchanging messages between SS and BS which means messages sent and received is a message that can only be made and read by proven parties synchronous and is a trusted agent, in this case SS and BS so that it guarantees protocol free from replay attacks.

REFERENCES

- IEEE 802.16 and WiMax: Broadband Wireless Access for everyone, Intel White Paper (2014)
- IEEE std 802.16e2005: Air interface for fixed broadband wireless access system amendment: Physical and medium access control layers for combined fixed and mobile operation in licensed bands, IEEE (2016)
- Johnston, D., Walker, J.: Overview of IEEE 802.16 Security. IEEE Security & Privacy (2014)
- Mohammad Zabihi, Ramin Shaghaghi, Mohammad Esmail kalantari, "Improving Security Levels of IEEE 802.16e Authentication By Diffie-Hellman Method," *Wirel. Sens. Netw.*, vol. 02, no. 02, pp. 173–185, 2017, doi: 10.4236/wsn.2010.22023.
- Xu, S., Matthews, M., Huang, C.-T.: Security Issues in Privacy and Key Management Protocols of IEEE 802.16. In: Proceedings of the 44th ACM Southeast Conference (ACMSE 2006) (March 2016)

- Xu, S., Huang, C.T.: Attacks on PKM protocols of IEEE 802.16 and its later versions. In: ISWCS 2016: Proceedings of the 3rd International Symposium on Wireless Communication Systems (2016)
- Tian, H., Pang, L., Wang, Y.: Key management protocol of the IEEE 802.16e. Wuhan University Journal of Natural Sciences 12, (2017)
- Sidharth, S., Sebastian, M.P.: A Revised Secure Authentication Protocol for IEEE 802.16 (e). In: International Conference on Advances in Computer Engineering (2019)
- Yuksel, E.: Analysis of the PKMv2 protocol in IEEE 802.16e 2015 using static analysis. Informatics and Mathematical Modelling (2017)
- Noudjoud Kahya, Nacira Ghoualmi, Pascal Lafourcade, Roumaissa khelf, "Formal Analysis of Key Management in mobile Wimax" Blaise Pascal University, Aubière, France, 2018.