CS 259 Final Report

Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol

Ju-Yi Kuo

1. Protocol Overview

802.16 is the wireless MAN standard for metropolitan area networks, and 802.16e is the amendment that enhances the standard to support mobile subscriber stations moving at vehicular speed. This report is based on the Sept 2005 draft standard of 802.16e. The standard includes several sub standards that govern how a mobile station (MS) communicates and authenticates to the base station (BS) in order to obtain various kinds of services. Our analysis focuses on the optional Multicast/Broadcast Service (MBS) group security association rekeying protocol in the spec.

Basically, each MS can subscribe to multiple MBS groups, and BS will multicast/broadcast group specific contents to subscribers. The purpose of the MBS security protocol is to distribute keying material which ensures that only subscribers can receive the content; unauthorized MS cannot steal the service.

But this MBS rekeying protocol does not handle a mobile station's initiation into the network nor its authentication to the base station. Before a MS starts this protocol to obtain MBS service, the following are assumed:

1. MS has already authenticated to the BS, perhaps using its embedded X.509 certificate.
2. MS has obtained a authorization key (AK) which is a long term secret shared between each MS and BS.
3. MS obtained a Key-Encryption-Key (KEK) which is used to encrypt traffic keys. This KEK is also a pair wise secret shared between each MS and the BS.
4. MS has established a group security association (GSA) with the BS for a particular group, or groups. For each group it has a GSA, it acquired a MBS authorization key (MAK) which is shared by all members of that group. How a MS receives the MAK is outside the scope of this spec.
5. The way that a MS leaves a group or the BS revokes its group membership is also outside the scope of this spec

Getting MAK and revoking group membership is not specified, probably to support flexibility of implementation. They should be implemented by higher layer protocols. In order to illustrate the details of the protocol, the following terminologies need to be explained:

- MS and BS mac address: they all have imbedded 48 bit media access control address. Part of the BS mac address is the carrier identification code.
- CID: a 16 bit connection ID. This identifies a connection between a MS and the BS. Each MS establish a connection with the BS with a different CID.
- GSAID: the ID of the group.
- UL & DL: uplink and downlink.
- GKEK: group key encryption key.
- GTEK: group traffic encryption key. This is changed more often than GKEK.
- MAC: message authentication code. The spec supports 2 MAC implementations, HMAC or CMAC.
- MAC keys: keys used to generate the MAC. There are 3 different kinds of MAC keys as explained below.

There are 2 types of communication between MS and BS: they can unicast to each other using the CID to identify destination, or the BS can multicast contents down to member MSs using the GSAID to identify the group. The MBS rekeying protocol consists of 2 sub-protocols. When a MS does not have any keying material, it is in the **Start** mode; it will use the following sub-protocol to request them from the. First, MS will send a KeyReq message to BS and enter into the **OpWait** mode. Upon authenticating the message, the BS will reply with the KeyRsp message:

MS -> BS: **CID, AK Seq#, GSAID, Nonce, PN_U, MAC**$_{MK\_U}$

BS -> MS: **CID, AK Seq#, GSAID, Nonce, {GTEK}**$_{GKEK}$**,**
GTEK Params, {GKEK}$_{KEK}$**, GKEK Params, PN_D,**
MAC$_{MK\_D}$

When MS receives the KeyRsp message it enters the **Operation** mode. PN_U and PN_D are unicast uplink and downlink packet number counter. They are incremented upon sending each packet. MK_U and MK_D are unicast uplink and downlink MAC keys. The GKEK and GTEK key parameters include key lifetime (in seconds), crytography parameters, etc. The entire message is MACed.

The BS would periodically timeout and rekey the entire group. BS re-distributes the GKEK by sending the KeyUpdGKEK message to MS's. This is done through unicasting to each MS in the group respectively:

BS -> MS: **CID, AK Seq#, GSAID, GKEK Counter, {GKEK}**$_{KEK}$**,**
GKEK Params, PN_D, MAC$_{MK\_D}$

BS re-distributes the GTEK by sending the KeyUpdGTEK message to MS's. This is done through multicasting to the entire group once:

BS -> MS: **GSAID, GTEK Counter, $\{GTEK\}_{GKEK}$, GTEK Params,**
PN_D, MAC_{MK_MBS}

MK_MBS is the MBS multicast MAC key. GKEK and GTEK counters are incremented for each generation of keys. The BS would rekey GTEK more often than the GKEK. But if GKEK is rekeyed, GTEK would definitely be rekeyed.

Key hierarchy is also specified in the standard. They are:

- MTK: this is the actual key used to encrypt the traffic. It is derived from MAC + GTEK.
- MK_U and MK_D are derived from AK + MS & BS mac addresses.
- MK_MBS is derived from GKEK.

2. Security Goals

We analyze this protocol using the murphi modeling tool. In the murphi model, the following security goals are checked:

- Secrecy of all KEK, GTEK and GKEK from MS's outside the group
- Secrecy of UL Mac Keys, DL Mac Keys, and MBS Mac Keys from MS's outside the group
- Membership Authentication
  - When MS is in **Operation** mode or **Start** mode, both MS and BS should agree on whether it is a member of the group or not. If the KeyReq message is being used as an evidence that the MS wants to join the group, then this security goal would be important.
- Key Lifetime Integrity
  - The lifetime of a key cannot be prolonged by any message.
- Key Parameter Integrity
  - Key parameters accepted cannot be different from what the BS specifies in the message. This prevents version rollback attacks.
- Key Freshness
  - MS always accepts the new generation of keys that BS demands, never older generations that has been used before.
- Cross Group Security
  - Even if the intruder joins group A (but not group B), he is not able to use his Dolev-Yao capability to compromise the privacy of group B. An intruder may join a low privilege group legally in order to compromise a high privilege group, hence the purpose of this security goal.

The following are not security goals:

- Compromised BS. BS is assumed to be honest. This is not saying that an intruder cannot impersonate the BS. The intruder can still impersonate the BS because CID is visible. If a MS accepts any KeyRsp or KeyUpd message sent by the intruder, then the intruder has successfully impersonated the BS. But this situation is already covered by the secrecy of group key & MAC key & key parameter security goals above because only when the MAC keys are compromised would the MS accept a forged message.
- Compromised MAK or AK. Since MAK & AK are long term secrets and are never directly used to encrypt/decrypt, they are assumed to be secret.

3. Modeling Details

We analyzed a slightly simplified version of the MBS rekeying protocol. We did not model the timeout situations, nor the 2 simultaneously existing keys. The murphi model is rationally constructed. The intruder is modeled using the Dolev-Yao model as usual.

The dimensions used for a typical model run are:

- 1 base station, 2 mobile stations
- 1 intruder
- 2 groups
- 2 generations of GKEK for each group
- 2 generations of GTEK, per GKEK, per group
- Each MS can join & leave a group 2 times max

MAC keys are unique for each unicast direction and multicasting, therefore they are modeled as nonces unique to each group, each MS, and each msg type (Uni UL, Uni DL, and MBS). GKEK & GTEK are incrementing numbers, representing generations of keys. This would facilitate key freshness checking. Key Lifetimes, on the other hand, are modeled as decrementing numbers. They are decremented each time the BS sends out some keying material. The key parameters are modeled the same as the keys, meaning that each generation of keys possess its own set of parameters.

The intruder is modeled as one of the MS's. A boolean constant defines whether he can join a group or not (maximum 1 group). The purpose of this design is to model cross group security goal. In that situation, after the intruder/MS joins one group, the security goal would check whether the keying materials of all other groups can be compromised or not.

The multicast message is a special case because it needs to be received by all members of the group; we cannot remove it from the network after just one MS received the message.

Therefore it is being modeled as a single message which contains a multiset of recipients. Only when all recipients have processed it and remove themselves from the multiset will the message be removed from the net.

Since group membership revocation is outside the scope, a MS leaving a group is modeled as an event that takes place instantly at a safe point (not in the middle of rekeying). No message is passed. And when this happens, BS immediately sends KeyUpd message to rekey the entire group. This is reasonable because without knowing the details of the revocation, we can't predict how it would behave.

It is also assumed that each MS and BS would authenticate the MAC before accepting a message. Therefore if the MAC does not match the body of the message then it's useless for the intruder to send it. This would be a optimization when modeling the intruder behavior because we don't have to append random MAC to a forged message anymore, and the model state space would be much smaller.

4. Analysis

Model Analysis

Using the final murphi model we built, no violation was found in the model run. Denial of Service analysis is done through spec inspection and will be covered in the next section. However, during the progressive construction of the model, we found out that the packet number counter plays an important role. Before PN is integrated into the model, murphi found the 2 attacks:

KeyReq replay attack:

After MS leaves a group, the intruder can replay a recorded KeyReq message previously sent by MS. When BS receives this, it would accept it. And if this is considered a request to join the group by the implementation, then BS would re-enlist MS into the group without MS's knowledge. If the group service is charged by the minute, then BS will start charging MS without MS's permission. In this case, the Membership Authentication security goal is violated.

KeyUpdGKEK replay attack

Before the current GKEK expires on a MS, the intruder can replay a previously recorded GKEK Key Update message. When the MS receives this it would accept it. Although the GKEK remains the same, the lifetime in that message would certainly be longer than the current lifetime. This could prolong the life of GKEK for a long time, and it could disturb MS's operation to some degree. In this case, the Key Lifetime Integrity security goal is violated. Also, if the key parameter is different in the replayed message, the MS would be fooled into accepting it and this could be a version rollback.

After adding the PN, these 2 violations disappeared.

Denial of Service Analysis

DOS attack analysis is per formed through manually inspecting the spec. Enlightened by the discovery of the importance of the packet number, we also found a potential DOS attack against the BS if PN is not implemented.

The intruder can replay previously recorded KeyReq messages to the BS. These messages all contain valid MAC, therefore the BS would accept them; then creates and sends out KeyRsp messages. The cost for the BS includes receiving msg, authenticating it, encrypting keys, MACing it and sending it. The cost for intruder is storing the messages plus sending it over and over. This cost is small when amortized over many replays. Therefore the ratio of BS cost versus intruder cost increases over many replays. Once again the addition of packet number counter mitigates this threat.

5. Conclusion

The protocol seems to be secure on its own. Considering the importance of PN, the protocol implementer must pay attention to the wrap-around situation. PN is 4 bytes long, and when it exceeds the maximum value, it will start from zero again. The spec says that before this counter wraps around, a new AK should be negotiated. This ensures that the AK and PN combination would be unique, and this should mitigate the number wrap-around risk. It is important to implement this correctly, as PN is a critical security factor as we noted above.

But what happens when this protocol interoperates with other necessary protocols? This is not a complete MBS protocol because the way to establish the MAK and to revoke a MS's group membership is not precisely defined by the spec. These are handled by other protocols. The details of these other protocols could add some risk factors to the operation of the combined protocol. We need to model them together in order to get a better picture of the security of the entire protocol suite.

From my experience of using murphi to analyze this protocol, it seems to be a suitable tool for modeling many aspects of this protocol. Adding cost based DOS attack analysis seems to be straight forward. On the other hand, it could be challenging to model all the timeout periods specified in the standard.

Future work may involve analysis using protocol composition logic. PCL has been used to analyze other wireless network protocols; therefore it might be suitable for this protocol as well.