An IBC and Certificate Based Hybrid Approach to WiMAX Security

Mete Rodoper, Wade Trappe, and Edward (Tae-Chul) Jung

Abstract: **Worldwide inter-operability for microwave access (WiMAX) is a promising technology that provides high data throughput with low delays for various user types and modes of operation. While much research had been conducted on physical and MAC layers, little attention has been paid to a comprehensive and efficient security solution for WiMAX. We propose a hybrid security solution combining identity-based cryptography (IBC) and certificate based approaches. We provide detailed message exchange steps in order to achieve a complete security that addresses the various kind of threats identified in previous research. While attaining this goal, efficient fusion of both techniques resulted in a 53% bandwidth improvement compared to the standard's approach, PKMv2. Also, in this hybrid approach, we have clarified the key revocation procedures and key lifetimes. Consequently, to the best of knowledge our approach is the first work that unites the advantages of both techniques for improved security while maintaining the low overhead for WiMAX.**

Index Terms: **Identity-based cryptography (IBC), IEEE 802.16, key m-anagement, key revocation, PKMv2, security, worldwide inter-operability for microwave access (WiMAX), wireless mesh networks (WMNs).**

I. INTRODUCTION

Worldwide inter-operability for microwave access (WiMAX) is an important emerging technology in the wireless world due to its potential for solving some of the problems that WiFi cannot. Additionally, WiMAX (also known as IEEE 802.16 [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. 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 eavesdropping and message injection into the network.

A natural line of defense to protect against such attacks is to 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. The flaws identified at PKMv1—mostly "stationary subscribers" related ones—were all fixed by PKMv2. However, it did not provide full and efficient security coverage for all WiMAX modes of operation and user types.

One shortcoming of the aforementioned standardized solutions is that 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 modes of operation and types of users are not fully taken into consideration during the design phase, which is a further drawback of the framework. 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, existing security methods fail to deliver a complete solution and have introduced a huge resource consumption issue.

In this paper, we propose a collection of security solutions that use a combination of identity based cryptography (IBC) [4] and certificate based cryptography: First, to reach complete system security for authentication, link establishment and traffic encryption key (TEK) derivation steps for all WiMAX modes of operation and user types. Secondly, we must ensure that device and network resources are being used both modestly and efficiently used while securing the connection. Lastly, to cover all the security features for WiMAX, we propose a more efficient and complete key revocation procedure compared to the current WiMAX standard. The reason for adding IBC to this system is to exploit its beneficial efficiency and security enhancing properties that we cannot easily achieve by certificate based systems. In Section II, we explain the WiMAX modes of operation, user types and illustrate the existing security deficiencies of the IEEE 802.16 standard family. In Section III, we provide a high-level explanation of IBC properties and our security solution. In Section IV, we give the protocol steps and details. In Section V, analysis of our solution will be explained. The related work will be summarized in Section VI. Finally, we present conclusion in Section VII.

II. WiMAX ARCHITECTURE AND SECURITY OVERVIEW

In this section, we provide an overview of the logical architecture, user types in WiMAX, and the different modes of operation. We then review and analyze the security problems of PKMv1. Finally, we indicate the solutions provided to some of these problems by PKMv2 and enumerate the remaining un-

Manuscript received April 15, 2009.

M. Rodoper and W. Trappe are with the Wireless Information Network Laboratory (WINLAB), Rutgers University, North Brunswick, NJ, USA, email: {mrodoper, trappe}@winlab.rutgers.edu.

E. Jung is with the School of Computing and Software Engineering, Southern Polytechnic State University, Marietta, Georgia, USA, email: ejung@spsu.edu.

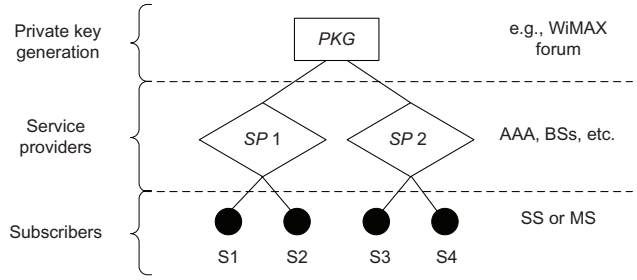

Fig. 1. WiMAX logical architecture.

solved flaws.

A. WiMAX Architecture, Entities, and Modes of Operation

The WiMAX logical architecture consists of three hierarchical components as seen in Fig. 1. At the top, there is the *private key generation (PKG)* entity, which is primarily responsible for the generation of materials associated with the X.509 certificate and (in our case) IBC parameters. For example, the PKG could be an entity associated with the WiMAX Forum [5]. Below the PKG are *service providers (SPs)* who maintain the basic network infrastructure, such as the AAA servers, base stations (BSs) and any other provisions associated with user connectivity to the network. The SPs are also responsible for security maintenance such as key distribution and revocation from the PKG to the lower layer (or, in our case the distribution of IBC private keys). At the bottom of the architecture are *Subscribers (S)* who connect to SPs looking for service.

WiMAX has two subscriber types: *Stationary subscribers (SSs)* and *mobile subscribers (MSs)*. The SSs are fixed to a location and have sufficient battery and computation power for complex calculations. The MSs 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.

Both types of WiMAX subscribers may use one of two modes of operation to get connectivity: *Point to multipoint (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 (subscribers). The BS itself either acts directly as a gateway to the IP network or forwards subscribers' IP packets to another gateway BS. On the subscriber side, entities can only make one connection at a time and this connection has to be with a BS. Therefore, all subscriber data has to go through a BS to reach the IP network. As Fig. 2(a) depicts, S1 and S2 are connected 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 IEEE 802.16-2004 [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

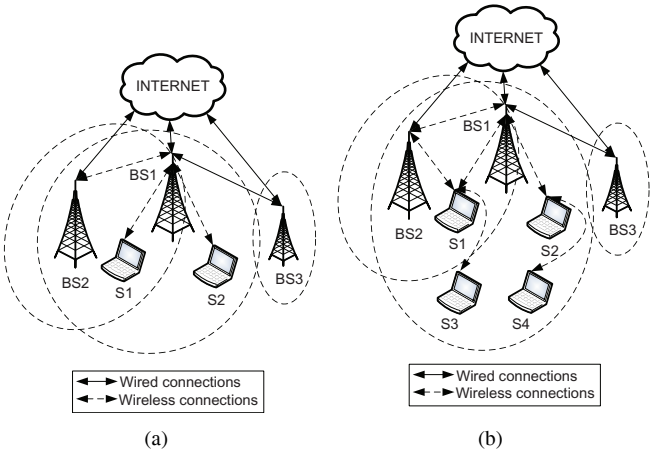

Fig. 2. WiMAX modes of operation: (a) WiMAX PMP mode and (b) WiMAX mesh mode.

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. Unlike in PMP mode, mesh mode allows subscribers to form multiple links between one another and the BSs. 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)*. For instance, in Fig. 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(b), where S1 forms connections with both BS1 and BS2). This not only provides different routes and link reliability but also eases the handoff mechanism for mesh mode.

B. WiMAX Security and the Threats Overview

PKMv1 was adapted from DOCSIS standard [7]. The main reason for the failure of this standard was that it was designed for wired networks and thus was not compatible with wireless networks. 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 TEK creation. The defects -such as node impersonation, message replay, message modification- 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 are some of the problems, 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 to the end of the messages. 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 example, once an intruder eavesdrops on the mesh network master secret (the operator shared secret (OSS), which is 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 among mesh network pairs and start relaying their data messages. Ultimately, neighbors' data can be decrypted and data confidentiality is compromised.

C. 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). Simply put, the mutual authentication problem was solved by pairwise X.509 certificate exchange, the message replay threat was solved by adding nonces to management messages and the message modification attack is resolved by adding signatures and MAC functions. However, PKMv2 did not address WiMAX mesh mode security issues. Note that this mode was proposed a year before PKMv2 so standard involvers did not have enough time to prepare PKMv2 for the mesh mode. Thus, the following problems still exist in WiMAX and the mesh mode still suffers.

- OSS related flaws:
  - Using the same OSS keys among all mesh network entities increases the risk of OSS being compromised and therefore the security is degraded.
  - It is unknown when OSS keys must be renewed in order to prevent compromise.
  - Unencrypted OSS transmissions during authentication can lead to OSS theft and decryption of all data messages in the network.
- TEK related flaws:
  - TEK and the parameters are mentioned at the standard, but key formation is skipped. Therefore, TEK creation is unclear.
  - Superfluous usage, insufficient lifetime and renewal details of TEK may lead to key discovery.

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 of mesh mode. If AK is used along with OSS, its purpose is unclear. Beyond these postponed mesh mode issues, we believe that PKMv2 is not taking the requirements of mobile subscribers (such as less communication overhead and timely link formations) into consideration, because the overhead loaded by PKMv2 to both the network and subscribers is in essence excess.

III. OVERVIEW OF OUR IBC AND CERTIFICATE BASED HYBRID WiMAX SECURITY APPROACH

The three main goals of our approach are: To ensure the solution is secure against all types of attacks identified above; to boost the speed and efficiency of secure link establishment; and to propose a complete key revocation procedure that will successfully refresh all the keys.

To achieve these goals our 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, we used a minimal amount of messages to increase bandwidth efficiency.

Using the threat model, the remainder of this paper 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.

A. Exploited Cryptographic Techniques

Meeting all the listed requirements is a difficult task and cannot be achieved easily with the current certificate based framework, PKMv2. We use IBC in our 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, we believe that with the combination of IBC and PKMv2 we can minimize the drawbacks that may exist with any single technique and maximize the benefits.

Simply put, the main idea of IBC is to use publicly known identity information to derive the public key of a subscriber. 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 we are exploiting to achieve the aforementioned goals;

- *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 to 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.

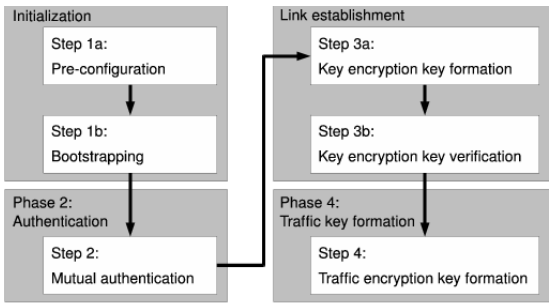

Fig. 3. Security phases and intermediate steps.

- *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, we still need to use the X.509 certificate, because IBC also has some drawbacks. 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, we use the existing hardware embedded WiMAX X.509 certificates and distribute IBC private keys encrypted by the RSA public key contained within.

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.

B. Proposed Security Phases and Intermediate Steps

PKMv1 and PKMv2 consist of three main phases for both modes of operation and user types: Authentication, link establishment, and TEK creation. Although there are some differences for both modes, we observe that each phase is formed by some intermediate steps. In addition; our proposed solution will contain the same three main phases but, before these phases, it will have an initialization phase for the preparation of keys and certificates. When our proposed steps are examined in detail, six intermediate steps can be discerned as follows.

As Fig. 3 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 20 ms) [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 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.

We note 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.

C. Proposed Key and Certificate Revocation Procedure

Our 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, we designed new message schemes and contents for our security approach explained above.

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 RFC 3280 [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, we propose our own IBC key revocation procedure for WiMAX security.

The IBC related keys that we propose a renewal procedure are:

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. KEK of all pairwise links
4. 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

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

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 our 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. We will see this in the subsequent section.

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.

IV. SECURITY PROTOCOLS OF PROPOSED HYBRID SECURITY APPROACH

In this section, we describe the security messages in our WiMAX security solution, for both modes and user types. For the rest of the section, we use the notation in Table 1. Also, the following messaging convention is used throughout the remainder of this paper. 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.

Step 1a: Pre-configuration

In this step X.509 certificates are acquired for subscribers and BSs. Additionally, we prepare the IBC key pairs for BSs. There are no messages being exchanged between any WiMAX network entities through the air at this step. As per the standard, we assume that BSs and subscribers have their own WiMAX X.509 Certificates embedded in their hardware. Besides certificates, we assume 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 $\mathrm{BS}_{\mathrm{pub}}$ as follows.

$$\mathrm{BS}_{\mathrm{pub}} = \mathrm{BS}_{\mathrm{id}} \,\|\, \mathrm{SP}_{\mathrm{id}} \,\|\, \mathrm{TS}_1$$

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

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.

$$\mathrm{BS} \Rightarrow * : \text{MSH-NCFG [} \mathrm{BS}_{\mathrm{pub}} \,\|\, \textit{param} \,\|\, \mathrm{TS}_1 \,\|\, E_{\mathrm{BS}_{\mathrm{pvt}}}(\textit{param} \,\|\, \mathrm{TS}_1 \text{)]}$$

Here, $\mathrm{BS}_{\mathrm{pub}}$ and *param* are embedded in the message to support the distribution of the IBC credentials of a WiMAX network to all potentials subscribers. $\mathrm{BS}_{\mathrm{pub}}$ 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.

$$S_{\mathrm{pub}} = S_{\mathrm{id}} \,\|\, \mathrm{BS}_{\mathrm{id}} \,\|\, \mathrm{TS}_1$$

S_{id} is the subscribers' built-in ID. $\mathrm{BS}_{\mathrm{id}}$ can be extracted from $\mathrm{BS}_{\mathrm{pub}}$. Consequently, usage of $\mathrm{BS}_{\mathrm{id}}$ results in prevention of any malicious node from getting connected to another BS using the same IBC key pair. We 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 paper.

1. $\mathrm{BS} \Rightarrow *$: MSH-NCFG [$\mathrm{BS}_{\mathrm{pub}} \,\|\, \textit{param} \,\|\, \mathrm{TS}_1 \,\|\, E_{\mathrm{BS}_{\mathrm{pvt}}}(\textit{param} \,\|\, \mathrm{TS}_1)$]
2. $\mathrm{BS} \Leftarrow$ Subs. : MSH-NENT [Net_Entry_Reg.]
3. $\mathrm{BS} \Rightarrow$ Subs. : MSH-NCFG [Net_Entry_Open]
4. $\mathrm{BS} \Leftarrow$ 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.

Step 2: Mutual Authentication

We elaborate on the subscriber and BS mutual authentication procedure in this section. 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. We follow the standard's PKMv2 authentication scheme and use X.509 certificates for proof of subscriber trustworthiness. In addition to the PKMv2 authentication scheme, we add more functionality to PKMv2 for S_{pvt} distribution purposes. Therefore, the network is ready for IBC based cryptographic calculations. The messages exchanged are as follows.

Table 1. Abbreviations for the keys and credentials.

Abbreviation	Explanation
$\mathrm{BS_{id}}$, S_{id}	The unique identifiers for the BS and subscriber
$\mathrm{SP_{id}}$	The unique identifier of a service provider
$\mathrm{BS_{pub}}$, 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
$\mathrm{BS_{pvt}}$, 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 (We assume a secure time synchronization method is employed)
$(C^{\mathrm{BS}}_{\mathrm{pub}}, C^{\mathrm{BS}}_{\mathrm{pvt}})$	The public RSA key pairs for the BS and subscribers, respectively
$(C^{S}_{\mathrm{pub}}, C^{S}_{\mathrm{pvt}})$	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, $E_{\mathrm{BS_{pvt}}}$ is the signature of a BS using its IBC private key and $E_{C^{S}_{\mathrm{pub}}}$ is an encryption by a subscriber using an RSA public key

1. BS $\Leftarrow$ Subs. : AUTH_REQ [$\mathrm{TS}_1 \parallel Cert_S \parallel$ *Capabilities* $\parallel S_{\mathrm{pub}} \parallel E_{C^{S}_{\mathrm{pvt}}}$ ($\mathrm{TS}_1 \parallel Cert_S \parallel S_{\mathrm{pub}}$)]
2. BS $\Rightarrow$ Subs. : AUTH_REP [$\mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel Cert_{BS} \parallel E_{C^{S}_{\mathrm{pub}}}$ (S_{pvt}) $\parallel$ SAID $\parallel E_{C^{\mathrm{BS}}_{\mathrm{pvt}}}$ ($\mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel Cert_{BS} \parallel E_{C^{S}_{\mathrm{pub}}}$ (S_{pvt}) $\parallel$ *SAID*)]
3. BS $\Leftarrow$ Subs. : AUTH_ACK [$\mathrm{TS}_2 \parallel E_{C^{S}_{\mathrm{pvt}}}$ (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 $E_{C^{S}_{\mathrm{pub}}}$ 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.

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 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
$\Downarrow$	$\Downarrow$
$\hat{e}(H_{\mathrm{sp}}(Entity1_{\mathrm{pvt}}, Entity2_{\mathrm{pub}}))$ =	$\hat{e}(H_{\mathrm{sp}}(Entity2_{\mathrm{pvt}}, Entity1_{\mathrm{pub}}))$
= 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, our 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.

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] [$Entity1_{\mathrm{pub}} \parallel$ *param* $\parallel \mathrm{TS}_1 \parallel E_{Entity1_{\mathrm{pvt}}}$(*param* $\parallel \mathrm{TS}_1$)]
2. Entity1 $\Leftarrow$ Entity2 : KEK-VER-REQ [$Entity2_{\mathrm{pub}} \parallel \mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel H_{\mathrm{KEK}}$ ($\mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel Entity1_{\mathrm{pub}}$) $\parallel E_{Entity2_{\mathrm{pvt}}}$($msgcontent$[b])]
3. Entity1 $\Rightarrow$ Entity2 : KEK-VER-REP [H_{KEK} ($\mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel Entity2_{\mathrm{pub}}$) $\parallel E_{Entity1_{\mathrm{pvt}}}$($msgcontent$[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 "$Entity2_{\mathrm{pub}} \parallel \mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel H_{\mathrm{KEK}}$ ($\mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel Entity1_{\mathrm{pub}}$)"

[c] $msgcontent$ is "H_{KEK} ($\mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel Entity2_{\mathrm{pub}}$)"

In the MSH-NCFG message, in other words the "beacon," the Entity1 announces its $Entity1_{\mathrm{pub}}$ to the network, so that

all of its neighbors know $Entity1_{\mathrm{pub}}$. In the next message, when Entity2 wants to form a link with Entity1, it transmits: $Entity2_{\mathrm{pub}}$ 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.

Step 4: Traffic Encryption Key Formation

The 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.

$$H_{\mathrm{KEK}}\,(\,\mathrm{TS}_1 \parallel \mathrm{TS}_2 \parallel Entity1_{\mathrm{pub}} \parallel Entity2_{\mathrm{pub}}\,) = \mathrm{TEK}$$

TS_1 and TS_2 are the timestamps exchanged at the step 3b. $Entity1_{\mathrm{pub}}$ and $Entity2_{\mathrm{pub}}$ 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 "$\mathrm{TS}_2 + keyduration$" expires, a new TEK using the active KEK and new timestamps is calculated. The details of revocation is given in the next section of this paper.

V. CERTIFICATE AND KEY REVOCATION OF PROPOSED HYBRID SECURITY APPROACH

This section gives the details of the certificate and key revocation procedures for our proposed security solution.

A. 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 be 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.

B. IBC Related Credential Revocation

We now define our key revocation procedure for individual IBC related keys. The additional notation we use in this section is in Table 2.

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)

Table 2. Additional abbreviations for the keys and credentials.

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

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.

We 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.

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 $\mathrm{BS}_{\mathrm{pvtnew}}$ immediately (matching $\mathrm{BS}_{\mathrm{pubnew}}$). 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, we use the active TEK. The protocol steps are as follows.

1. Subs. $\Leftarrow$ BS : IBC_REP [$\mathrm{TS}_1 \parallel S_{\mathrm{pubnew}} \parallel E_{\mathrm{TEK}}\,(\,\mathrm{TS}_1 \parallel S_{\mathrm{pvtnew}})$]
2. Subs. $\Rightarrow$ BS : IBC_ACK [$\mathrm{TS}_2 \parallel E_{S_{\mathrm{pvtnew}}}\,(\,\mathrm{TS}_1 \parallel \mathrm{TS}_2)$]

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.

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 are no messages broadcast to air, just a pairing calculation on device is necessary.

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, we can use TEK encrypted data messages and without halting the data transmissions on the network.

VI. EVALUATION

For a complete evaluation of our approach, we first assess the completeness of our security approach by doing a security analysis for each phase. Then, for efficiency purposes, we run a simulation and calculate the communication overhead of both our approach and that of PKMv2.

A. Security Analysis

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

Initialization

At the beginning of this phase, X.509 certificate and IBC credential distribution are performed by using another secure medium (we 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 our framework protects against the threat of authentication violation.

Mutual Authentication

The authentication process we 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.

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, we eradicated OSS completely and instead used the bilinear mapping property of IBC for neighbor authentication. As mentioned above, the Bilinear Diffie-Hellman Problem is assumed to be an NP-complete problem [4]. Another advantage of our 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.

Traffic Encryption Key Creation

One benefit of our 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 our case the "code" is the KEK) are known.

Compared to the standard, another advantage of our 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. Our hybrid approach solves this problem by using the bilinearity property of IBC.

B. Performance Analysis

In this part of our evaluation, we analyze the communication performance of our security scheme. The performance here mainly is based on the communication overhead analysis since we believe that 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 we mainly analyze the communication overhead of our approach and compare it to PKMv2. The reason for not comparing our approach with the previous works (e.g., [11]–[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 our approach do. Hence, comparison of the previous works with our approach is not completely convenient and hold validity.

In order to analyze the communication overhead of our approach, we compared 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, for both our approach and those of PKMv2. Additionally, to identify the improvements made by our approach more precisely, we run our simulation on mesh mode. As a result, more links will be formed and the implications of our solution will be apparent.

To observe the overhead of the individual messages, we assigned some constant values for credentials inside the message as shown in Table 3. Most of these values are collected from [2], [6], [16]. However, for some variable values we were forced to make realistic assumptions. Based on these values, the message sizes of our approach and PKMv2 are calculated the same as in Table 4. As can be observed from this table, our 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 our approach, and Phase3 for PKMv2) are compared, our

Table 3. Sizes of the items inside the messages.

TS_i	8 B	*param*	50 B[a]
$\mathrm{BS}_{\mathrm{pub}}$, S_{pub}	30 B[a]	$\mathrm{BS}_{\mathrm{pvt}}$, S_{pvt}	128 B
$Cert_S$	1000 B[a]	H_{MAC}, E_{pvt}	128 B
$\mathrm{BS}_{\mathrm{id}}$, 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

Table 4. 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

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, our approach apparently outperforms PKMv2.

In addition to these messages, we designed a simple mobility model similar to the random waypoint model (RWP) [34] for simulating the mobility of subscribers as accurately as possible. Using our 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 we believe 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 using this simple model, we can achieve more realistic results than compared to any random movement model. In all of our simulation, the results presented are averaged over 10 separate runs.

Using our message size assignments and model to calculate the efficiency of our security protocols, we measure the network load in Bytes. 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 we vary the number of subscribers in the network and then, the number of links that an entity can form.

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

As we can see from Fig. 4, as the number of subscribers increases, our 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 overhead. Since our approach uses less bandwidth for link establishment it gives superior values for denser networks.

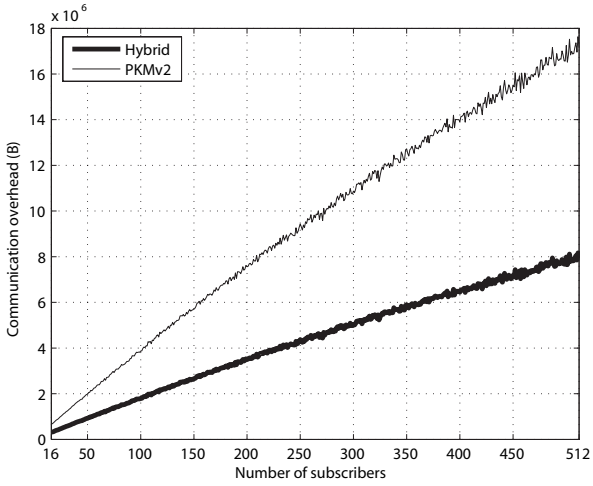

Fig. 4. Communication overhead vs. number of subscribers.

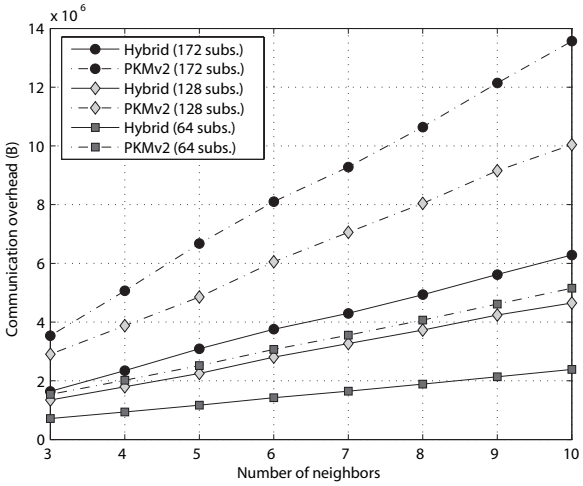

Fig. 5. Communication overhead vs. maximum number of links.

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

As Fig. 5 indicates, as the number of links that a subscriber can establish increases, we achieve roughly a 53% increase in efficiency compared to PKMv2. As the number of subscribers increases from 64 to 172, the performance of our solution does not degrade and maintains dominance over PKMv2. Consequently, the bandwidth usage based on security establishment is reduced by a critical amount. Thus, our proposed solution is also better than PKMv2 in terms of communication overhead.

VII. RELATED WORK

In this section, we review the work related to our study. WiMAX security analysis related papers have been published

by many researchers. Johnston and Walker identified the mutual authentication problem, key management failures and data protection errors in [8], though, their approach did not involve many detailed solutions. Some more papers analyze authentication flaws, link establishment attacks were also published in recent years [9], [10], [23]–[25].

Apart from analysis publications, some more efforts have been made in proposing new solutions for the existing problems. Xu and Huang identify several existing problems, provide countermeasures to these flaws and propose new protocol steps [26]. Although they eliminate the interleaving attack and replay attack, their approach introduces significant communication overhead and is short of providing a comprehensive solution to all WiMAX security phases. Zhou and Fang propose 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, some other publications also targeted individual modes and proposed some partial solutions to WiMAX security [12], [13].

Besides the fundamental IBC papers [4], [27], some other theoretical IBC papers have been published. Hoeper and Gong proposed a bootstrapping procedure for IBC [20]. Also, [19], [21] provided IBC key refreshing procedures. Different from these works specific for individual phases, [14], [28] have analyzed the network issues superficially and proposed possible generic security solutions using IBC. Besides these theoretic studies, IBC is used to address the real world security problems. [29] examined the applicability of IBC on DTNs [31], [30] applied IBC on VANETs, and [32] used IBC for sensor networks security. Lastly, Zhang and Fang have proposed a IBC security architecture for mesh networks. The proposed network architecture and the authentication steps are very clear. However, the applicability related information does not reside in this paper.

VIII. CONCLUDING REMARKS AND FUTURE WORK

In this paper, we presented an IBC and certificate based security scheme for WiMAX and its steps we presented in detail. Unlike other partial solutions for WiMAX security, our 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. Our message framework authenticates entities using X.509 certificates mutually, forms fast and multiple links between entities, and, creates the TEK securely using the timestamps exchanged at the early steps. Furthermore, the proposed framework has a simple key renewal process, which does not halt the connections. Moreover, the proposed message steps use less bandwidth compared to the WiMAX standard, PKMv2. Overall, we have achieved a more comprehensive and efficient security scheme for WiMAX. As the future work, we intend to study handover between different BSs and SPs using the properties of Hierarchical IBC [33].

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*, pp. 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)*, pp. 0–822, 2006.

[3] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Commun. Mag.*, vol. 43, no. 9, pp. S23–S30, Sept. 2005.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO4 on Advances in Cryptology*, USA, 1985, pp. 47–53.

[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)*, pp. 0–857, 2004.

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

[8] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," *IEEE Security Privacy*, vol. 2, no. 3, pp. 40–48, 2004.

[9] S. Xu, M. Matthews, and C.-T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16," in *Proc. ACM-SE*, USA, 2006, pp. 113–118.

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

[11] Y. Zhou and Y. Fang, "Security of IEEE 802.16 in mesh mode," in *Proc. IEEE MILCOM*, Oct. 2006, pp. 1–6.

[12] Z. Hamid and S. A. Khan, "An augmented security protocol for wireless-man mesh networks," in *Proc. ISCIT*, 2006, pp. 861–865.

[13] B. Kwon, C. P. Lee, Y. Chang, and J. A. Copeland, "A security scheme for centralized scheduling in IEEE 802.16 mesh networks," in *Proc. IEEE MILCOM*, 2007, pp. 1–5.

[14] L. Martin, "Identity-based encryption comes of age," *Computer*, vol. 41, no. 8, pp. 93–95, Aug. 2008.

[15] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks," *Wireless Netw.*, vol. 13, no. 5, pp. 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), Aug. 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] K. Hoeper and G. Gong, "Key revocation for identity-based schemes in mobile ad hoc networks," *LNCS*, vol. 4104, pp. 224–237. Springer, 2006.

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

[21] S. Balfe, K. D. Boklan, Z. Klagsbrun, and K. G. Paterson, "Key refreshing in identity-based cryptography and its applications in manets," in *Proc. IEEE MILCOM*, Oct. 2007, pp. 1–8.

[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] M. Nasreldin, H. Aslan, M. El-Hennawy, and A. El-Hennawy, "Wimax security," in *Proc. AINA Workshops*, 2008, pp. 1335–1340.

[24] E. B. Fernandez, M. VanHilst, and J. C. Pelaez, "Patterns for wimax security," 2007.

[25] L. Maccari, M. Paoli, and R. Fantacci, "Security analysis of IEEE 802.16," in *Proc. IEEE ICC*, June 2007, pp. 1160–1165.

[26] S. Xu and C.-T. Huang, "Attacks on pkm protocols of IEEE 802.16 and its later versions," in *Proc. ISWCS*, Sept. 2006, pp. 185–189.

[27] Dan Boneh and Matthew Franklin, *Identity-Based Encryption from the Weil Pairing*, pp. 213–229. Springer-Verlag, 2001.

[28] J. Baek, J. Newmarch, R. Safavi-naini, and W. Susilo, "A survey of identity-based cryptography," in *Proc. Australian Unix Users Group Annual Conference*, 2004, pp. 95–102.

[29] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo, "Applicability of identity-based cryptography for disruption-tolerant networking," in *Proc. MobiOpp*, USA, 2007, pp. 52–56.

[30] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for vanets," in *Proc. VANET*, New York, NY, USA, 2006, pp. 94–95.

[31] K. Fall, " A delay-tolerant network architecture for challenged internets," in *Proc. SIGCOMM*, USA, 2003, pp. 27–34.

[32] L. B. Oliveira, R. Dahab, J. Lopez, F. Daguano, and A. A. F. Loureiro,

"Identity-based encryption for sensor networks," in *Proc. IEEE PerCom*, Mar. 2007, pp. 290–294.

[33] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in *Proc. ASIACRYPT*, UK, 2002, pp. 548–566.

[34] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, pp. 153–181. 1996.

Mete Rodoper Mete Rodoper received his B.S. degree in Telecommunications Engineering from Sabanci University at Istanbul, Turkey in 2007, and working on his Ph.D. degree in the Electrical and Computer Engineering Department at Rutgers University since 2007. He is currently a Graduate Assistant at the Wireless Information Network Laboratory (WINLAB). His research focus is on the wireless ad-hoc mobile networking and network security. Recently, he also has conducted research on channel quality prediction, link failure detection for bandwidth optimization by using cross-layer mechanisms at Telcordia Technologies.

Wade Trappe Wade Trappe received his B.A. degree in Mathematics from The University of Texas at Austin in 1994, and the Ph.D. in Applied Mathematics and Scientific Computing from the University of Maryland in 2002. He is currently Associate Director at the Wireless Information Network Laboratory (WINLAB) and an associate professor in the Electrical and Computer Engineering Department at Rutgers University. His research interests include wireless security, wireless networking, multimedia security, and network security. He has led projects involving security and privacy for sensor networks, physical layer security for wireless systems, a security framework for cognitive radios, the development of wireless testbed resources, and new RFID technologies. Recently, his research group has developed several cross-layer security mechanisms for wireless networks, has developed jamming detection and jamming defense mechanisms for wireless networks, and has investigated privacy-enhancing routing methods for wireless networks. He has published over 100 papers, including two best papers in media security, a best paper on the localization of cognitive radios, and several wireless security papers in premier conferences. His experience in network security and wireless systems spans 12 years, and he has co-authored a popular textbook in the field, Introduction to Cryptography with Coding Theory, as well as four other books on wireless systems and multimedia security. He is a Member of the IEEE Signal Processing and Communications societies, and a Member of the ACM.

Edward (Tae-Chul) Jung is currently an Assistant Professor in the School of Computing and Software Engineering at Southern Polytechnic State University, Georgia. His research interest is in security, privacy, and trust. Current application areas are wireless networking and mobile computing. He was a Murray Visiting Professor of computer science and a visiting professor of WINLAB at Rutgers University, New Brunswick, NJ (2008–2009). From 2003 until 2007, his research focus was in wireless and mobile system security at Samsung Research (SAIT), where he was a director of the Information Security Research Group. From 1997 until 2003, he conducted research work at Bell Labs, New Jersey, in the areas of secure mobile Internet architecture and wireless data networks. He has co-authored about 30 technical publications and holds 60 US/international patents on these topics. He received both an undergraduate degree and a Ph.D. in computer science from University of Minnesota, Minneapolis. He is a Senior Member of IEEE and a Member of ACM.