Formal Verification of Initial Network Entry in WiMAX Networks

Beth N. Komu, Mjumo Mzyece and Karim Djouani
Department of Electrical Engineering/French South African Institute of Technology
Tshwane University of Technology, Private Bag X680, Pretoria 0001, South Africa
Tel: +27 (0) 12 382 4191, Fax: +27 (0) 12 382 5294
Email: {bethkomu@gmail.com, mzyecem@tut.ac.za, djouanik@tut.ac.za}

Abstract- The Initial Network Entry procedure is the first stage in establishing a connection in an IEEE 802.16 (WiMAX) network. The process involves the transmission of unencrypted management messages, which constitutes a major security flaw. The Man-In-The-Middle (MITM) attack exploits this weakness in the network by eavesdropping, interception and fabrication of the management messages, resulting in a breach in the reliability of the entire network. In this paper, we analyse a modification of the Diffie-Hellman key exchange protocol proposed to mitigate the man-in-the-middle attack in WiMAX by modelling the protocol in Promela. Verification is then performed by use of the Spin model checker with the concurrent interaction of an intruder process so as to prove or disprove the protocol’s validity.

Index Terms— WiMAX, Initial Network Entry, Man-in-the-Middle, Formal analysis, Spin

1. INTRODUCTION

A. Background

The Worldwide Interoperability for Microwave Access (WiMAX-802.16) is an emerging standard that offers broadband wireless access with high bandwidths and transmission rates. However, like all other wireless networks, WiMAX is vulnerable to network attacks that compromise the radio links between the communicating Subscriber Station (SS) and the serving Base Station (BS) [1] [2]. With the integration of mobility in the 802.16e-2005 Mobile WiMAX standard [3], complexities in ensuring secure access to the network are introduced. Mobile WiMAX employs the Privacy and Key Management protocol version 2 (PKMv2) that supports robust mutual authentication mechanisms, the Advanced Encryption Standard (AES) and message confidentiality by of use Hash-based Message Authentication Code (HMAC) or Cipher-based MAC (CMAC).

Unfortunately, even with its enhanced security measures, Mobile WiMAX is still considered vulnerable to network attacks. One such threat is the MITM attack that targets the unencrypted management messages at the Initial Network Entry point be it in Fixed WiMAX (802.16d-2004) or Mobile WiMAX. The Initial Network Entry process in WiMAX consists of security-sensitive unprotected management information being exchanged between the respective communicating parties for ranging, capabilities negotiations, authentication and key exchange and registration purposes. The Advanced Encryption Standard (AES) implemented by Mobile WiMAX only protects the data messages after the Initial Network Entry procedure, leaving the MAC management messages to be sent in the clear and thus exposing them to the man-in-the-middle attack.

The MITM attack passively listens to an insecure channel of communication, in this case, the Initial Network Entry procedure, creates detailed profiles of the victim Subscriber Station (SS) inclusive of its security settings and associations with the serving Base station (BS), imitates the legitimate station and then modifies the management messages exposing the network to other destructive attacks like replay attacks, masquerade attacks and denial-of-service (DoS) attacks. The MITM attack fools legitimate stations participating in a communication process into operating as if they are still communicating with each other while disrupting the efficient functioning of the network [4].

B. Related Work

Most research work done on the security of Mobile WiMAX did not establish any security leaks due to the extra security capabilities integrated in PKMv2 and thus assumed that the Initial Network Entry point is secure. A few papers have analysed the Initial Network Entry process in WiMAX and proposed various security protocols aimed at mitigating the MITM attack which are believed to be correct and resistant to malicious manipulation.

Formal methods for protocol analysis and verification have so far been successfully used to check for correctness in communication protocols and complex sequential circuit designs. Model checking [5] is an automatic formal verification approach that entails correctly modelling the specific protocol into a formalism accepted by a certain model checking tool, specifying the properties that the design must satisfy and automatically verifying the protocol by producing traces for purposes of protocol analysis. Different tools for formal verification have been successfully implemented to expose vulnerabilities that may still exist in security protocols especially in WiMAX, a clear indicator on the emphasis of correctness of security protocols. The authors of [6] applied the Scyther tool to expose vulnerabilities in the PKMv1 and PKMv2 authentication protocols implemented in WiMAX. They
discovered a breach in information confidentiality in both protocols. Similarly, the authors of [7] proposed the use of TLA+ to check for denial-of-service (DoS) attacks in network protocols especially in authentication and ranging processes in WiMAX. They identified some possible DoS attacks in the Initial Ranging process, but by using their attacker model, they could not detect a DoS flaw in PKMv2. The authors of [8] implemented the Strand space method to uncover the MITM attack in cryptographic authentication protocols. By finding a match between the participating principals’ protocol parameters, the approach was a guideline to detecting a flaw in the authentication protocols. In addition, the authors of [9] also analysed the vulnerabilities of Mobile WiMAX and came up with a new model using the Strand Space approach, but inclusive of Athena (a model detector) to cater for the state explosion problem present in other modelling tools. The model proved resistant to attacks that compromise the confidentiality and authentication of WiMAX.

Simple Promela Interpreter (Spin) [10] is yet another Model Checking tool used to identify protocol weaknesses. Process Meta-language (Promela) is the description language for Spin used to implement the individual principal’s processes in the protocol. The authors of [11] analysed and verified the Needham-Schroeder Public Key Authentication protocol using the Spin model checker and succeeded in identifying a crack in the protocol. Likewise, the authors of [12] used the same approach as [11] to analyse and check for correctness in the Helsinki protocol and were successful in discovering a flaw in the protocol.

C. Focus of this paper

In this paper, we present the vulnerabilities of the basic Diffie-Hellman key exchange protocol and focus on the modified version of the protocol proposed by the authors of [13] towards curbing the MITM attack. We apply the Spin Model Checking tool to model the proposed protocol and an intruder process with MITM capabilities in Promela formalism and to verify the protocol’s validity. We borrow the concept of process formalism of the principals in the protocol from [11] and [12].

Section 2 explains basic and modified versions of the Diffie-Hellman (DH) key exchange protocol. Section 3 presents a Promela-based model of the DH key exchange protocol and its associated results. Section 4 concludes the paper.

2. DIFFIE-HELLMAN (DH) KEY EXCHANGE PROTOCOL

A. Basic Version

The Diffie-Hellman key exchange protocol [14] [15] [16] originally supports unauthenticated key agreements between stations wishing to communicate. The stations need not know each other’s identities to establish a shared secret key through exchanging their public key messages in an open channel. This poses a threat since a malicious station can exchange its own public key with a legitimate base station (BS) or can exchange it with a legitimate mobile station (MS) so as to generate the shared key used for encryption purposes. This compromises the security of the entire WiMAX network and thus entity authentication before implementation of the Diffie-Hellman key exchange protocol is vital as proposed by the authors of [13]. The basic version of the Diffie-Hellman protocol is described as follows:

Message 1: MS _ PkMs → BS
Message 2: MS _ PkBs → BS

where:

- PkMS = G^a mod P
- PkBS = G^b mod P
- PkMS is the mobile station’s public key
- PkBS is the base station’s public key
- G and P are global variables called primes numbers and G is a primitive root of P
- ‘a’ and ‘b’ are the private keys of the mobile station and the base station respectively.

After the respective exchange of the public keys, the MS and the BS calculate the shared encryption key as follows:

Ka = (PkB)^a mod P
Kb = (PkMS)^b mod P

Since the resulting key is shared, it implies that Ka = Kb.

B. The Modified Diffie-Hellman Key Exchange Protocol as proposed in [13]

The first phase of the implementation of the modified Diffie-Hellman protocol towards curbing the MITM attack involves entity authentication of the principals wishing to communicate over the WiMAX network. A mobile station (MS) claiming to be legitimate receives a challenge (Nb) from the serving base station (BS). It calculates the solution to the challenge using its cryptographic function and then sends the result and its identity to the BS. The BS confirms the MS’s solution and sends an acceptance token as proof of authentication. Upon receipt, the MS sends a challenge (Na) to the BS which calculates the corresponding solution based on the MS’s cryptographic function and sends it to the MS. The MS in turn verifies the solution and sends back an acceptance token to the BS as proof of successful authentication. Finally, successful mutual entity authentication is achieved. In this model, it is assumed that it is only the legitimate BS and the legitimate MS that have knowledge of the cryptographic function used to calculate the challenge sent in the protocol run. Therefore, a perpetrator in the network is not able to bring forth the correct value to the given challenge and is thus isolated as an intruder to the network. This process is illustrated in Figure 1 below.
After successful authentication, the basic Diffie-Hellman key exchange protocol is adopted to generate a shared encryption key with trust having been established between the MS and the BS. The symmetric key generated together with the Vernam Cipher is used to encrypt the unprotected management messages.

3. METHODOLOGY AND RESULTS

We employ the Spin model checker tool to check for vulnerabilities in the modified Diffie-Hellman protocol.

A. The Promela Equivalent of the Modified DH protocol

We first implement the entities in the proposed protocol and their protocol sessions in Promela formalism without interference from an intruder station. The mobile station is the Initiator of the protocol run while the Responder is the serving base station in the WiMAX network. The Responder takes part in the protocol run with the Initiator if, and only if, the Responder initiates a protocol session with the Initiator. On the other hand, the Responder commits to a protocol session with the Initiator if, and only if, it has correctly finished the session with the Initiator. The authentication property in this Promela model is expressed in this light. The Responder will only commit to the Initiator if the latter is correctly authenticated by the Responder and the same applies to the Initiator, if it correctly validates the identity of the Responder as expressed in the challenge-response process of the model in Figure 2. Nb is the nonce generated by the Responder, while Na is the nonce generated by Initiator. The Legit token in the respective principals’ processes is an indicator that successful authentication has been achieved. The Promela equivalent model of the protocol is shown below.

In the above Promela model, the International Subscriber Station Identity (ISSI) as specified in [13] is represented by unique letters like ‘A’ which in this case represents the Initiator’s identity. The cryptographic function implemented herein is set to a constant value only known to the MS and the BS while the respective nonces in the protocol run are assigned different values in each process. This model of the DH protocol assumes that identity authentication of principals that want to communicate in the WiMAX network is securely achieved through the challenge-response procedure illustrated in Figure 1. The basic DH protocol is then implemented after entity authentication at step 26 of Figure 2 to establish a shared encryption key. Pk_Ini in the model is the Initiator’s Public key while Pk_Res is the Responder’s Public key. n and g are global prime numbers used to calculate Pk_Ini and Pk_Res.

B. The Promela Model with the Intruder’s Interference

The initial knowledge of the Intruder is made up of the identities of the participating principals in the protocol run and its own identity and generic data, developed from scratch. The modelled Intruder process with MITM capabilities intercepts all the sent messages in the protocol run so as to increase its knowledge for attack launch. Based on the results we got, the most valuable items in the protocol run are successfully captured by the adversary inclusive of the generated base station’s nonce. The results generated from the respective nonces and cryptographic function as a measure of the principal’s validity, are easily intercepted by the Intruder since any measure of confidentiality to the critical information is lacking. This information can be used...
by the Intruder to fool the legitimate principals that they are actually communicating with each other yet they are exchanging messages with the Intruder and thus the MITM attack. The simulation results obtained are shown below.

![Figure 3: The Modified Diffie-Hellman Output with the Interference of an Intruder process.](image)

The Subscriber’s Station authentication fails the first instance as shown in the output window in Figure 3 since the Intruder’s process did not match the cryptographic function used to calculate the result even after successfully capturing the nonce from the Base Station. The Responder fails to commit to the Initiator and so does the Initiator, as indicated by ResCommitAB = 0 and IniCommitAB = 0 in Figure 3. This is because most independent principal’s communication takes place with the Intruder and never with both the legitimate stations at a single protocol run. The Intruder’s process floods the channels with parameters in its knowledge in an attempt to penetrate the network and launch an attack as illustrated by the ‘too many params in rv-send’ statement in Figure 3. Generally, it is evident that the protocol proposed by [13] has traces of weaknesses against the MITM attack.

A summary of the verification results obtained is shown in Figure 4. Without the intruder process interference, the number of reachable states for the verification of the authentication property (B correctly authenticates A, and A correctly authenticates B) is observed to be great compared to the protocol run with the intruder’s interference. This is because communication takes place between legitimate processes uninterrupted, and in turn, all the authentication parameters are set to 1, an indicator that authentication is successful. On the other hand, an error is observed in the protocol run with the intruder process interference at depth 17 since the authentication property is violated at this step and Spin ceases to search the entire state space. Moreover, the authentication parameters keep on changing in each simulation due to the constant interruption by the intruder process which disrupts the normal operation of the protocol.

<table>
<thead>
<tr>
<th>Without Intruder process interference</th>
<th>With Intruder process interference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Depth reached</td>
<td>39</td>
</tr>
<tr>
<td>Errors</td>
<td>None</td>
</tr>
<tr>
<td>States stored</td>
<td>38</td>
</tr>
<tr>
<td>Authentication parameters</td>
<td>All 1s</td>
</tr>
<tr>
<td>IniRunning, ResRunning, IniCommit, ResCommit</td>
<td>Varying</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4: Verification results comparison table

4. CONCLUSIONS

In this paper, we have modelled a modified cryptographic protocol using Promela, in this case, the Diffie-Hellman key Exchange protocol. We further modelled the Intruder process with MITM capabilities and introduced it to the specified protocol for behaviour analysis. The Intruder model is the most difficult to develop due to its varied behaviours as illustrated in [2] and the never-ending interactions with a legitimate protocol run. Nonetheless, we succeeded in identifying some traces of vulnerability in the identified protocol. Our future works include specifying the protocol’s properties to be checked in Spin using Linear Temporal Logic (LTL) as a measure of improving the verification process.

Beth Komu is currently studying towards her Master of Technology degree at Tshwane University of Technology. Her research interests include Security in Wireless Networks, WiMAX Network and Formal verification of communication protocols.

Mjumo Mzyece is an associate professor at the French South African Institute of Technology (F’sATI) in the Department of Electrical Engineering at Tshwane University of Technology (TUT) in Pretoria, South Africa, where he is engaged in research and teaching on communications-related themes. His research interests are in next generation wireless networks, particularly those built around TCP/IP; the design and evaluation of communications protocols; and the interaction of technological and other critical factors (e.g. policy, regulatory, commercial/economic, etc.). Outside of the academic world, he has held various technical, management and consulting roles.

Beth Komu
Mjumo Mzyece
positions locally and internationally. He holds a BEng (Honours) degree in Electronic & Electrical Engineering from the University of Manchester (England), an MSc (with Distinction) in Communications Technology & Policy and a PhD in Electronic & Electrical Engineering, both from the University of Strathclyde (Scotland).

Prof. Karim Djouani is a professor, scientist and the technical group supervisor of soft computing, complex systems and optimization. He works at the French South African Institute of Technology (F'SATI) at Tshwane University of Technology and with the SCTIC team of the LISSI lab, University Paris Est. His current works focus on the development of novel and highly efficient algorithms for reasoning systems with uncertainty as well as optimisation, for distributed systems, networked control systems, wireless ad-hoc network, wireless and mobile communication, wireless sensor networks and robotics.

REFERENCES


