An Identity-Based Cryptography (IBC) Scheme for WiMAX Security

Rutgers, The State University of New Jersey

www.winlab.rutgers.edu

Mete Rodoper, MSc

Under supervision of Prof. Wade Trappe and Dr.Edward Jung

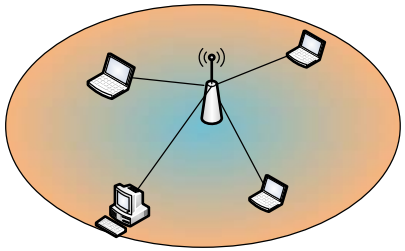
mrodoper@winlab.rutgers.edu

Content

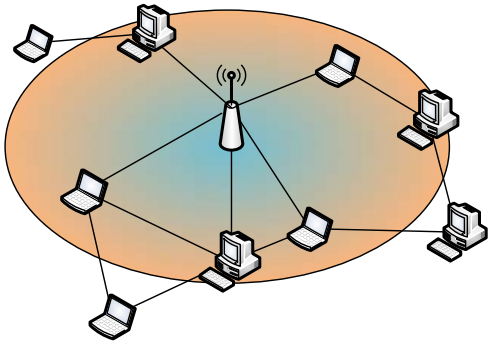
- Introduction
- Existing WiMAX Security and Problems
- IBC and its beneficial properties
- Our Approach
- Evaluation
- Concluding Remarks and Future Works
- Questions

WiMAX security design has many security flaws and inefficiencies

- WiMAX is intended to support
  - High data rates
  - Minimal delay jitter for long distances
  - Stationary subscribers
  - Mobile subscribers
  - Point to Multipoint (PMP) Mode
  - Mesh Mode



PMP Mode



Mesh Mode

- **Problem:** Security solutions for WiMAX were not comprehensively planned.
  - Not all subscriber types were considered
  - Not all modes of operations and their requirements were taken into consideration.
  - No detailed message exchange planning for Mesh Mode and its keys' creation.
  - No efficient security solution for Mobile Subscriber needs.
- **Motivation:** We have tried to develop a holistic security solution that takes all requirements into consideration.
  - Present a generic security architecture for Next Generation Networks
  - Propose an IBC based system and its protocol message on a real time system

WiMAX security standard PKMv2 is incapable of covering Mesh Mode and Mobile Subscribers

- The WiMAX standard seeks to accomplish security objectives through two proposed security frameworks:
  - PKMv1(2001)
  - PKMv2(2005).

  PKMv2 is the latest and an advanced version of PKMv1.
- PKMv2 left many security flaws and vague concepts for Mesh Mode security. For example:
  - The same Operator Shared Secret (OSS) key is used among all mesh network entities.
  - No details on OSS renewal frequency (to prevent compromise) were given.
  - Traffic Encryption Key (TEK) and the parameters are mentioned in the standard but key formation is ignored.
  - A dilemma exists related to the existence of the Authentication Key (AK) used during PMP Mode in the presence Mesh Mode.
- Also, PKMv2 is not capable of meeting Mobile Subscriber requirements:
  - Fast and simple calculations.
  - Fewer message exchanges.

3 important properties of IBC supported with X.509 certificates leads to a more secure and faster approach

- The main idea of IBC is to use publicly known identity information to derive the public key of a subscriber by using Service Provider (SP) parameters and SP Secret Key.
- The advantages of IBC that we utilize:
  1. Just in-time key generation (on-the-fly): There is no need for the pre-distribution of public keys
  2. Pairwise key establishment: By using the bilinearity and symmetry properties of pairing, pairwise keys can be formed among pairs during link formation simultaneously
  3. Extensibility: Additional information can be embedded into the identifier
- One crucial drawback is the necessity for a private key distribution mechanism from a Private Key Infrastructure (PKI) to Subscribers

4 phases and 6 intermediate steps exist for the formation of IBC + X.509 based hybrid security solution

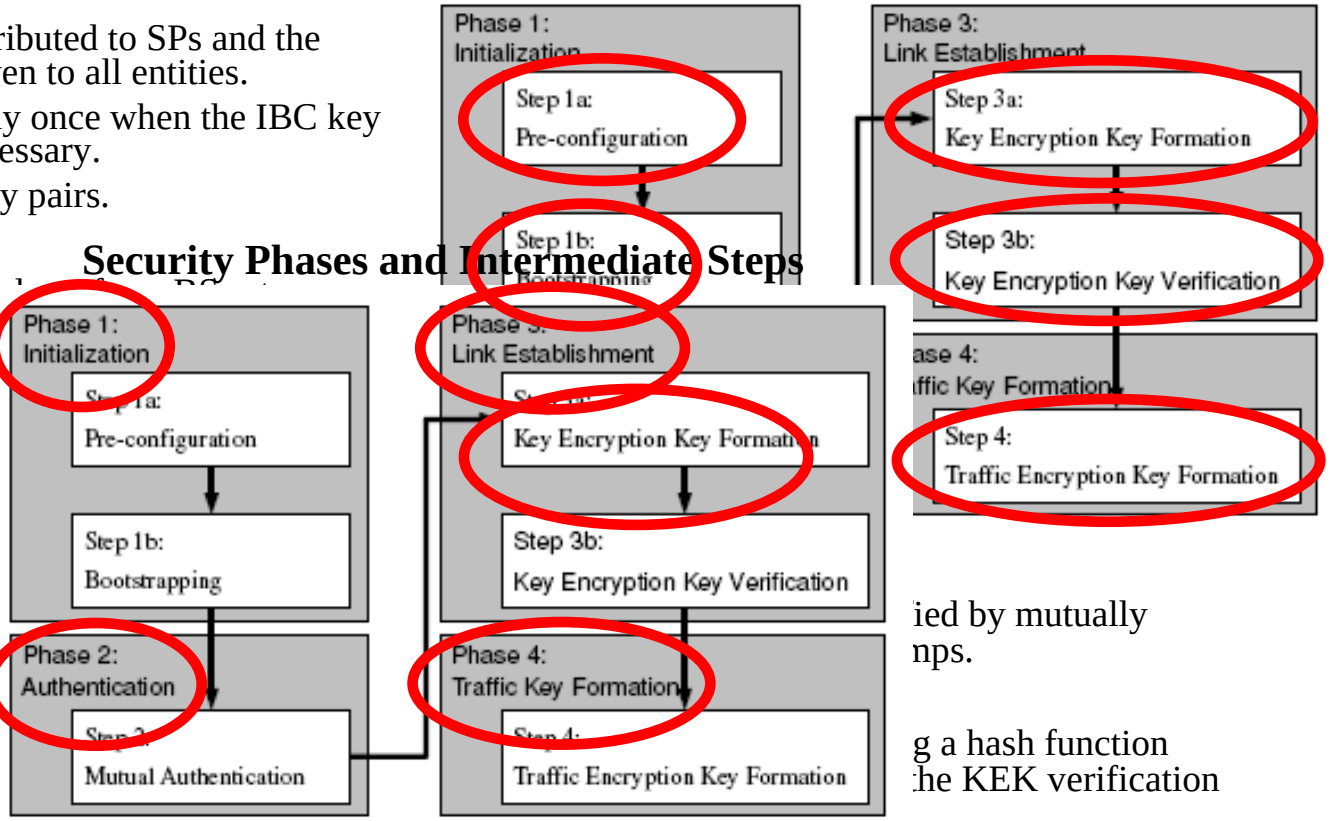
Step 1a:
- IBC parameters are distributed to SPs and the X.509 certificate are given to all entities.
- This step is repeated only once when the IBC key revocation becomes necessary.
- BS prepare their IBC key pairs.

Step 1b:
- IBC parameters are broa… beacon period (2.5 to 20…
- Subscribers are able to … public keys. (Details on …

Step 2:
- Mutual authentication is … X.509 certificates.
- EAP is performed for th…
- **Important:** IBC private… subscribers by encryptin… keys. (Details on next s…

Step 3a:
- Both ends of a connecti… Key (KEK) using the IE… IBC keys.
- **Significant:** During this step the KEK is created without any message being exchanged between the two ends. (Details on next slide)

Security Phases and Intermediate Steps



Security Phases and Intermediate Steps

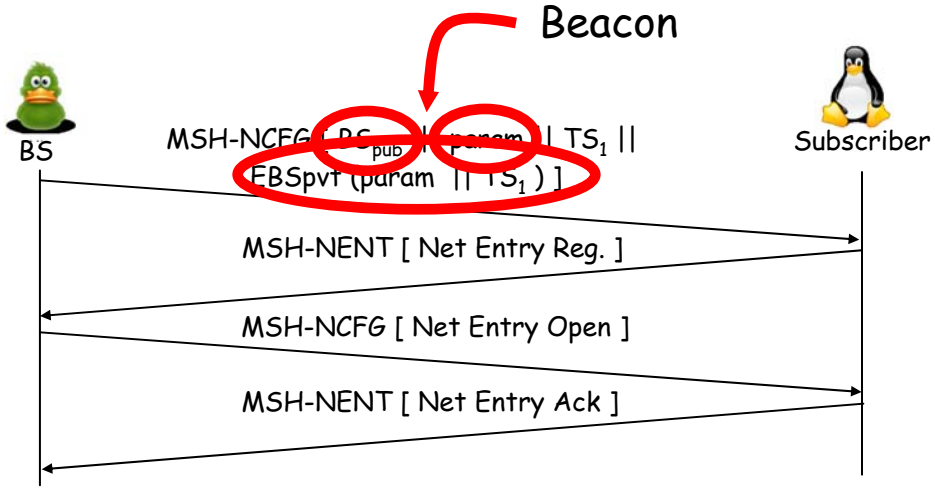
…ied by mutually …nps.

…g a hash function …he KEK verification

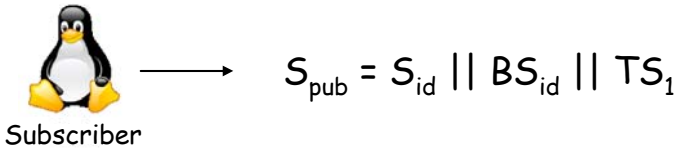
Same steps for both Mesh and PMP Mode and both Stationary and Mobile Subscribers

BS create their IBC key pairs and distribute the IBC domain parameters to subscribers (details of step 1b)

- Notation: MSG_NAME [concatenated credentials]
- Step 1b: Bootstrapping

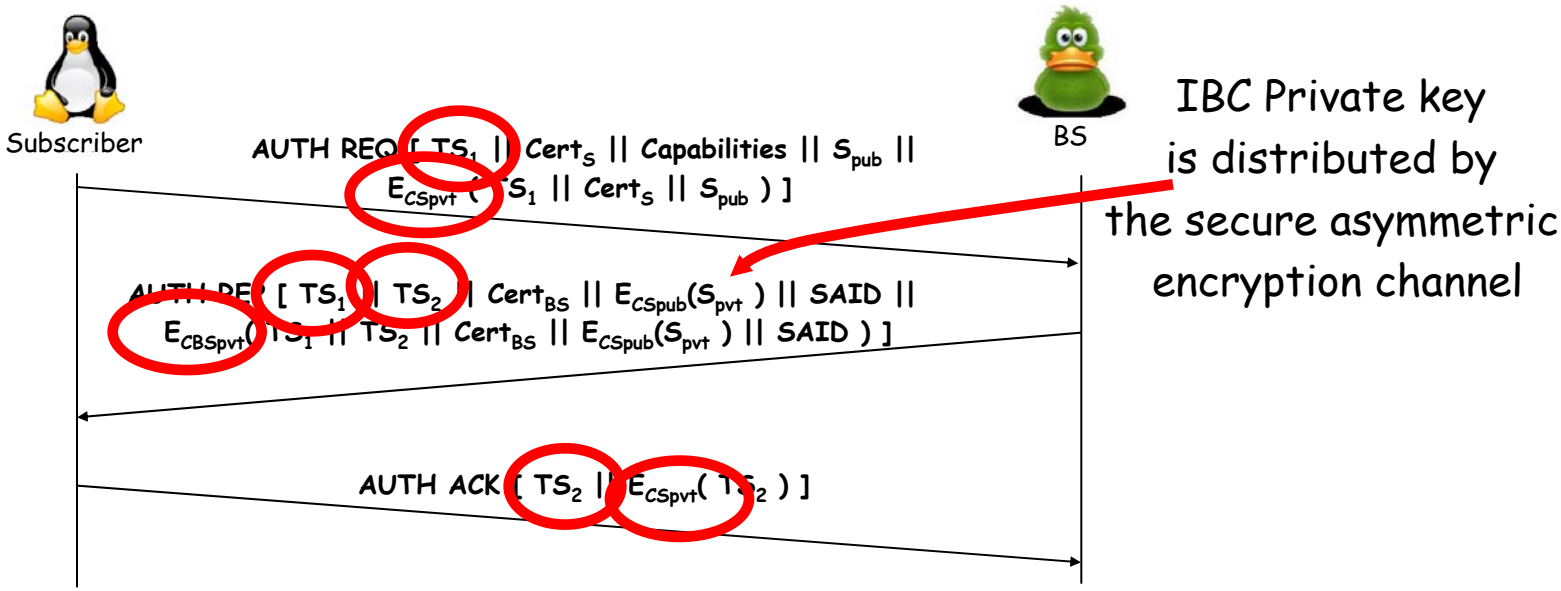


- Unauthenticated malicious node subscription is prevented by adding BS_{id} to S_{pub}.



The mutual authentication is done by using X.509 certificates and IBC private keys are distributed (step 2)

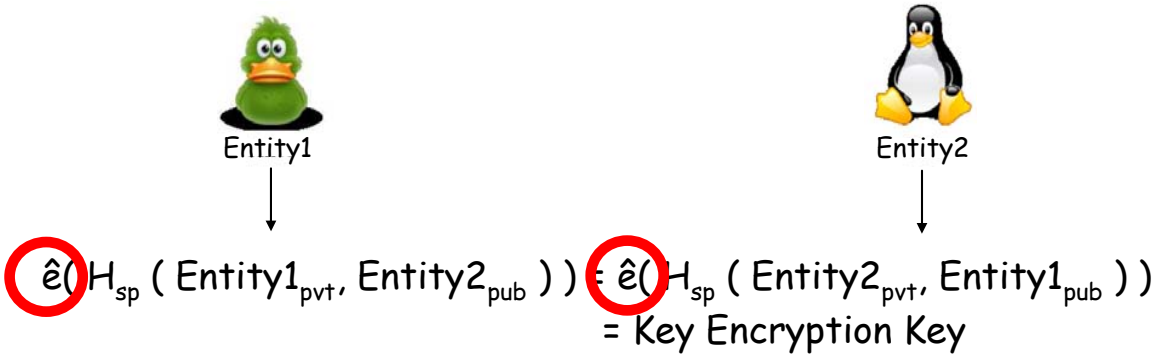
- Step 2: Mutual Authentication



- **Important:** The IBC private key is distributed by this secure channel to subscribers
- Messages are signed against forgery
- Timestamps added against replay attack (Alternatively nonces can be used)

Key Encryption Keys are formed by using the bilinear mapping (details of step 3a)

- Step 3a: Key Encryption Key Formation



- Bilinear Pairing is used for KEK formation
- The Bilinear Diffie Hellman Problem is a NP complete problem

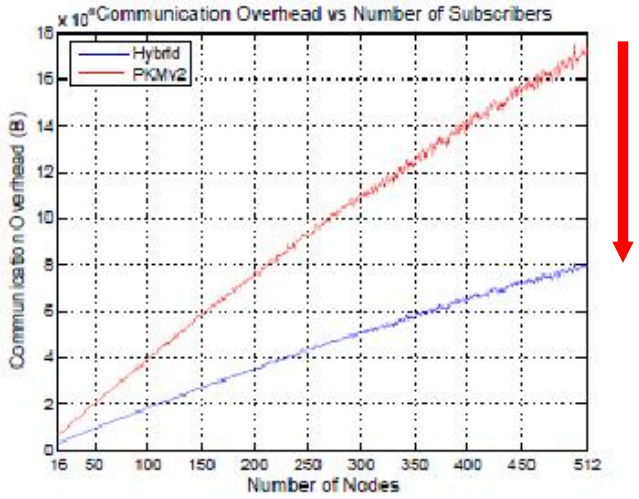
For better comparison of our work with PKMv2, communication overhead was estimated

- Mobility Model
  - Similar to random waypoint model
  - Subscribers are distributed around a BS with a normal distribution.
  - The probability distributions of the directions are uniform.
  - The probability distributions of the speeds are normal with a mean zero.
  - 10 runs for each simulation
- Using our model and the assigned values we compared the performance of our **IBC based scheme** with **PKMv2**.

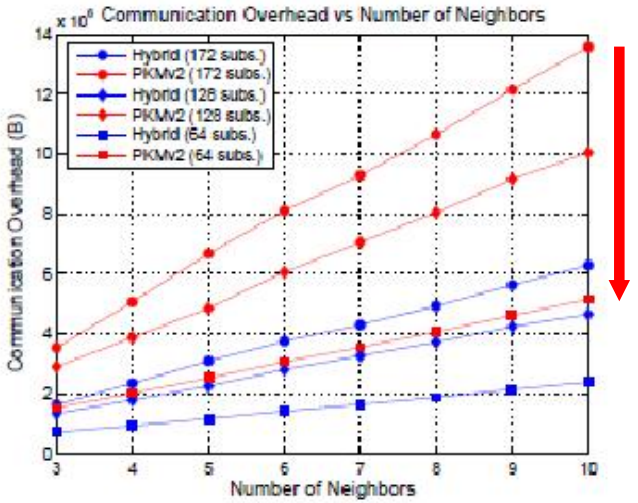
- Cryptographic Parameters
  - Timestamp: 8 bytes
  - BSpub, Spub: 30 bytes
  - CertS: 1000 bytes
  - BSid, Sid: 4 bytes
  - AKseq: 0.5 bytes
  - OSSseq: 0.5 bytes
  - SAID: 4 bytes
  - Param: 50 bytes
  - BSpvt, Spvt: 128 bytes
  - HMAC, Epvt: 128 bytes
  - AK (MSK): 32 bytes
  - OSS: 32 bytes
  - TEK param: 50 bytes
  - Capabilities: 50 bytes

On the average reduced number of messages and their sizes increased the efficiency by 53 %

- To observe the effect of varying number of subscribers
  - 16 to 512 subscribers used
  - Movement variation is 400,
  - Connection range is 100 meters
  - Each can form maximum 5 links
- Around 50% decrease in bandwidth usage



- To examine the impact of possible number of neighbors
  - 3 to 10 number of neighbors
  - 64, 128 and 172 subscribers
  - Variance of movement is 400
  - Connection range is 100 meters
- Around 53% decrease in bandwidth usage



The proposed hybrid approach has achieved a desired security and performance level

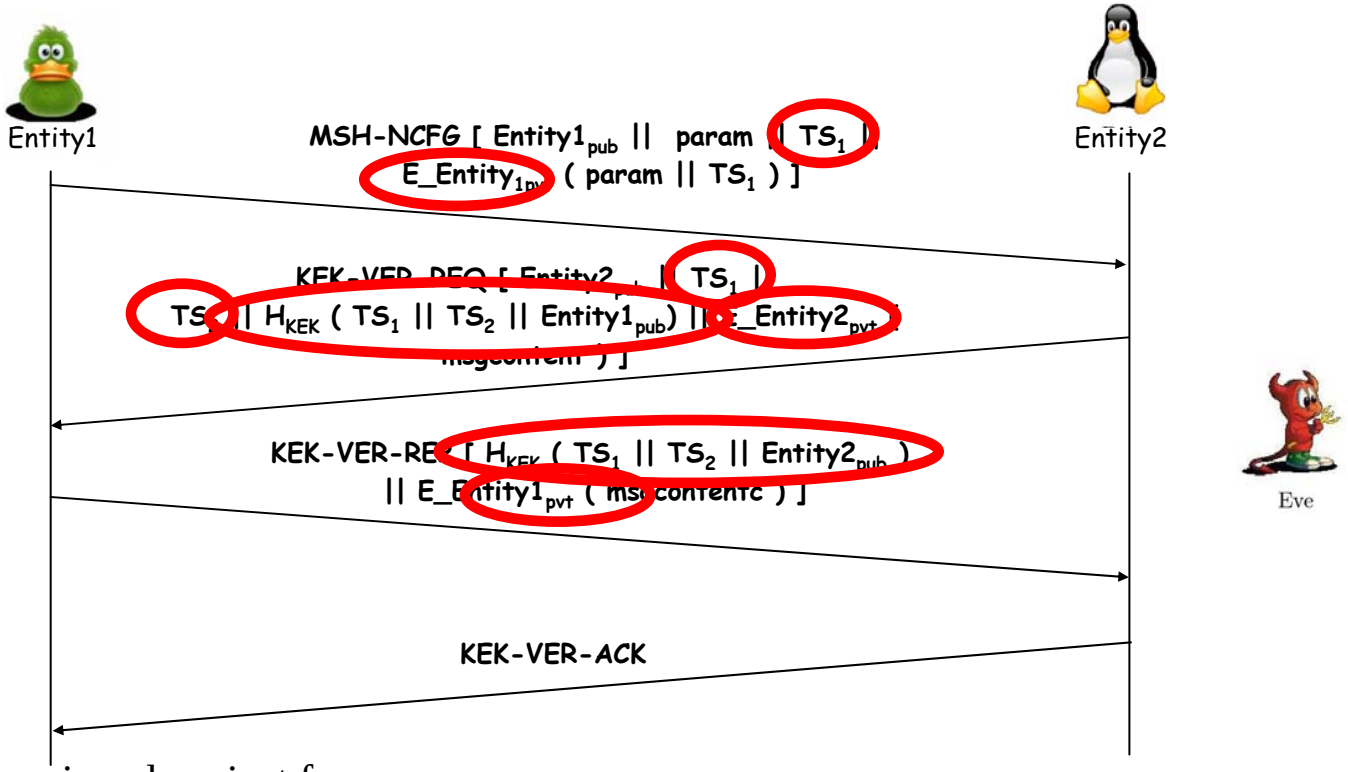
- IBC Based Hybrid Scheme for WiMAX
  - A comprehensive solution for both WiMAX modes of operation and for both subscriber types
  - Maintains the communication overhead at a minimal level.
  - Authenticates entities using X.509 certificates mutually
  - Forms fast and multiple links between entities
- What we are doing now:
  - We completed a key renewal process for IBC based security methods.
  - As the future work, we intend to study handover between different BSs and SPs using the properties of Hierarchical IBC.

Thank you

Questions?

KEK are verified without actually transferring them, but using HMAC'ed timestamp comparison

- Step 3b: Key Encryption Key Verification



- Messages are signed against forgery
- Timestamps added against replay attack
- KEK is verified but without actually being transferred. HMAC'ed timestamps are compared

Traffic Encryption Keys are formed on both sides by HMACing information from both ends

- Step 4: Traffic Encryption Key Formation

- Keyed-Hash Message Authentication Code (HMAC) is used (1024 bit codes are suggested)
- The key discovery risk by the malicious nodes is eliminated