AN IBC AND CERTIFICATE BASED HYBRID APPROACH TO WIMAX SECURITY

BY METE RODOPER

A thesis submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Master of Science

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Prof. Wade Trappe

and approved by

_____

_____

_____

_____

New Brunswick, New Jersey

May, 2010

ABSTRACT OF THE THESIS

An IBC and Certificate Based Hybrid Approach to WiMAX Security

by Mete Rodoper

Thesis Director: Prof. Wade Trappe

WiMAX is a promising technology that provides high data throughput with low delays for various user types and modes of operation. These advantages make WiMAX applicable both for infrastructure purposes and end-client usage. Since WiMAX is presented as a network framework and a last-mile technology, it is believed to be capable of handling a wide range of usage scenarios. For example, while the end users have an opportunity to use WiMAX as the primary connection medium for acquiring services such as on-demand video streaming, VoIP connections and mobile bank transactions, the service providers may use it for data relaying purposes among access points. To meet the technical requirements of these various scenarios, majority of the WiMAX research has been conducted on physical and MAC layers; however little has been invested in a comprehensive and efficient security solution, which has resulted in a wide range of security weaknesses and reactive solutions. Many security problems remain to be addressed in different modes and for different user types even in the final security standard of WiMAX, PKMv2.

In this thesis, we present a hybrid security solution combining Identity-Based Cryptography (IBC) and certificate based approaches to overcome the existing security problems of WiMAX without degrading service quality. IBC has potential benefits that can

provide enhancements to the overall security and efficiency of the security standard. One such enhancement is combining user identity with the public key and therefore eliminating the public key distribution load from the network. However, IBC has a few caveats, such as the necessity of a secure medium to distribute private keys. To compensate for these disadvantages, in this study, IBC is combined with certificate-based security. As a result, the benefits of IBC are maintained while the disadvantages are eliminated.

Using the hybrid approach, this study also aims to clarify the key revocation procedures and key lifetimes of WiMAX. To achieve this goal, key renewal intervals are examined and corresponding lifetimes are assigned to the credentials missing in both PKMv2 and PKMv1. Additionally, the key distribution procedures are investigated and a pattern is provided with the message exchange details.

To be able to correctly assess the efficiency of this approach, a new mobility model is defined in the evaluation chapter of this thesis. Based on this model, the analysis has shown that our hybrid solution that combines IBC and the certified based security scheme results in a significant bandwidth improvement over the standards approach, PKMv2. This work is the first study that unites the advantages of both IBC and the certified-based security scheme for improved security while maintaining low overhead for WiMAX.

Acknowledgements

First of all, I would like to express my gratitude to my adviser Prof. Wade Trappe for his support, encouragement and guidance throughout my MS thesis research. He gave me vision and enough freedom to do research along my interests while making sure that I was always on the right track towards my degree. Starting from the first day of my studies, he constantly guided me and gave me invaluable advices.

I would also like to extend my appreciation and thanks to Prof. Edward Jung, my co-advisor, for our long discussions and his extremely positive contribution to this thesis work. His advices and the quality time we spent will influence my vision throughout my life.

Additionally, I would like to thank Prof. Dipankar Raychaudhuri and Prof. Narayan Mandayam for participating my thesis committee, and for the invaluable comments and insights. I am very thankful to the many friends and office mates I have known in WINLAB as well.

I would also like to express my appreciation to my dear roommates Eyup Akdemir and Basar Karacor who encourage me all the time and make my life in the United States enjoyable. Also, I want to thank to my precious friends Anil, Erman, Bahar, Mesut, Marita, Berrak, Merve and Mercedes and my cousin Yalgin for all the support that they gave me.

Last but not least, I want to thank my parents and my brother for their endless love, encouragement and faith in me.

Dedication

To my mom, Leyla Rodoper, and dad, Huseyin Rodoper.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

WiMAX is an important emerging technology in the wireless world due to its potential for solving some of the problems that WiFi and other wireless technologies cannot. Additionally, WiMAX (also known as IEEE802.16 [1]) has many benefits including supporting high data rates with minimum delay and jitter from long distances. This makes WiMAX a viable alternative to conventional wireline networks that support such popular uses as on-demand video streaming, VoIP connections and mobile bank transactions. Besides these last-mile solutions WiMAX is designed as an alternate and a replacement for backhaul networks, where it is inefficient to use wired connection types. Therefore, it is believed that it can serve as the relay network for other wireless networks such as 2G, 3G. Hence, it has a huge potential to be placed both as a last-mile and/or backbone technology. Unfortunately, securing wireless networks faces many challenges. Perhaps the most fundamental of these is the fact that proper security planning for these networks is desperately needed. Like other wireless technologies, WiMAX involves data being broadcast over an open medium (the air), which facilitates many different kind of threats such as eavesdropping and message injection into the network.

A natural line of defense to protect against such attacks is to, first, design the security architecture proper according to the technology requirements and as well as user types and, then, employ cryptographic protocols that support confidentiality and authentication. The WiMAX standard seeks to accomplish these objectives through two proposed security frameworks: PKMv1[1] and PKMv2[2]. PKMv2, the advanced amendment of PKMv1, provided potential solutions for the security of WiMAX. This framework was a part of the IEEE802.16-2001 standard. The flaws identified at PKMv1 -mostly “Stationary Subscribers” related ones- were all fixed by PKMv2, which was the

security section in IEEE802.16e-2005. However, it did not provide full and efficient security coverage for all WiMAX modes of operation and user types and therefore many existing flaws carried on.

One shortcoming of the aforementioned standardized solutions is that they were not completely designed to meet all the needs of this technology. As new features added to the WiMAX, these new solutions are proposed as patches and therefore they were never capable of satisfying the requirements, even they added more complexity and burden. For instance, these security methods are not intended for use in "Mesh Mode" operation. Therefore, it is critical that additional security solutions be developed as effective Mesh Mode operation in WiMAX would allow for low start-up costs and easy network maintenance, all while maintaining signal robustness and reliable service coverage[3]. Additionally, the requirements of different types of users are not fully taken into consideration during the design phase, which is a further drawback of these frameworks. For example, mobile subscriptions need fast and easy correspondence, as well as short and small amount of messages. Even PKMv2 was not able to meet this requirement. As a result of this faulty design approach, existing security methods fail to deliver a complete solution and have introduced a huge resource consumption issue.

In this thesis work, I present a security architecture design that provides a comprehensive solution. This design is a collection of security solutions that use a combination of Identity Based Cryptography (IBC) [4] and Certificate Based Cryptography. The reason of adding IBC to this system is to exploit its unique beneficial efficiency and security enhancing properties that cannot be easily achieved by certificate based systems. Consequently, this work presents the following contributions to the area.

1. Provision of a complete system security for authentication, link establishment and Traffic Encryption Key (TEK) derivation steps for all WiMAX modes of operation and user types.

2. Certification of efficient device and network resource usage while enhancing the connection security level. The bandwidth utilization is maintained at the possible lowest level by decrementing the certification usage without degrading the security

grade.

3. Proposal of a more efficient and complete key revocation procedure compared to the current WiMAX standard, that does not degrades the security and increases the network overhead.

The rest of this work is organized as follows, in Chapter 2, the WiMAX modes of operation, user types and the existing security deficiencies of the IEEE802.16 standard family are explained. In Chapter 3, a high-level explanation of IBC properties and proposed security solution are provided. In Chapter 4, the detailed protocol steps and the reasoning behind the usages of individual credentials are given. In Chapter 5, analysis of hybrid solution will be explained. The related work will be summarized in Chapter 6. Finally, conclusion is presented in Chapter 7.

Chapter 2

WiMAX Architecture and Security Overview

In this chapter, WIMAX system architecture framework and some background information regarding to its security are described, first, by providing an overview of the logical architecture, user types in WiMAX, and the different modes of operation. Then, review and analysis of the security problems of PKMv1 are examined. Finally, the solutions provided to some of these problems by PKMv2 are indicated and the remaining unsolved flaws are enumerated.

2.1 WiMAX Architecture, Entities and Modes of Operation

The WiMAX logical architecture is simple and mainly consists of three hierarchical components as seen in Fig. 2.1. At the top level, there is the *Private Key Generation (PKG)* entity, which is primarily responsible for the generation of security related materials associated with the X.509 Certificate and (in proposed case) IBC parameters. For example, the PKG could be an entity associated with the WiMAX Forum[5]. Moreover, recently WiMAX product vendors can apply WiMAX Forum for X.509 certificate creation for their hardware. Below, the PKG, there are *Service Providers (SPs)* who maintain the basic network infrastructure, such as AAA servers, base stations (BSs) and any other provisions associated with user connectivity to the network. Mainly, SPs are

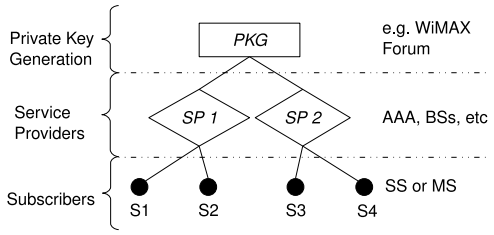


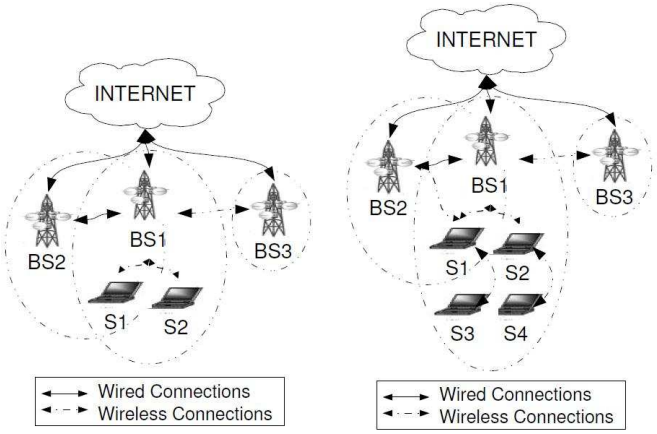
Figure 2.1: WiMAX Logical Architecture

responsible for providing applications to end users or relaying of data as backbones for other kind of communication networks. The SPs are also responsible for security maintenance such as key distribution and revocation from the PKG to the lower layer (or, in proposed case the distribution of IBC private keys). Also, the private key creations for independent sessions are duties of SPs. Finally, at the bottom of the architecture are *Subscribers (S)* who connect to SPs looking for service. Basically, these entities start the association and then follow the message flaw and consequently acquire service.

WiMAX has two subscriber types: *Stationary Subscribers (SSs)* and *Mobile Subscribers (MSs)*. The SSs are the primitive user types and they are defined by the first standard in 2001. These subscribers are fixed to a location and assumed that have continuous connections to power resources -sufficient battery- and enough computation power for complex calculations. Therefore, they do not posses so much complexity to the system and its security. However, the MSs -which were added to the WiMAX standard in 2005- are capable of moving from one point to another at various speeds, which requires a fast link establishment scheme. As MS bandwidth is significantly more limited, they must transmit shorter and fewer messages. Thus, bandwidth efficiency arises as a crucial criteria to be considered for the design of the security system.

Both types of WiMAX subscribers may use one of two modes of operation to get connectivity: *Point to Multi-point (PMP) Mode* and *Mesh Mode*.

The *PMP Mode* is the basic connection mode for WiMAX and was first announced in the IEEE 802.16 standard[1]. As the name PMP implies, there is a central network point (*Base Station (BS)*) that is responsible for establishing a number of one-to-one connections to a multitude of different user points (both types of subscribers). Since BSs have the capability to make multi-links at a time, they can form a mesh network between other BSs. Based on this, the BS itself either acts directly as a gateway to the IP network or forwards subscribers' IP packets to another gateway BS that its connected. On the subscriber side, entities are allowed to make only one connection at a time and this connection has to be with a BS. Therefore, all subscriber data has to go through at least one BS to reach the IP network. There are no MSs involved on the path towards to the IP network. As Fig. 2.2(a) depicts, S1 and S2 are connected



(a) WiMAX PMP Mode (b) WiMAX Mesh Mode

Figure 2.2: WiMAX Modes of Operation

directly to BS1. Even though S1 hears S2, establishing a link among subscribers is not allowed. On the other hand, BS1 can establish many wireless connections to different WiMAX entities, including S1, S2 and BS2.

The *Mesh Mode* is an optional mode added in 2004 by the IEEE802.16-2004[6] standard. It consists of one or more BSs and many subscribers where the interconnection of all these entities form one unique WiMAX mesh network for an SP. BSs act as the skeleton of the mesh network and are surrounded by WiMAX subscribers that are connected to these BSs directly or via other WiMAX subscribers. The role and the functionality of the BSs do not change and they operate same as PMP Mode; act as relay nodes to IP network and supply security credentials to subscribers. Nevertheless, unlike in PMP Mode, Mesh Mode allows subscribers to form multiple links between one another the BSs and/or subscriber. If a node is not able to transmit to the BS directly, then another subscriber may be used for relaying purposes. This relaying subscriber is called a *Sponsor Subscriber (SpS)* and SpS may either be SS or MS. Therefore, the complexity of this mode is much more compared to PMP Mode and involves more detailed design patterns.

For instance, in Fig. 2.2(b), S1 and S2 are connected to BS1, directly. However, S3 and S4 use S1 and S2 respectively as SpSs. Although, both S3 and S4 can hear BS1 directly, this is done to reduce the transmit power consumption in order to elongate battery life. Another advantage is that any subscriber is capable of forming links with

one or more BSs (as exemplified in Fig. 2.2(b), where S1 forms connections with both BS1 and BS2). This not only provides different routes and link reliability but also eases the handover mechanism for Mesh Mode.

2.2 WiMAX Security and the Threats Overview

The primary WiMAX security standard, PKMv1, was adapted from DOCSIS standard[7]. DOCSIS is an international combined standard by the contributioin of many companies. It is intended to provide communications and operation support interface requirements for cable connection systems. However, it was an unsuccessful trial to modify DOCSIS for WiMAX. The main reason for this failure was that DOCSIS was designed for wired networks and thus was not compatible with wireless networks, although the security of DOCSIS is also based on MAC layer security same as WiMAX. Understandably, the application of this standard to WiMAX resulted in numerous security flaws at all three of the security phases of PKMv1: authentication, link establishment and Traffic Encryption Key (TEK) creation. The defects at all phases were pointed out shortly in[8, 9, 10]. Furthermore, after the addition of the Mesh Mode in 2004 to WiMAX standard, PKMv1 was too cumbersome to meet the requirements[11, 12, 13]. Below some of the problems are provided, primarily seen at the authentication phase.

- *Sponsor Node Impersonation Threat* was caused by the lack of mutual authentication. As a result of this defect, malicious unauthenticated subscribers acting as if they are the part of the mesh network, could convince new subscribers to use themselves as the SpSs and decrypt their data. Mesh Mode is especially vulnerable to this attack.

- *Message Replay Threat* was caused by the lack of distinguishing credentials enclosed in messages. As a result of the deficiency of a liveness indicator, any intruder could sniff the valid authentication messages and then replay them to other BSs or SPs.

- *Message Modification Threat* was caused by the lack of integrity providing information concatenated. Therefore, various attacks, such as the alteration of Security Associations, which may lead to either security level degradation or denial of service (DoS), and could be performed by malicious entities.

Besides authentication related security threats, attacks targeting the link establishment and TEK creation phases also exist for both modes and subscriber types. For example, one significant flaw in Mesh Mode is that once an intruder eavesdrops on the mesh network master secret (the Operator Shared Secret (OSS), which is shared by all network entities and used for mesh link and data encryption formation) at the authentication phase, it can form mesh links with neighbors without getting authenticated and become part of the network. Once an intruder establishes a mesh link, it can retrieve a Traffic Encryption Key (TEK) among mesh network pairs and start relaying their data messages. Ultimately, neighbors' data can be decrypted and data confidentiality is compromised.

2.3 Shortcomings of Current WiMAX Standard

The response to the above security warnings were proposed in 2005 by PKMv2[2], which was an advanced version of PKMv1. PKMv2 provides solutions to almost all of the problems identified with the PKMv1 (2001 standard, esp. PMP Mode). Referring to the issues identified above, simply put, the mutual authentication problem was solved by pairwise X.509 certificate exchange by applying different kinds of EAP framework, the message replay threat was solved by adding nonces to management messages and the message modification attack is resolved by concatenating signatures and MAC functions to the end of association and security messages exchanged. However, still, PKMv2 did not address WiMAX Mesh Mode security issues - for example the OSS related thread mentioned in the previous section- and MS relevant concerns. Note that Mesh Mode was proposed merely a year before PKMv2 so standard involvers might not have enough time to prepare PKMv2 fot this mode. In any case, the following enumerated problems still exist in WiMAX and the Mesh Mode and MSs still suffer. The problems are

grouped under two categories: Operator Shared Secret (OSS), Traffic Encryption Key (TEK) related flaws.

1. Operator Shared Secret (OSS) related flaws:

    - Using the same OSS keys among all mesh network entities increases the risk of OSS theft. In case of key compromise, all the TEK keys can be generated and relayed traffic can be decrypted. As a result of the excess OSS usage, the security is put under serious danger.
    - It is unknown when the OSS keys must be renewed in order to prevent compromise. The lifetime is never mentioned in the standard. Besides the key revocation procedure is never touched. Even, during a known attack, prevention by no means is existent and, informing and isolating the other subscribers in a timely manner is impossible.
    - Unencrypted OSS distribution to subscribers during authentication carries a high risk to key compromise and may lead to OSS theft and decryption of all data messages in the network.

2. Traffic Encryption Key (TEK) related flaws:

    - The way of using TEK and the TEK generation parameters are mentioned at the standard, but the TEK formation steps are skipped. Therefore, how to create the TEK is unclear for subscribers.
    - Similar to OSS based renewal thread, superfluous usage problem exists for TEK. Insufficient lifetime and renewal details of TEK may lead to key discovery and therefore data decryption by malicious subscribers.

Furthermore, some of the new generic solutions for WiMAX authentication were subject to criticism because of the ambiguity about the Mesh Mode applicability of PKMv2. For example, the dilemma occurs with the existence of the Authentication Key (AK) used during PMP Mode in the presence Mesh Mode. If AK is used along with OSS, its purpose is unclear. Beyond these postponed Mesh Mode issues, PKMv2

is obviously not taking the requirements of mobile subscribers into consideration, with less communication overhead and timely link formations. Since the overhead loaded by PKMv2 to both the network and subscribers is in essence excess.

Chapter 3

Overview of the IBC and Certificate Based Hybrid WiMAX Security Approach

This chapter of this theses first revises the goals of the hybrid approach, then enlightens the readers about some basic advantages of the used cryptographic techniques. Based on these fundamental knowledge, the steps of the solution is presented. It is important to note that the details of these steps construct the content of the next chapter, therefore the reader in this chapter is merely comprehend the overall framework of the solution. The last part of this chapter is acknowledging in terms of the security credential refreshment and revocation.

Once more it is crucial to state that the three main goals of this proposed hybrid approach are, simply

- To ensure the solution is secure against all types of attacks identified above.
- To boost the speed and efficiency of secure link establishment.
- To propose a complete key revocation procedure that will successfully refresh all the keys.

Once more, to achieve these goals the presented envisioned security system must cover both modes as well as both user types. Messages exchanged at every step must contain all the necessary credentials and the cryptographic techniques should consume minimal amounts of resources. Additionally, a minimal amount of messages are used to increase bandwidth efficiency.

However, the boundaries of what a malicious entity can perform on this security solution must be set. Using the threat model, the remainder of this work will make the following assumptions. A malicious entity can eavesdrop, modify the transmission

and inject new messages into the network. As a result, it can attempt to impersonate a node to form links with neighbors and authenticated subscribers can attempt to form links with malicious nodes. However, once a subscriber gets authenticated securely, it is a completely trusted entity until the next re-authentication. Therefore, none of the authenticated subscribers perform a denial of service or data sniffing while they are acting as SpSs. In short interior attack in this work approach are omitted.

3.1 Exploited Cryptographic Techniques

Meeting all the listed requirements is a difficult task and cannot be achieved easily with the current certificate based framework, PKMv2. Hence, IBC is utilized in this solution to achieve what PKMv2 has failed to accomplish, because by using the unique properties of IBC, the exchanged security messages load less communication overhead to the channels, and security flaws mentioned earlier can be solved with less delay and computation. Therefore, by the combination of IBC and PKMv2, the drawbacks that may exist with any single technique can be minimized and the benefits can be maximized.

Simply put, the main idea of IBC is to use publicly known identity information to derive the public key of a subscriber (For more detailed mathematical information, please refer to Appendix A). This will eliminate the need to bind a subscriber with a public key and the public key distribution problem all together. Based on its mathematical properties, the following are the differentiating benefits of IBC that are being exploited to achieve the goals that are mentioned;

- *Just in-time key generation (on-the-fly):* There is no need for the pre-distribution of keys, which helps us to reduce the number of messages exchanged in order to get the public key of a neighbor node for establishing a link. Since it is easy calculate IBC public keys, it is also possible to change them frequently[14].
- *Pairwise key establishment:* By using the bilinearity and symmetry properties of pairing, pairwise keys can be formed among pairs during link formation simultaneously[4, 15]. Therefore, the number of messages exchanged may be minimized as well as

the network delay.

- *Extensibility:* The ability to encode additional information into the identifier allows us to insert key expiration times inside the IBC Public Key, so the link connectivity of subscribers can be managed precisely and key revocation times easily can be maintained[4, 16].

Besides these significant benefits, the X.509 certificate still has to be used, because IBC also has crucial drawbacks that have to be addressed. One crucial drawback of IBC is the need for subscriber private key distribution from a trusted central authority[14, 16]. The public keys of subscribers can be generated easily while the corresponding private keys are calculated by the SPs using SP IBC parameters and an IBC Secret Key[1], because the IBC Secret Key is not broadcast to subscribers. Therefore, there is a need for a secure private key distribution mechanism. To overcome this problem, the existing hardware embedded WiMAX X.509 certificates are used and IBC private keys encrypted by the RSA public key contained within are distributed.

Another disadvantage of IBC is its impracticality for authentication. Since the private keys do not exist with the subscribers initially, IBC cannot be used as a confirmation tool for trustworthiness. However, WiMAX X.509 certificates can be trusted for authentication purposes (c.f. WiMAX Forum[5]). Furthermore, the PKMv2 authentication for PMP Mode is proven to be safe and can be used with minimal modification. As a result, both disadvantages of IBC can be surmounted by using X.509 certificates without extra burden. Ultimately, all entities (both the BSs and the subscribers) enclose X.509 certificates and IBC key pairs securely.

3.2 Proposed Security Phases and Intermediate Steps

This subsection addresses the phases of the proposed solution and the sub-steps placed under these phases. The details of the sub-steps and message contents will be presented in detail in the next chapter.

[1]Each SP is assigned one unique Secret Key and BSs must keep them confidential to themselves

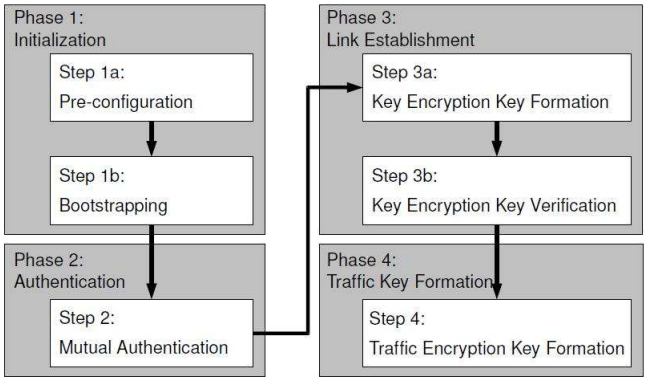


Figure 3.1: Security Phases and Intermediate Steps

3.2.1 Phases of the Framework

PKMv1 and PKMv2 consists of three main phases for both modes of operation and user types: authentication, link establishment and Traffic Encryption Key (TEK) creation. Superficially, authentication as described before done by using certificates and EAP methods. The link establishment is completed by verification of OSS -Mesh Mode- or AK -PMP mode. Finally, the TEK creation is based on the credential exchange, which are encrypted by OSS -Mesh Mode- or derived from AK -PMP Mode.

In addition to these three phases defined in the standard; the proposed solution will contain an additional phase, operated before these three mentioned above. This supplementary phase is called initialization phase for the preparation of keys and certificates. As indicated formerly, since both IBC and certificates are being used, there emerges a preparation duration necessity for the distribution and generation of IBC SP parameters, public keys and certificates. This duration is called initialization Phase in this solution. Therefore, the four phases of this hybrid solution is as follows: initialization, authentication, link establishment and Traffic Encryption Key (TEK) creation.

3.2.2 Steps of the Framework

When the hybrid proposed phases are examined in detail, six intermediate steps can be discerned. Although there are some differences for both modes of operation, it is observed that each phase is formed by these six intermediate steps. As Fig. 3.1 illustrates, *Step 1a* is the distributive step of IBC parameters to SPs and the X.509

certificates to all network entities, including both SPs and subscribers. This step is repeated only once the key revocation becomes necessary (once every couple of years). Following the distribution of the credentials, since SPs have the IBC parameters and secret key, they can prepare their BSs' IBC key pairs. In *Step 1b*, IBC parameters are broadcast from BSs at every beacon period (2.5 to 20ms)[6], so, subscribers are able to create their own IBC Public keys, using the IBC parameters. *Step 2* is the mutual authentication step using X.509 certificates. A 3-way handshake, EAP[17], is performed once new subscribers attemp to join the network and IBC private key is distributed to subscribers by encrypting them with RSA public keys. Consequently, the subscribers have their own IBC pairs ready for the next steps. In *Step 3a* both ends of a connection create a Key Encryption Key (KEK) using the IBC pairing property and IBC keys simultaneously. Importantly, during this step the KEK is created without any message being exchanged between the two ends. Then in *Step 3b*, the formed KEKs are verified by mutually exchanging encrypted timestamps. Lastly, in *Step 4*, the TEK is formed by using a hash function timestamp, exchanged during the KEK verification step. When the key creation order is examined, it can be seen that the IBC parameters form the IBC keys and IBC keys form the KEK.

It should be noted that there is no difference in message content for PMP and Mesh Modes of both user types. However, as a consequence of the Mesh Mode subscribers being capable of forming many links to one or more BSs and neighbors at the same time, creation of KEK and TEK for each individual connection is needed. Based on this observation, a subscriber in Mesh Mode has to repeat Steps 3a, 3b and 4 (see below) for each link. This is the only security message exchange difference between the two modes.

3.3 Proposed Key and Certificate Revocation Procedure

The goals for a successful revocation are to refresh the keys as quick as possible and use minimal resources while maintaining the connectivity. To achieve this, new message schemes and contents for the security approach explained above are designed.

The proposed revocation procedure is divided into two phases: certificate revocation and IBC related credentials' revocation. The reason for this division is the existence possibility of two different Public Key Infrastructures (PKI) for different techniques. The revocation for X.509 certificates is conventional and defined in RFC3280[18]. However, the IBC related credentials' revocation procedure is not simple and, though, there are some application based IBC revocation approaches [19, 20, 21], there is no standardized approach. Therefore, this work proposes a IBC key revocation procedure for WiMAX security.

The IBC related keys those need a renewal procedure are as follows:

1. IBC Secret Key, sent from PKG to the Service Provider along with the IBC parameters
2. IBC key pairs of all network entities
3. Key Encryption Key (KEK) of all pairwise links
4. Traffic Encryption Key (TEK) of all pairwise links

Remember that when key creation order is examined, the first 3 keys are dependent on each other. Whenever the first one changes, the second has to change as well. When second changes, the third must also be renewed. However, a significant point to be noted here is that the TEK does not contain any information either from the IBC keys or KEK. Therefore, in the case of IBC related credentials' revocation or renewal, the TEK by itself does not become affected and stays active. Data connectivity carries on during key revocation and this is one of the advantages of presented design: new credentials and keys from PKG can be distributed to the network entities without discontinuity by encrypting them with the TEK.

Apart from connectivity maintenance, the number of messages exchanged is minimized, so, the procedure is accelerated. Renewal of IBC parameters and Secret Key happens once every few years. IBC public keys are not distributed by a central authority and private keys can be sent in a short message. KEK keys are calculated at

the devices without using any bandwidth, but the KEK verification for each connection needs several message exchanged, which is the source of most of the overhead in the system. Ultimately, considering all the above conditions, there are not many messages exchanged and the process is completed fast. This will be seen in the subsequent chapter.

Besides these advantage, another benefit of IBC is the ability to embed the expiration time of an IBC key to its public key. Consequently, any node would be able to see the expiration time of neighbors' IBC related keys and stop transmitting data. Additionally, it would be easier for a central authority to keep a key revocation list.

Chapter 4

Security Protocols of Proposed Hybrid Security Approach

In this chapter, the security messages in this WiMAX security solution, for both modes and user types, are described. For the rest of the chapter, the notation in Table 4.1 will be used. Also, the following messaging convention is used throughout the remainder of this thesis. All messages are presented according to their order. There are corresponding name abbreviations: *BS* for Base Station, *Subs.* for subscriber, *Entity#* for either BS or subscriber, and * for broadcasting to the network. The message names are given in capital letters, such as MSH-NCFG or AUTH_REP. Last, the message content is given between two square brackets, and "‖" symbol is used for concatenation.

4.1 Step 1a: Pre-configuration

In this step X.509 certificates are acquired for subscribers and BSs. Additionally, the IBC key pairs for BSs are prepared. There are no messages being exchanged between any WiMAX network entities through the air at this step. As per the standard, it is assumed that BSs and subscribers have their own WiMAX X.509 Certificates embedded in their hardware. Besides certificates, it is assumed that BSs obtain SK_{sp} and *param* from the Private Key Generator (PKG) using another secure medium. Following the reception of *param*, BSs calculate their BS_{pub} as follows:

$$\boxed{BS_{pub} = BS_{id} \parallel SP_{id} \parallel TS_1}$$

TS_1 is used as the expiration time of the BS_{pub}. Therefore, before any authentication request from any entity, BSs prepare their own IBC key pair and its expiration time.

Table 4.1: Abbreviations for the Keys and Credentials

Abbreviation	Explanation
BS_{id}, S_{id}	The unique identifiers for the BS and subscriber
SP_{id}	The unique identifier of a Service Provider
BS_{pub}, S_{pub}	The IBC public keys for the BS and subscriber, respectively. Each consists of an unique identifier and an expiration time for the key
BS_{pvt}, S_{pvt}	The IBC private keys for the BS and subscriber, respectively
SK_{sp}, *param*, H_{sp}	The IBC Secret Key (also referred to as IBC Master Key), IBC Domain Parameters and the hash function distributed within the IBC Domain Parameters, respectively. These are shared among the BS
TS_i	The timestamp at time i (Assumed a secure time synchronization method is employed)
$(C^{BS}_{pub}, C^{BS}_{pvt})$	The public RSA key pairs for the BS and subscribers, respectively
$(C^{S}_{pub}, C^{S}_{pvt})$	The private RSA key pairs for the BS and subscribers, respectively
$E_{keytype}$	The cryptographic operation abbreviation. If *keytype* is a *pvt* key, it is a signing operation, else *pub* denotes encryption. For example, $E_{BS_{pvt}}$ is the signature of a BS using its IBC private key and $E_{C^S_{pub}}$ is an encryption by a subscriber using an RSA public key

4.2 Step 1b: Bootstrapping

In this step BSs announce the existence of the WiMAX network to air, and subscribers become aware of active WiMAX networks. Then, subscribers register themselves. Periodic WiMAX beacon messages are broadcast by the BSs. Any new WiMAX subscriber that receives these can identify the network and obtain the necessary information for getting connected to this network. The periodic beacon messages are as follows:

$$\boxed{\text{BS} \Rightarrow * : \text{MSH-NCFG } [\ BS_{pub} \parallel param \parallel TS_1 \parallel E_{BS_{pvt}}(\ param \parallel TS_1\ )\ ]}$$

Here, BS_{pub} and *param* are embedded in the message to support the distribution of the IBC credentials of a WiMAX network to all potentials subscribers. BS_{pub} is also concatenated to the beacon for manipulating the creation of S_{pub}. TS_1 is broadcast to prevent the potential replay attack. Thus, upon receipt of a beacon message, a WiMAX subscriber can create its own S_{pub}, by using the "Just-in-time key generation" property of IBC, as follows:

$$\boxed{S_{pub} = S_{id} \parallel BS_{id} \parallel TS_1}$$

S_{id} is the subscribers' built-in ID. BS_{id} can be extracted from BS_{pub}. Consequently, usage of BS_{id} results in prevention of any malicious node from getting connected to another BS using the same IBC key pair. Note that TS_1 implicitly is used to define the expiration of the IBC key pair.

The first advantage of IBC here is: because the subscribers are able to create their own S_{pub} keys, the communication overhead caused by the distribution of S_{pub} is omitted. The second benefit is that the lifetime of the key, TS_1,is embedded in IBC public key, and, thus, can easily be tracked by all network entities.

The rest of the standard-based bootstrapping message steps for completing the connection are as below. Note that Steps 2-4 are included for compliance with the standard and are outside of the security objectives in this work.

1. BS $\Rightarrow$ * : MSH-NCFG [BS_{pub} $\|$ *param* $\|$ TS_1 $\|$ $E_{BS_{pvt}}$(*param* $\|$ TS_1)]
2. BS $\Leftarrow$ Subs. : MSH-NENT [Net_Entry_Reg.]
3. BS $\Rightarrow$ Subs. : MSH-NCFG [Net_Entry_Open]
4. BS $\Leftarrow$ Subs. : MSH-NENT [Net_Entry_Ack]

Ultimately, after the above bootstrapping messages, both sides have their own IBC Public Keys, with explicit expiration times embedded in the public keys.

4.3 Step 2: Mutual Authentication

In this section, the subscriber and BS mutual authentication procedure are elaborated on. Since the lack of mutual authentication triggers various security flaws, this step is one of the most important steps in the formation of a secure link. The standard's PKMv2 authentication scheme is followed and X.509 certificates are used for proof of subscriber trustworthiness. In addition to the PKMv2 authentication scheme, more functionality is added to PKMv2 for S_{pvt} distribution purposes. Therefore, the network is ready for IBC based cryptographic calculations. The messages exchanged are as follows.

1. BS $\Leftarrow$ Subs. : AUTH_REQ [TS_1 $\|$ $Cert_S$ $\|$ *Capabilities* $\|$ S_{pub} $\|$ $E_{C^S_{pvt}}$ (TS_1 $\|$ $Cert_S$ $\|$ S_{pub})]
2. BS $\Rightarrow$ Subs. : AUTH_REP [TS_1 $\|$ TS_2 $\|$ $Cert_{BS}$ $\|$ $E_{C^S_{pub}}$ (S_{pvt}) $\|$ SAID $\|$ $E_{C^{BS}_{pvt}}$ (TS_1 $\|$ TS_2 $\|$ $Cert_{BS}$ $\|$ $E_{C^S_{pub}}$ (S_{pvt}) $\|$ *SAID*)]
3. BS $\Leftarrow$ Subs. : AUTH_ACK [TS_2 $\|$ $E_{C^S_{pvt}}$(TS_2)]

In the first message, the WiMAX Node sends a request to a potential BS to establish mutual authentication. It sends the TS_1 to eliminate the probability of message replay attack. Then for Node verification, $Cert_S$ is added to the message. The S_{pub} is attached to the message next and sent to the BS to verify S_{id} and receive S_{pvt}. In the AUTH_REP message, the BS sends back the received TS_1, TS_2, and $Cert_{BS}$ for message freshness and BS authentication. The crucial point is that the BS encrypts S_{pvt} with $E_{C^S_{pub}}$ and

sends it to the WiMAX Subscriber. Therefore, during authentication the IBC private key distribution issue is solved using only a couple of bytes. In the last step, the subscriber sends back TS_2 and completes the mutual authentication step.

More importantly, in Mesh Mode, the messages above may be transferred through an authenticated SpS. Therefore, the above notations "Subs. $\Rightarrow$ BS", "Subs. $\Leftarrow$ BS" instead become "Subs. $\Rightarrow$ SpS $\Rightarrow$ BS", "Subs. $\Leftarrow$ SpS $\Leftarrow$ BS", respectively.

4.4 Step 3a: Key Encryption Key Formation

Following the mutual authentication phase between a BS and a new subscriber, the link establishment phase begins. For link establishment purposes, the first intermediate step is to form a secure Key Encryption Key (KEK). The purpose of this key is to verify that both sides of a connection are previously authenticated by the same SP and authorized to make a link. A secondary aim is to exchange timestamps, which will be used for TEK creation in the last phase. This KEK creation step is based on the IBC mathematical properties, specifically the pairing method[4]. Below is the formation of the key for both ends.

Entity1	Entity2
$\Downarrow$	$\Downarrow$
$\hat{e}(H_{sp}(Entity1_{pvt}, Entity2_{pub}))$	$= \hat{e}(H_{sp}(Entity2_{pvt}, Entity1_{pub}))$
	$=$ Key Encryption Key

The above equations are based on the bilinearity and symmetry of the $\hat{e}$ function. Since, it is assumed that the Bilinear Diffie-Hellman Problem is NP-hard to solve[4]; and, since information from both sides of the link is used to form the KEK, this proposed method is more secure compared to WiMAX standards' proposed KEK formation, which is directly created by one side and transferred to the other side. Nevertheless, note that the KEK is created on both sides and have not been compared yet, to see whether they match or not.

4.5 Step 3b: Key Encryption Key Verification

After the KEK creation on both sides of the connection, the next step is proving that both pairs have the same key; but without actually transferring it to the other end. Therefore, no intruder would be able to obtain the KEK by eavesdropping. To verify the KEK keys, the pairs send the HMAC of their public key concatenated with timestamps and with KEK. The timestamps are used for preventing replay attacks.

1. Entity1 $\Rightarrow$ * : MSH-NCFG[a] [$Entity1_{pub}$ $\|$ $param$ $\|$ TS_1 $\|$ $E_{Entity1_{pvt}}$($param$ $\|$ TS_1)]
2. Entity1 $\Leftarrow$ Entity2 : KEK-VER-REQ [$Entity2_{pub}$ $\|$ TS_1 $\|$ $TS_2\|$ H_{KEK} (TS_1 $\|$ TS_2 $\|$ $Entity1_{pub}$) $\|$ $E_{Entity2_{pvt}}$($msgcontent$[b])]
3. Entity1 $\Rightarrow$ Entity2 : KEK-VER-REP [H_{KEK} (TS_1 $\|$ TS_2 $\|$ $Entity2_{pub}$) $\|$ $E_{Entity1_{pvt}}$($msgcontent$[c])]
4. Entity1 $\Leftarrow$ Entity2 : KEK-VER-ACK

[a]The beacon message from an entity is broadcast to whole network. Same beacon message send by any BS at the bootstrapping step. Since, all entities at Mesh Mode may act as a SpS to reach gateway to IP network, they all have their own beacons

[b]$msgcontent$ is "$Entity2_{pub}$ $\|$ TS_1 $\|$ $TS_2\|$ H_{KEK} (TS_1 $\|$ TS_2 $\|$ $Entity1_{pub}$)"

[c]$msgcontent$ is "H_{KEK} (TS_1 $\|$ TS_2 $\|$ $Entity2_{pub}$)"

In the MSH-NCFG message, in other words the "beacon", the Entity1 announces its $Entity1_{pub}$ to the network, so that all of its neighbors know $Entity1_{pub}$. In the next message, when Entity2 wants to form a link with Entity1, it transmits: $Entity2_{pub}$ for identification; timestamps for replaying prevention; the H_{KEK} of the credentials for KEK verification; and, the signature of the content for thwarting message modification. Then Entity1 can verify the message content and if the corresponding KEKs match, it replies back with KEK-VER-REP, which is almost the same as KEK-VER-REQ. Consequently, Entity2 would also be able to verify the KEK by using the same procedure. Last, Entity1 is informed of the completion of the verification procedure and a link is established.

4.6 Step 4: Traffic Encryption Key Formation

The Traffic Encryption Key (TEK) (as sometimes referred to as session key) is used for data encryption between any two network entities. Since the data traffic between any two entities is the most bandwidth consuming operation, the encryption chosen is symmetric encryption. For this reason a symmetric key has to be calculated using the information contributed by the both sides of the connection.

$$H_{KEK}\ (\ TS_1 \parallel TS_2 \parallel Entity1_{pub} \parallel Entity2_{pub}\ ) = \text{TEK}$$

TS_1 and TS_2 are the timestamps exchanged at the step 3b. $Entity1_{pub}$ and $Entity2_{pub}$ are the IBC public keys of both entity. Therefore, without any messages being exchanged the TEK can be calculated. Moreover, TS_2 is assumed to be the formation time of the TEK. As a result, given the key usage duration, expiration time can easily be calculated and whenever "$TS_2 + keyduration$" expires, a new TEK using the active KEK and new timestamps is calculated. The details of revocation is given in the next chapter of this work.

Chapter 5

Certificate and Key Revocation of Proposed Hybrid Security Approach

This chapter gives the details of the certificate and key revocation procedures for this proposed security solution.

5.1 X.509 Certificate Revocation

The initial WiMAX X.509 certificates are issued to the entities during the manufacturing process of the hardware by the only authority that can issue and renew the certificate, the WiMAX Forum. Therefore, in case of revocation, the new X.509 certificates have to approved and distributed by the Forum.

Since a unique trusted authority and the certificate revocation architecture is already presented[22], the standardized approach can be used directly. As a result, the X.509 certificate revocation process does not need any special design requirements and can simply be handled.

5.2 IBC Related Credential Revocation

Now the key revocation procedure for individual IBC related keys is defined. The additional notation in this chapter represented in Table 5.1.

Table 5.1: Additional Abbreviations for the Keys and Credentials

Abbreviation	Explanation
S_{pubnew}, S_{pvtnew}	The new IBC key pair of a subscriber
BS_{pubnew}, BS_{pvtnew}	The new IBC key pair of a BS
E_{TEK}	Symmetric data encryption using TEK
$E_{BS_{pubnew}}$, $E_{BS_{pvtnew}}$	Encryption and signing using the new IBC key pair

5.2.1 IBC Secret Key Revocation

SK_{sp} and *param* are the shared credentials among the BSs of an SP and not released to the subscribers. It is distributed by the PKG by using any secure medium (either wired or wireless) and must be revoked only by the PKG for each trusted domain. Briefly, the IBC Secret Key revocation procedure for a trusted domain takes place between an SP and a PKG. For this SK_{sp} revocation procedure, RSA asymmetric encryption can be used and a new SK_{sp} can be given to trusted domains.

Note that the revocation is not simple. All IBC related keys for the entities are derived from the SP's SK_{sp}. Although subscribers do not acquire SK_{sp}, they obtain the keys extracted from it. As a result, frequent alteration of this key SK_{sp} is not desirable and should be avoided as much as possible. Otherwise, there may occur a network slowdown or collapse, because new IBC key distribution to each entity consumes great significant bandwidth and time. Further, new pairwise link calculations may use significant amount if device resources.

5.2.2 IBC Key Pair Revocation

Each SP maintains an IBC Key Revocation List, thus they know when to revoke entity IBC keys. When the expiration times of the keys approach, two separate revocation procedures are triggered for BSs and subscribers. The BS IBC key pair revocation is simple, because all BSs know the unique SK_{sp} and they can create their own BS_{pvtnew} immediately (matching BS_{pubnew}). However, the case is more complicated for the subscriber IBC keys. Since subscribers are not allowed to know the SK_{sp}, they have to get the new private key from the BSs, through a reliable channel, similar to the authentication case.

To form the secure channel, the active TEK is used. The protocol steps are as follows:

1. Subs. $\Leftarrow$ BS : IBC_REP [$TS_1 \parallel S_{pubnew} \parallel E_{TEK}$ ($TS_1 \parallel S_{pvtnew}$)]

2. Subs. $\Rightarrow$ BS : IBC_ACK [$TS_2 \parallel E_{S_{pvtnew}}$ ($TS_1 \parallel TS_2$)]

In the first message, for prevention of replay attacks timestamps are used. The S_{pubnew} is given in clear to the subscriber; but, the corresponding S_{pvtnew} is encrypted with the active TEK. In response, the subscriber replies back with the latest timestamp,TS_2, and also with a signature, which includes TS_2 and TS_1. Therefore, with simple messages new public and private keys are given to subscribers.

Last but not least, if a node fails to acquire its new IBC Private Key before the expiration time, since its neighbors are aware of the expiration time, they disconnect from the node. Therefore, this node will not be able to stay as a part of the network.

5.2.3 Key Encryption Key (KEK) Revocation

KEK is based on public and private IBC key pairs of both sides of the link, so, its duration is same as the duration of IBC key pairs. When one side renews the IBC key pair, KEK has to be recalculated using bilinear mapping. Ultimately, the process is quite simple and fast. There is no messages broadcast to air, just a pairing calculation on device is necessary.

5.2.4 Traffic Encryption Key (TEK) Revocation

TEK is based on TS_1, TS_2. Its expiration time is also calculated using TS_2, therefore, as long as the expiration time has not been reached, the key is active, whether KEK has been revoked or not. In case KEK is revoked before TEK, the new TEK is calculated using the new KEK. Therefore, only time TEK revoked is when it expires.

The crucial point here to mention is, since TEK's revocation time is not related to IBC Keys or KEK, it does not have to be changed when SK_{sp} of SP, IBC keys or KEK expires. Therefore, when distributing new IBC credentials and X.509 certificates, TEK

encrypted data messages can be used without halting the data transmissions on the network.

Chapter 6

Evaluation

For a complete evaluation of this approach, first, the completeness of the hybrid security approach is assessed by doing a security analysis for each phase and sub-step. Then, for efficiency comparison purposes, two simulations are run and the communication overhead of both the proposed approach and that of PKMv2 are calculated.

6.1 Security Analysis

In this section, a security analysis and comparison between proposed hybrid security solution and that of PKMv2, on the basis of the presented four security phases provided above, are given. Each of the phases is compared with PKMv2's phases.

6.1.1 Initialization

At the beginning of this phase, X.509 certificate and IBC credential distribution are performed by using another secure medium (this work did not intend to solve this issue). Therefore, the risk of any intruder eavesdropping on the X.509 certificates and/or IBC keys and parameters is minimized.

Later, during the bootstrapping section S_{id} is added to the message to protect against subscribers who belong to a different SP from joining unauthenticated ones. Therefore, the use of S_{id} in this framework protects against the threat of authentication violation.

6.1.2 Mutual Authentication

The authentication process defined through this work is based on the trustworthiness of the X.509 certificates and the corresponding public key algorithms (e.g. RSA) being

used. The RSA keys reside inside the certificates, restricting malicious entities from spoofing messages by signing the message. Therefore, the message content is protected against modification and information forgery. Additionally, by verifying the trustworthiness of a relaying subscriber by checking its X.509 certificate, the risk of the *sponsor node impersonation threat* in Mesh Mode is eradicated.

6.1.3 Link Establishment

The approach presented by the standard for link establishment does not provide a complete solution to securing Mesh Mode. To devise a comprehensive method, OSS is eradicated completely and instead the bilinear mapping property of IBC for neighbor authentication is used. As mentioned above, the Bilinear Diffie-Hellman Problem is assumed to be an NP-complete problem[4]. Another advantage of hybrid approach is that the KEK is derived by using information from both ends, as opposed to the cumbersome approach of the standard. Besides KEK creation, KEK verification message exchanges at this solution are more secure because all messages encapsulate timestamps which prevents expired messages from being used in a replay attack because the message content is signed by the sender and concatenated to it.

6.1.4 Traffic Encryption Key Creation

One benefit of this approach is that the TEK is created using a keyed-Hash Message Authentication Code (HMAC); it is therefore easy to calculate the key if the credentials and the "code" (in the proposed case the "code" is the KEK) are known.

Compared to the standard, another advantage of hybrid approach is that it is more explicit and the TEK content is clearly given for both modes of operation. PKMv2 describes the TEK content and creation for PMP Mode. However, formation of the TEK for the Mesh Mode is left undefined. Also, though TEK creation for PMP Mode is clearly explained at PKMv2, ex parte creation and distribution of TEK by the BS still brings out problems. The hybrid approach solves this problem by using the bilinearity property of IBC.

Table 6.1: Sizes of the Items inside the Messages

TS_i	8 B	*param*	50 B[a]
BS_{pub}, S_{pub}	30 B[a]	BS_{pvt}, S_{pvt}	128 B
$Cert_S$	1000 B[a]	H_{MAC}, E_{pvt}	128 B
BS_{id}, S_{id}	4 B	*AK (pre-PAK or MSK)*[b]	32 B
AK_{seq}	0.5 B	OSS	32 B
OSS_{seq}	0.5 B	TEK_{param}	50 B[a]
SAID	4 B[a]	*Capabilities*	50 B[a]

[a]These values are the approximate values based on [2, 6, 16]

[b]These are the keys originally sent from BS to subscribers during authentication for calculating AK at PKMv2

6.2 Performance Analysis

In this part of the evaluation, the communication performance of proposed security scheme is analyzed. The performance here mainly is based on the communication overhead analysis since the needs for storage and computation can easily be met with the help of the rapid progress in software and hardware development. Nevertheless, because of limited bandwidth allocation for individual users, communication overhead is still a crucial issue to be addressed. Thus, here mainly the communication overhead of hybrid approach is analyzed and compared to PKMv2. The reason of not comparing this approach with the previous works (e.g. [11, 12, 13]) is that these works supply simple modifications merely in specific phases and do not provide a comprehensive solution for the aforementioned problems as PKMv2 and the new approach do. Hence, comparison of the previous works with proposed approach is not completely convenient and hold validity.

In order to analyze the communication overhead of the hybrid approach, the sizes and amounts of messages transferred between any two entities starting from the beginning of the first phase to the end of the last phase of security establishments are compared, for both the hybrid approach and those of PKMv2. Additionally, to identify the improvements made by hybrid approach more precisely, the simulation is run on Mesh Mode. As a result, more links will be formed and the implications of new solution will be apparent.

Table 6.2: Sizes of the Messages

Hybrid	Phase1	Pre-Configuration	0 B
		Bootstrapping	216 B
	Phase2	Mutual Authentication	4536 B
	Phase3	KEK Formation	0 B
		KEK Verification	750 B
	Phase4	TEK Formation	0 B
PKMv2	Phase1	Mutual Authentication	2143 B
	Phase2	Link Establishment	256 B
	Phase3	TEK Creation	1364.5 B

To observe the overhead of the individual messages, some constant values for credentials inside the message as shown in Table 6.1 are assigned. Most of these values are collected from [2, 6, 16]. However, for some variable values I was forced to make realistic assumptions. Based on these values, the message sizes of this approach and PKMv2 are calculated the same as in Table 6.2. As can be observed from this table, the hybrid approach adds more overhead in the first two phases compared to PKMv2, until to the end of authentication phase. However, when link formation phases (combination of Phase3 and Phase4 for the new approach, and Phase3 for PKMv2) are compared, the proposed approach uses half the bandwidth that PKMv2 uses. Hence, as a result of repeating the link formation phases many times in Mesh Mode during a network lifetime, the approach apparently outperforms PKMv2.

6.2.1 Mesh Mode Mobility Model

In addition to these messages, a simple mobility model similar to the Random Waypoint model (RWP)[23] is designed for simulating the mobility of subscribers as accurately as possible. Using this model, all subscribers are distributed around a central point (such as BS), but unlike RWP, the subscribers are distributed around this point following a normal distribution, not uniformly since perhaps the subscribers will be denser the closer to the BS. Each iteration of the model subscribers have varying velocities and random directions. Though the probability distributions of the directions are uniformly distribution, the distribution of the speed is normal distribution with a mean zero (negative velocity corresponds to moving in the reverse direction). Consequently, by

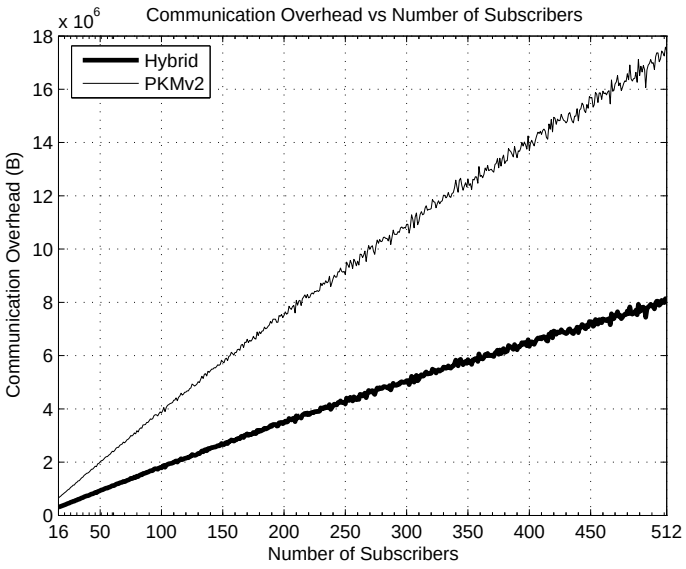


Figure 6.1: Communication Overhead vs Number of Subscribers

using this simple model, more realistic results can be achieved compared to any random movement model.

6.2.2 Simulation Results

Using the message size assignments and model to calculate the efficiency of the new security protocols, the network load in Bytes is measured. The values observed below for the performance evaluation of the experiments are the total amount of Bytes transmitted from one end of communication to other end throughout the simulation iterations. To do this, first the number of subscribers in the network are varied and then, the number of links that an entity can form. In all of the simulation, the results presented are averaged over 10 separate runs.

In the first experiment, 16 to 512 subscribers are used to observe the effect of varying number of subscribers for the new model. It is assumed that nodes had a radio connection range of 100 meters and that each node could form a maximum of 5 links.

As can be seen from Fig. 6.1, as the number of subscribers increases, the proposed approach performs better compared to PKMv2. This is because in parallel to the increase of subscribers the total number of links increases sharply and so does the

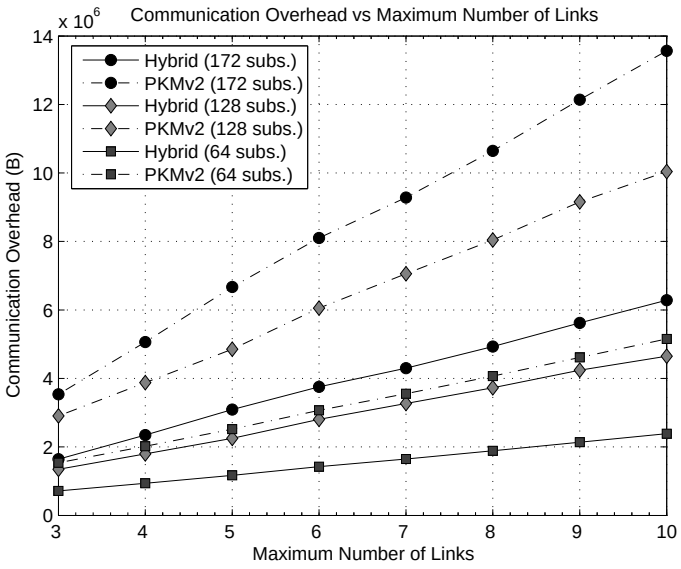


Figure 6.2: Communication Overhead vs Maximum Number of Links

overhead. Since the new approach uses less bandwidth for link establishment it gives superior values for denser networks.

Next, in order to examine the impact of possible number of links that a subscriber can form, the number of links are varied between 3 and 10. Also the number of subscribers in the network are varied from 64 to 128 and then to 172.

As Fig. 6.2 indicates, as the number of links that a subscriber can establish increases, roughly a 53% increase in efficiency compared to PKMv2 is achieved. As the number of subscribers increases from 64 to 172, the performance of hybrid solution does not degrade and maintains dominance over PKMv2. Consequently, the bandwidth usage based on security establishment is reduced by a critical amount. Thus, hybrid proposed solution is also better than PKMv2 in terms of communication overhead.

Chapter 7

Related Work

WiMAX security analysis related papers have been published by many researchers since 2001, right after the publication of the WiMAX standard. Johnston and Walker are the ones who identified the mutual authentication problem for the first time. They also indicated key management failures and data protection errors in[8], though, their approach did not involve many detailed solutions. They preferred to present a few superficial ways to overcome the threads. Some more papers analyzing the authentication flaws, link establishment attacks were also published in recent. For example, [10] concentrated on evaluating the risk level of the threads and analyzed the key formation steps. [24] worked more on describing different kind of attacks and the generic solutions. [9] provided more detailed analysis and additionally introduced some modified message exchange steps. Also, this paper contributed to WiMAX security by adding the nonces to messages for preventing message replay attacks. The key creation order and management were studied in [25] as well. Another paper that is about WiMAX security analysis is [26], which is mostly concentrated on Mesh Mode weaknesses and OSS usage. It also analyzes DES usage in PKMv1.

Apart from publications that analyze the existing problems, some other efforts have been made in proposing new solutions for the existing problems. Xu and Huang identified several existing problems (such as interleaving attack and replay attack), provided countermeasures to these flaws and proposed new protocol steps[27]. Although they eliminate these attacks, their approach introduces significant communication overhead and is short of providing a comprehensive solution to all WiMAX security phases. Zhou and Fang proposed solutions for Mesh Mode of WiMAX for securing the mesh link formation phase and creating secure TEKs[11]. However, new individual mesh

certificates and their distribution to all subscribers decrease the bandwidth usage efficiency critically. Additionally, [12] also presented a synopsis of the Mesh Mode and introduced detailed message exchange steps, which have timestamps and signatures for the prevention of various attacks. They claimed that they provided solutions for man-in-the-middle and replay attacks in an efficient way, but signing all the messages with private keys before sending loads huge computation burden to the subscriber devices. [13] provides message steps for Mesh Mode as well, however, this work is very shallow and does not provide a solution to the whole WiMAX problems. Nevertheless, their approach for end to end security is successful and applicable.

The main paper for Identity Based Cryptography was published by famous Shamir in 1985[4] and the basic concept is introduced to cryptography society. The paper is very simple and many of the details are omitted. Then, until Boneh and Franklin in 2001 published a more detailed IBC work[28], there had not been much done on this cryptography area. After the publication in 2001, this technique obtained a sudden attention and many researchers concentrated on this area. In a couple of years, besides these fundamental IBC papers, some other theoretical IBC papers have been published. Hoeper and Gong proposed a bootstrapping procedure for IBC[20]. Also, [21, 19] provided IBC key refreshing procedures. Since, the main problem for IBC is the distribution of private key in a secure way -by using another secure medium or technology-, the key refreshing works gained enormous attention. Considering the technical IBC research and the publications, it is possible to indicate that there are sufficient cryptographic tools to apply IBC to a real time system or a technology.

Different from these specific cryptographic works, there are a few publications that utilize IBC's terrific benefits and provide a generic architecture for IBC applications. For example, [14, 29] have analyzed the network issues superficially and proposed possible generic security solutions using IBC. Besides these cryptographic studies, IBC is used to address the real world security problems. Some of these applied research works are as follows; [30] applied IBC on VANETs, [31] examined the applicability of IBC on DTNs[32],[33] used IBC for sensor networks security. Lastly, Zhang and Fang have

proposed an IBC security architecture for mesh networks. The proposed network architecture and the authentication steps are very clear[15]. However, the detailed message content does not reside in this paper.

Chapter 8

Concluding Remarks and Future Work

In this thesis, I presented an IBC and certificate based security scheme for WiMAX. The individual security leaks were identified and previous security approaches, standards were examined. Based on these observations the security establishment is divided into phases and sub-steps. The phases are: Initialization, Authentication, Link Establishment, Traffic Key Formation. The sub-steps are: Pre-configuration, Bootstrapping, Mutual Authentication, Key Encryption Key Formation, Key Encryption Key Verification and Traffic Encryption Key Formation. These steps' purposes and their content are presented in detail in individual sections. Unlike to other partial solutions for WiMAX security, proposed hybrid approach proposes a comprehensive solution for both WiMAX modes of operation and for both subscriber types, while maintaining the communication overhead at a minimal level. To achieve these goals, the message content for the security establishment is designed from scratch. In the end, the message framework authenticates entities using X.509 certificates mutually, forms fast and multiple links between entities, and, creates the Traffic Encryption Key (TEK) securely using the timestamps exchanged at the early steps. Also, WiMAX security standard does not provide so much detail in terms of key renewal and revocation, therefore this was increasing the security risks sharply. This work proposes a simple key renewal process as well, which does not halt connections and minimizes the distribution delays. Hence, it is completely efficient and secure.

Moreover, to observe that the proposed message steps -including both security establishment and key renewal processes- utilize less bandwidth compared to the WiMAX standard, PKMv2, in both modes of operation, simulation results are presented in the evaluation part. The realistic results are achieved, first, by developing a new mobility

model, which is a modified RWP mobility model, and, then, by assigning true values to all used credentials reside inside the messages exchanged. The two simulations -one for examining the effect of varying number of subscribers and one for examining the impact of possible number of links that a subscriber can form- show that this hybrid solution achieved 53% bandwidth gain compared to standard approach.

Overall, by looking at these results it can be concluded that this work proves that by using IBC and certificate based hybrid security approach, it is possible to achieve a more comprehensive and efficient security scheme for wireless networks, specifically WiMAX. As the future work, I intend to study handover between different BSs and SPs using the properties of Hierarchical IBC[34]. Therefore, IBC key pair generation and distribution can be done in a more fast and distributed way. Furthermore, during the key revocation, the networks can be isolated much faster and warning messages can be delivered in a timely manner.

Appendix A

Identity Based Cryptography

Identity-Based Cryptography (IBC)[4] is considered as an alternative technique to the traditional certificate based cryptography, especially after the detailed work of Boneh and Franklin in 2001[28]. The main idea of IBC is to use publicly known identity information of an entity to derive its public key. This will eliminate the need for the public-key distribution problem that arises in certificate based cryptography[15]. Also, all entities in the same network using the common parameters are able to generate any of entity's public key without requesting any additional information from a third party. Note that certificate based cryptography requires the binding of the certificate to the user and can introduce the high cost of key management due to the problem of certificate revocation.

The rest of this appendix is based on the work in[15]. Mathematically, IBC is based on the pairing technique. Let p, q be two large primes and $\mathbb{E}/\mathbb{Z}_p$ indicates an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}p = i|0 \leq I \leq p-1$. Then $\mathbb{G}1$ is denoted as a q-order subgroup of the additive group of points on $\mathbb{E}/\mathbb{Z}_p$ and $\mathbb{G}2$ by a q-order subgroup of the multiplicative group of the finite field $\mathbb{F}(p^2)$. It is important to point out that solution to the Discrete Logarithm Problem (DLP) is assumed to be a hard operation in both $\mathbb{G}1$ and $\mathbb{G}2$. That is, it is computationally not possible to acquire x in $\mathbb{Z}_q = i|1 \leq i \leq q1$, given that P, Q in $\mathbb{G}1$ (respectively, P, Q in $\mathbb{G}2$) such that $Q = xP$ (respectively, $Q = P^x$). Once more note that, a pairing is a map $\hat{e}^1 : \mathbb{G}1 \times \mathbb{G}1 \rightarrow \mathbb{G}2$. This mapping brings crucial properties as follows:

1. Bilinearity: For all $P, Q \in \mathbb{G}1$ and all $c, d \in \mathbb{Z}^*_{p^2}$,

[1]Note that $\hat{e}$ is symmetric.

$\hat{e}(cP, dQ) = \hat{e}(cP, Q)^d = \hat{e}(P, dQ)^c = \hat{e}(P, Q)^{cd}$

2. Non-degeneration: If P is a generator of $\mathbb{G}1$, then $\hat{e}(P, P)$ is a generator of $\mathbb{G}2$.

3. Easy computation: There exists a computable algorithm to obtain $\hat{e}(P, Q)$ for all $P, Q \in \mathbb{G}1$.

The modified Weil[28] and Tate parings[35] exemplify such bilinear maps for which the Bilinear Diffie-Hellman Problem is hard. That is, given (P, xP, yP, zP) for random x, y, z in $\mathbb{Z}_q$ and P in $\mathbb{G}1$, there does not exist any algorithm that is running in polynomial time, which can compute $\hat{e}(P, P)^{xyz}$ in $\mathbb{G}1$ with non-negligible probability. [28, 35] supply more detailed information regarding to this area.

References

[1] IEEE std. 802.16-2001 ieee standard for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems. *IEEE Std 802.16-2001*, pages 0–322, 2002.

[2] IEEE standard for local and metropolitan area networks part 16: Air interface for fixed and mobile broadband wireless access systems amendment 2: Physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1. *IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004)*, pages 0–822, 2006.

[3] I.F. Akyildiz and Xudong Wang. A survey on wireless mesh networks. *Communications Magazine, IEEE*, 43(9):S23–S30, Sept. 2005.

[4] Adi Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[5] WiMAX Forum, 2008.

[6] IEEE standard for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems. *IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001)*, pages 0–857, 2004.

[7] Data-over-cable service interface specification.

[8] D. Johnston and J. Walker. Overview of ieee 802.16 security. *Security & Privacy Magazine, IEEE*, 02(3):40–48, 2004.

[9] Sen Xu, Manton Matthews, and Chin-Tser Huang. Security issues in privacy and key management protocols of ieee 802.16. In *ACM-SE 44: Proceedings of the 44th annual Southeast regional conference*, pages 113–118, New York, NY, USA, 2006. ACM.

[10] Michel Barbeau. Wimax/802.16 threat analysis. In Azzedine Boukerche and Regina Borges de Araujo, editors, *Q2SWinet*, pages 8–15. ACM, 2005.

[11] Yun Zhou and Yuguang Fang. Security of ieee 802.16 in mesh mode. *Military Communications Conference, 2006. MILCOM 2006*, pages 1–6, Oct. 2006.

[12] Zara Hamid and Shoab A.Khan. An augmented security protocol for wirelessman mesh networks. *Communications and Information Technologies, 2006. ISCIT '06. International Symposium on*, pages 861–865, 18 2006-Sept. 20 2006.

[13] Bongkyoung Kwon, Christopher P. Lee, Yusun Chang, and John A. Copeland. A security scheme for centralized scheduling in ieee 802.16 mesh networks. *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1–5, 2007.

[14] L. Martin. Identity-based encryption comes of age. *Computer*, 41(8):93–95, Aug. 2008.

[15] Yanchao Zhang and Yuguang Fang. A secure authentication and billing architecture for wireless mesh networks. *Wirel. Netw.*, 13(5):663–678, 2007.

[16] X. Boyen and L. Martin. Identity-based cryptography standard (ibcs) #1: Supersingular curve implementations of the bf and bb1 cryptosystems. RFC 5091 (Informational), dec 2007.

[17] B. Aboba, D. Simon, and P. Eronen. Extensible Authentication Protocol (EAP) Key Management Framework. RFC 5247 (Proposed Standard), August 2008.

[18] R. Housley, W. Polk, W. Ford, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280 (Proposed Standard), April 2002. Obsoleted by RFC 5280, updated by RFCs 4325, 4630.

[19] Katrin Hoeper and Guang Gong. Key revocation for identity-based schemes in mobile ad hoc networks. In Thomas Kunz and S. S. Ravi, editors, *ADHOC-NOW*, volume 4104 of *Lecture Notes in Computer Science*, pages 224–237. Springer, 2006.

[20] Katrin Hoeper and Guang Gong. Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation. Technical report, 2006.

[21] Shane Balfe, Kent D. Boklan, Zev Klagsbrun, and Kenneth G. Paterson. Key refreshing in identity-based cryptography and its applications in manets. *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1–8, Oct. 2007.

[22] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard), May 2008.

[23] David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. pages 153–181. 1996.

[24] Mahmoud Nasreldin, Heba Aslan, Magdy El-Hennawy, and Adel El-Hennawy. Wimax security. In *AINA Workshops*, pages 1335–1340. IEEE Computer Society, 2008.

[25] Eduardo B. Fernandez, Michael VanHilst, and Juan C. Pelaez. Patterns for wimax security. 2007.

[26] L. Maccari, M. Paoli, and R. Fantacci. Security analysis of ieee 802.16. *Communications, 2007. ICC '07. IEEE International Conference on*, pages 1160–1165, June 2007.

[27] Sen Xu and Chin-Tser Huang. Attacks on pkm protocols of ieee 802.16 and its later versions. *Wireless Communication Systems, 2006. ISWCS '06. 3rd International Symposium on*, pages 185–189, Sept. 2006.

[28] Dan Boneh and Matthew Franklin. Identity-based encryption from the weil pairing. pages 213–229. Springer-Verlag, 2001.

[29] Joonsang Baek, Jan Newmarch, Reihaneh Safavi-naini, and Willy Susilo. A survey of identity-based cryptography. In *Proc. of Australian Unix Users Group Annual Conference*, pages 95–102, 2004.

[30] Pandurang Kamat, Arati Baliga, and Wade Trappe. An identity-based security framework for vanets. In *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 94–95, New York, NY, USA, 2006. ACM.

[31] N. Asokan, Kari Kostiainen, Philip Ginzboorg, Jörg Ott, and Cheng Luo. Applicability of identity-based cryptography for disruption-tolerant networking. In *MobiOpp '07: Proceedings of the 1st international MobiSys workshop on Mobile opportunistic networking*, pages 52–56, New York, NY, USA, 2007. ACM.

[32] Kevin Fall. A delay-tolerant network architecture for challenged internets. In *SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 27–34, New York, NY, USA, 2003. ACM.

[33] Leonardo B. Oliveira, Ricardo Dahab, Julio Lopez, Felipe Daguano, and Antonio A.F. Loureiro. Identity-based encryption for sensor networks. *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, pages 290–294, March 2007.

[34] Craig Gentry and Alice Silverberg. Hierarchical id-based cryptography. In *ASIACRYPT '02: Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security*, pages 548–566, London, UK, 2002. Springer-Verlag.

[35] Paulo S. L. M. Barreto, Hae Yong Kim, Ben Lynn, and Michael Scott. Efficient algorithms for pairing-based cryptosystems. In *CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, pages 354–368, London, UK, 2002. Springer-Verlag.