Misbehaviour metrics in WiMAX networks under attack

Misbehaviour metrics in WiMAX networks under attack

D. J. Parish and F. J. Aparicio-Navarro

Department of Electronic and Electrical Engineering,
Loughborough University, Ashby road,
Loughborough, LE11 3TU, U.K.
E-mail: d.j.parish@lboro.ac.uk

***Abstract*—Much effort has been taken to make WiMAX a secure technology. Due to its broadcast nature, WiMAX is more susceptible to security threats than a wired network. In this paper, we give a general overview of the security architecture and possible attacks that a WiMAX network may face. For each type of attack the misbehaviour metrics that may vary under these attacks are listed. This work can be used to select an appropriate threshold for detecting attack and can be applied to future research on IDS.**

***Index Terms*—WiMAX, Misbehaviour metrics, Key exchange, Wireless security, IEEE 802.16.**

I. Introduction

The IEEE 802.16 standard [1], also known as Worldwide Interoperability of Microwave Access (WiMAX), is a promising technology that has taken a growing importance as a way to provide high-speed broadband wireless access to the final user. The first amendment, IEEE 802.16-2001, was designed to operate within a frequency band of 10-66GHz, in a point-to-point or point-to-multipoint setting. After the 802.16-2004 amendment, WiMAX also supports the 2-11GHz frequency band, and the use of OFDM and OFDMA. WiMAX supports both, Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD). The amendment IEEE 802.16e added functionalities of mobility, and advances in security and Quality of Service (QoS). The latest amendment, IEEE 802.16j-2009, added a framework for multi-hop relay, also known as mesh networking.

Due to the broadcast nature of WiMAX transmissions, both the Subscriber Station (SS) and Base Station (BS) are inherently more susceptible to security threats than a wired network, such as interception, modification, impersonation or injection attacks. Much effort has been taken since the IEEE 802.16-2001 standard was approved, to make WiMAX a secure technology. Indeed, WiMAX specifies a security sublayer specifically to address all the security issues. It has sought to avoid the same mistakes that were conducted by WiFi, in security. In the IEEE 802.11 standard, security was added to the standard after the first standard and successive amendments were approved, that made WiFi a technology with several vulnerabilities. Even though, and despite of all efforts taken in security, the IEEE 802.16 standard still has vulnerabilities.

At present, several papers have been published to address these vulnerabilities in WiMAX. So far, mainly these papers are focused on summarising the type of attacks that a WiMAX network may experience [2], shows standard improvements in order to obtain stronger security [3], or both, summarise type of attacks and improve the standard security [4]. Currently, in wireless networks, researches attempt to secure these wireless networks by performing Intrusion Detection (IDS). Much progress has been made in technologies such as WiFi, within which IDS is a widely studied topic [5]. Several publications present studies that develop IDS based on cross-layer techniques [6]. However, little progress has been made in developing IDS focused on the IEEE 802.16 standard. One of the few publications in this area is [7], which describes a system to enhance the network resistance to jamming attack, based on a link adaption algorithm.

In this paper we give a general overview of the attacks that a WiMAX network may face, focusing on the MAC layer. According to each attack, the misbehaviour metrics that may vary under these attacks are highlighted. This study aims to facilitate the task of selecting an appropriate threshold able to reflect the behaviour of the communications, detect whether the network is under attack and apply to developing an IDS. This study is a subjective work. It has been done from what the IEEE 802.16 standard explains. No practical experiment has get been performed, but will form future work.

This paper is organized as follows. In section II, a brief overview of the security architecture in the IEEE 802.16 standard is given. In section III, the networks entry and key exchange protocols that the MAC layer performs are analysed. In section IV, possible attacks are presented and the misbehaviour metrics due to these attacks are listed.

II. Security Architecture

The IEEE 802.16 standard supports two types of transmission duplexing, TDD and FDD. In both, transmissions are scheduled using DL-MAP and UL-MAP messages, which describe the timing and contents of the downlink and uplink respectively. In the TDD case, the uplink is Time Division Multiple Access (TDMA), the bandwidth is divided into time slots within which an individual SS is allowed to transmit. The downlink schedules when the BS transmits. In the FDD case, uplink and downlink transmissions occur simultaneously on different frequencies.

In WiMAX, security is an important aspect to consider. The IEEE 802.16 standard provides a security sublayer in the MAC layer to support privacy issues across the wireless network, which provides security mechanisms for privacy and access control, such as authentication, authorisation, key exchange and encryption of data across the network. As

specified in [3], this security sublayer is based on two main components, an encapsulation protocol for providing packet data encryption, and a Privacy and Key Management (PKM) protocol for providing the secure distribution of the keying material and authorised access to connections between BS and SS.

As explained in more detail by [8], the encapsulation protocol determines the encryption and authentication methods supported by each SS. It consists of the data encryption algorithm, the data authentication algorithm and the Traffic Encryption Key (TEK) encryption algorithm. The PKM protocol defines the set of rules responsible for authentication and authorisation of the SS, periodic reauthorisation, reception and renewal of key material. As defined in [3], the PKM protocol can be divided in two main parts, authorisation and Authentication Key (AK) exchange, and the key management protocol, during which the TEK is exchanged. There are two versions of PKM protocols supported by the IEEE 802.16 standard. The protocol supported since the first IEEE 802.16 standard, PKMv1, which only provides SS authentication, and the protocol incorporated by the IEEE 802.16e standard, PKMv2, which provides mutual authentication and supports mobile SS.

The IEEE 802.16 standard introduces the idea of a Security Association (SA), a set of security parameters of the connection, such as selected encryption algorithms and keying method, that BS and SS share with each other, in order to establish secure communications. There are two types of SA, authorisation SA, responsible for protect the authentication of the SS, and data SA, responsible for protect the transport connections. More details of its structure are described by [8].

III. PHASES

A. Network entry procedure

SS goes through multiple steps to join a WiMAX network**.** The procedure aims to establish a communication between SS and BS, and negotiate the proper parameters utilised on this communication. Initially, the SS attempts to get synchronisation with the most suitable downlink frequency. Through the DL-MAP and Downlink Channel Descriptor (DCD) messages, the SS obtains information about the downlink characteristics, such as the downlink channel ID, modulation type, forward error correction code type, usage time and the BS ID. Similarly, SS gets information about the uplink characteristics from UL-MAP and Uplink Channel Descriptor (UCD) messages, as the Connection Identifier (CID) and the details of the initial ranging interval. If any of the downlink and uplink channels are unsuitable, the SS restarts the process attempting to synchronise with the next most suitable downlink frequency.

Since each SS has unique characteristics, it is critical to synchronise the channel parameters, such as transmission power level and timing, between SS and BS. The SS makes use of contention windows to randomly select one available ranging slot that the SS will utilise to perform the initial ranging. The BS uses a ranging response (RNG-RSP) message to inform the SS about the timing, transmission power level and frequency adjustments. Through the exchange of ranging request (RNG-REQ) message and RNG-RSP, the BS and SS negotiate these parameters.

Once the SS has obtained a determinate slot within which communicate to the BS, it determines and negotiates with BS the security parameters both will use in the authorisation protocol. It is done by exchanging basic capabilities request (SBC-REQ) and basic capabilities response (SBC-RSP) messages.

B. Authentication protocol

To establish a shared key between both, the BS and SS perform the authentication protocol. This protocol is begun by the SS sending its Cert(SS.Manufacturer) to the BS, which is used to verify and decide if SS is a trusted device or not. This authentication protocol is described in more detail in [3]. Afterwards, SS sends an authorisation request (Auth-REQ) message, requesting for an authentication key (AK) to the BS. This message consists of the X.509 certificate of SS, which contains the Public Key (PK) and MAC address of the SS, its security capabilities, which are the authentication and data encryption algorithms supported by SS, and a SA identification (SAID).

After having validated the SS identity, the BS generates an AK and sends it to the SS, via an authorisation replay (Auth-REP) message. This message contains the AK, which is RSA encrypted by the PK of SS, a sequence number to differentiate between consecutive AK (SeqNo), AK lifetime and a SAIDList. Besides, if the SS identity is not validated, the BS replies with an invalid authentication (Auth-INVALID) message, rejecting the request of SS.

This protocol differs in some aspects to the new authentication protocol, PKMv2, illustrated in Fig. 1. The AK is simultaneously derived by BS and SS. Instead of generating an AK by itself, the BS derives and sends to SS a pre-AK. Once exchanged, both SS and BS are able to generate the same AK from this pre-AK. Additionally, PKMv2 provides mutual authentication between BS and SS, adding the Cert(BS), X.509 certificate of BS, within the Auth-REP message, that is used by the SS to verify the identity of BS. Also, in other to avoid any message that could be replayed, some numbers-used-once (nonce) are added and an additional Auth-Acknowledgement message.

Once the AK lifetime expires or is about to, the SS sends an Auth-REQ message to the BS, requesting new keying material. The BS generates a new AK or pre-AK, depending

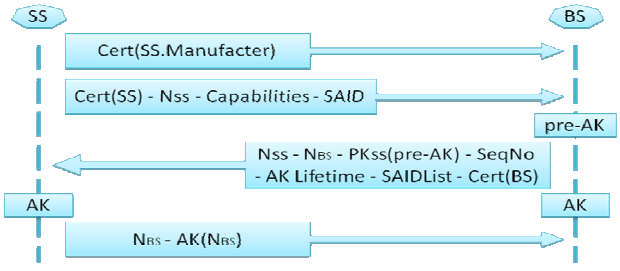

Fig. 1. PKMv2 Authentication protocol.

on the protocol, and sends it to the SS within in an Auth-REP message [9]. During the time the current AKs remains active, both AK are active simultaneously. In case the AK expires before reauthentication, the BS will treat the SS as unauthorised.

C. *Key management protocol*

Once BS and SS share the AK, a key management protocol, exchanges a TEK between both two. The Key Encryption Key (KEK), which is derived from the AK, is used to encrypt the transfer of the TEK. BS always maintains two active sets of keying material per each SAID, to prevent data traffic corruption when the currently used TEK expires, OldTEK and NewTEK. Duration of these two TEKs overlaps. Before one TEK expires, the new TEK is activated and a new one is requested.

The process, illustrated in Fig. 2, may be started by either, by the BS sending the Rekey message, if it determines rekeying is necessary, or by the SS with the Key-Request message. The Rekey message consists of SeqNo, a sequence number, sent to SS in the Auth-REQ message by BS, to differentiate between consecutive AKs, SAID which represents the rekeyed SA, and the HMAC(1), which is derived from the AK and allows the SS to authenticate the message and detect message forgery.

The Key-Request message consists of a SAID, the HMAC(2), which allows to the BS to authenticate the message and detect message forgery, and SeqNo. In case HMAC(2) is not valid, BS rejects this request by sending a Key-Reject message to SS. Otherwise, BS replies with the Key-Reply message, which includes renew keying materials, OldTEK and NewTEK, HMAC(3), SeqNo and SAID.

The aim of TEK exchange is to provide data traffic encryption. The employed encryption method varies between each standard. According to [10], the IEEE 802.16-2004 standard only supports DES-CBC, while the IEEE 802.16e standard supports DES-CBC and AES in different modes, CBC, CTR, CCM, ECB and AES-Key-Wrap.

IV. Vulnerabilities and Misbehaviour Metrics

PHY Layer

As with other wireless technologies, WiMAX is vulnerable to different types of *Jamming attacks*. Jamming, considered as a Denial-of-Service (DoS) attack, is the act of injecting interference into the frequency channel being utilised by BS and SS, at a level high enough to disrupt the authorised wireless communication.

These attacks can be summarised as brute force jamming, periodic jamming, precision jamming or message flooding. In brute force jamming, an attacker constantly injects a noise signal into the frequency channel used by the BS and SS. In periodic jamming, an attacker injects a noise signal, intermittently, for short intervals of time, either with a static or variable periodicity. In precision jamming, an attacker injects a noise signal, for short intervals, during the BS or specific SS transmissions, and only over determined messages. This type of attack requires the attacker to have knowledge of when messages of a specific source or destination are being sent. In Message flooding, an attacker constantly sends messages, in order to keep the destination of the messages busy processing or rejecting them.

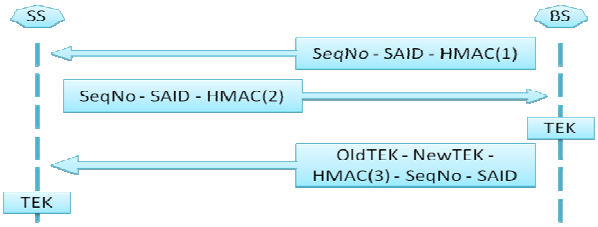

Fig. 2. Key management protocol.

Jamming is an easy attack to mount and difficult to prevent. Indeed, there is no mechanism efficient enough to protect against jamming attack on wireless networks. Some of the defence mechanisms are based on link adaption, for instance, increasing the power of signal transmission or using spectrum spreading techniques as Frequency Hopping Spread (FHSS) and Direct Sequence Spread Spectrum (DSSS).

Under jamming attack, there would be expected to be:

- A variance in the signal-to-noise rate.
- An increased number of collisions in slots different to the ranging slots, which theoretically are collision free.
- An increased number of switches of the frequency used for communication.

MAC Layer

1) *Network Entry Procedure*

An *Eavesdropping attack* is based on intercepting messages exchanged between BS and SS and obtaining sensible information. An attacker may create a detailed profile about the BS or SS, including capabilities or security information, and afterwards performs an active attack, such as DoS. Eavesdropping is a passive attack difficult to detect because it does not modify the intercepted data traffic.

As said, the information exchanges between BS and SS before the authentication protocol and the MAC management messages are unencrypted. An attacker may easily obtain secret information from these messages. Reference [2] gives a summary of unencrypted messages exchanged during the network entry procedure and the information that an attacker may obtain from them.

Some of the messages that an attacker may obtain secret information from are DL-MAP, DCD, UL-MAP, UCD, RNG-REQ and RNG-RSP, which contain timing information. Therefore, an attacker can determine the specific moment when the BS or SS is going to transmit, and use it to facilitate a *Jamming attack*.

The SS stays in synchronisation with the BS as long as it keeps receiving DL-MAP, UL-MAP, DCD and UCD messages at specified intervals of 600ms and 50s, respectively [2]. If an attacker disrupts one of these messages, it causes loss of synchronisation, and consequently, the SS will try to synchronise with the next more suitable downlink frequency.

Under a jamming attack, there would be experienced:

- A low number of DL-MAP, UL-MAP, DCD or UCD

messages received by the SS.

- A high number of RNG-REQ messages, with different CID, sent by an individual SS.
- A difference between the number of sent SBC-REQ messages and the number of received SBC-RSP messages.

As happens with the messages explained above, if an attacker disrupts the RNG-REQ, RNG-RSP, SBC-REQ or SBC-RSP messages within a given period of time, the SS will restart the full process.

During initial ranging, the SS makes use of contention windows to select an available ranging slot. Once a slot is selected, the SS transmits and waits for a RNG-RSP message. If the response message is not received within 50ms and 200ms, it assumes that a collision has happened and will select a ranging slot within a larger backoff time period before retransmitting again, using this time a higher transmission power level [2]. If an attacker disrupts the retransmission for a maximum of 16 times, the SS will restart and try to synchronise using another downlink frequency.

This would lead to:

- An increase in the number of collisions within the ranging process.
- An appreciable increase of the delay to accomplish the ranging process.
- An increase in the value of the backoff period for an individual SS.
- The number of times that a RNG-REQ message is sent by an individual SS, using the same CID, would reach 16.
- A difference between the number of sent RNG-REQ messages and the number of received RNG-RSP messages.

The RNG-RSP message, transmitted by BS in response to a RNG-REQ message, contains timing information, transmission power level and frequency adjustments that the SS uses to set its parameters. Also, the BS is allowed to send a RNG-RSP message in order to readjust in the transmission parameters.

Due to the fact that this message is unencrypted and unauthenticated, it makes the process vulnerable to a *Forgery attack*. An attacker may intercept the RNG-RSP message, modify it with false timing, power level or frequency information, and send this fake message to the SS. If the transmission power level is not high enough, the signal may not reach the BS. In addition, if the transmission power level is very high, it may consume excessive energy resources from the SS. If the SS sets a different frequency than the BS expects, both parts will never establish a communication with each other. Furthermore, if the uplink timing information is altered, the SS might cause collisions with the communication of other SSs, due to the fact that the SS under attack will transmit within the time slots reserved for these SS. In any case, the QoS will be degraded.

Under forgery attack, there would be:

- A difference between the number of sent RNG-REQ messages and the number of received RNG-RSP messages.
- A drop in the number of messages received by the SS, after have been received a RNG-RSP message.
- A high number of unanswered SBC-REQ messages by a SS, after having received a RNG-RSP message.
- A high number of RNG-REQ messages, with different CID, sent by an individual SS.
- Loss of synchronisation between BS and SS, if both are already synchronised to each other.
- An increased number of collisions in slots different from the ranging slots, which theoretically are collision free.
- An increase in the number of slots unutilised.

Reference [2] claims that the RNG-RSP message can be used to cause the SS to abandon the currently used downlink channel and try to synchronise with other downlink frequencies. In the same way as before, an attacker can intercept the RNG-RSP message, modify it and make the SS restart the process.

This would cause:

- Loss of synchronisation between BS and SS, if both are already synchronised to each other.
- An increase in the number of sent RNG-REQ messages, with different CID, following the reception of RNG-RSP messages.
- A high number of RNG-RSP messages with the ranging status field set to the value 2.

As presented in [11], an attacker can modify the security capabilities in the SBC-RSP message and modify the security capabilities used in the communication. For instance, selecting the weakest encryption method or establishing no security.

To accomplish all these types of forgery attacks, the attacker must transmit at the same time that the legitimate BS does. This has to be done with a higher transmission power level than the BS, in order to make the SS think that the signal from the BS is background noise.

2) Authentication Protocol on PKMv1

The effect of a *Jamming attack* would be similar in PKMv1 and PKMv2. SS sends an Auth-REQ message requesting for an AK. The BS generates and sends back, an Auth-REP message, to the SS. If an attacker causes a collision with the Auth-REP message, the SS will not receive the keying material within a given period. Hence, the authentication fails and the SS start from the network entry procedure. A jamming attack is also applicable to the reauthentication process.

Under a jamming attack, there would be:

- A high number of RNG-REQ messages, with different CID, sent by an individual SS.
- An increase in the number of Auth-REP messages immediately followed by a RNG-REQ message, with different CID, sent by the destination SS of the Auth-REP messages.
- A difference between the number of sent Auth-REQ messages and the number of received Auth-REP messages.
- A high number of unanswered Auth-REQ messages by a

SS.
- An increase in the number of AKs exchanged unaccomplished because of time expiration.

On the other hand, [3] explains that, after receiving an Auth-REQ message, the BS may define a time period within which it rejects any Auth-REQ messages containing the same Cert(SS). By replaying multiple times an Auth-REQ message, the attacker makes the BS consume resources rejecting these replayed messages. This would cause:

- A high number of Auth-INVALID messages to be sent to the same SS.
- A high number of Auth-INVALID messages received, without any Auth-REQ messages having been sent.
- A difference between the number of sent Auth-REQ messages and the number of received Auth-INVALID messages.
- A high number of Auth-REQ messages received by the BS, containing the same Cert(SS), in a short time period.

Slightly different than the attack explained above, if an attacker intercepts an Auth-REQ message and replays it to the BS, it will make the BS suffer a Replay attack. Once it receives the Auth-REQ message, the BS will perform a reauthentication of the SS, by generating and sending to SS new keying material.

Under replay attack, there would be:

- A large difference between the number of sent Auth-REQ messages and the number of Cert(SS.Manufacturer) received by a SS.
- A high number of Auth-REP messages received by the SS, without have been sent any Auth-REQ message.

As presented in [2], the BS may send the Auth-INVALID message, unauthenticated, without having received an Auth-REQ message. If an attacker makes use of this property, intercepts and replays an Auth-INVALID message, the SS restarts the full process from the network entry procedure.

This would cause:

- A high number of Auth-INVALID messages sent to the same SS.
- A high number of Auth-INVALID messages received, without have been sent any Auth-REQ message.
- A high number of RNG-REQ messages, with different CID, sent by an individual SS.
- A difference between the number of Auth-INVALID and Auth-REP messages sent by the same BS.
- A difference between the number of sent Auth-REQ messages and the number of received Auth-RSP messages.

Attackers can benefit from the lack of mutual authentication between the BS and SS, to perform a *Forgery attack*. After intercepting an Auth-REQ message, the attacker can create its own AK and send it back to the SS. Due to the fact the SS cannot differentiate between the attacker and the legitimate BS, if the SS accepts the fraudulent AK, the attacker will take control over the communication of the SS [8]. Under a forgery attack, there would be:

- An increase in the number of received Auth-REP messages, by a SS, immediately followed by a second Auth-REP message, containing different keying material.
- A difference between the number of sent Auth-REQ messages and the number of received Auth-REP messages.
- A high number of Key-Reject messages sent by a BS.
- A difference between the number of sent Key-Request messages and the number of received Key-Reply messages.

3) Key Management Protocol

After sending the key-request message, the SS expects to receive a response from the BS within the next 3 seconds to successfully accomplish the TEK exchange. Otherwise, the SS resends the Key-Request message until it gets response or reaches a given number of retransmissions. If an attacker performs a *Jamming attack* on the Key-Request message, the SS will not receive the keying material. Hence, the process fails and the SS has to restart the network entry procedure.

Under a jamming attack, there would be:

- An increase in the number of Key-Request messages sent by an individual SS.
- The number of times that a Key-Request message is sent by an individual SS would reach the maximum number of retransmissions.
- A high number of unanswered Key-Request messages by a SS.
- A difference between the number of sent Key-Request messages and the number of received Key-Response messages.

As show in [3], the key management protocol is vulnerable to a *Replay attack*. SS cannot detect if a Rekey message is legitimate or replayed by an attacker. Whether an attacker intercepts and resends a Rekey message to the SS, it will cause a restart of the key management protocol. Similarly, the BS cannot detect if an attacker has intercepted and replayed a Key-Request message from a legitimate SS. In that case, the BS will reply a Key-Request message with new keying material, the OldTEK and NewTEK.

Under a replay attack, there would be:

- An increase in the number of Rekey messages sent to an individual SS, without TEK lifetime has expired.
- An increase in the number of Key-Request messages sent from an individual SS, without TEK lifetime has expired.
- An increase in the number of Key-Request and Key-Reply messages exchanged.

Network Layer

Once the keying material is exchanged, a secure data transmission can occur, by encrypting the data. The Network layer, through the use of the Internet Protocol (IP), allows the sending of datagrams, taking routing, addressing or segmentation decisions, from a source to a destination. However, IP lacks a mechanism to report errors or to inform if a datagram has been discarded. Because of that, the Internet Control Message Protocol (ICMP) was added to the Network layer, to allow routers of a network to report errors or to inform about unexpected channel anomaly.

One type of ICMP message is the destination unreachable message. If a router cannot deliver a datagram, because of any channel anomaly, the router will inform the source that the datagram has been discarded. This is done through the use of an ICMP destination unreachable message. Other type of ICMP message is the source quench message. IP lacks a flow control mechanism, so the source of the packet never knows if the destination or an intermediate router suffers overflow. This type of ICMP message is sent to the source of the datagram when it has been discarded due to congestion.

The Network layer is directly affected by the *Jamming attack* which occurs over the PHY and MAC layers. If an attacker launches a jamming attack over the data transmission and the communication is completely disrupted, this will not allow the datagram to be delivered. Hence, as explained, destination unreachable ICMP messages will be sent by the network layer. On the other hand, if the attacker launches the attack and causes packet loss and long delay, it will be interpreted by the network layer as congestion. As happens with destination unreachable ICMP messages, source quench ICMP messages will be sent by the network layer.

Under jamming attacks, there would be:

- An increase in the number of destination unreachable ICMP messages sent.
- An increase in the number of source quench ICMP messages sent, with code field set to the value 0.
- An increase in the number of source quench ICMP messages sent, with code field set to the value 1.

If an attacker successfully impersonates a source of datagrams, it may perform a *Forgery attack*, and send datagrams using this fraudulent identity. From the point of view of the destination, a datagram sent either from the legitimate source or from the attacker seems to be sent from the same source. Assuming that, on average, the datagrams sent from and to the same source and destination tend to use similar routes, the value of Time To Live (TTL) field remains constant. This property may be utilized to detect forgery attack, if the legitimate source and the attacker are situated multiple hops apart by checking the TTL value.

Under a forgery attack, there would be:

- A difference between the values of the TTL of consecutive IP datagrams sent from the same source.

Transport Layer

Only Transmission Control Protocol (TCP) is considered here as the transport protocol. The Transport layer, through the use of TCP, provides ordered segment delivery, without duplications or data loss.

Because the segments sent by the transport layer are encapsulated into the data portion of datagrams, the Transport layer is directly affected by a *Jamming attack* as happens with the Network layer. According to TCP protocol behaviour, a source of segments will retransmit them until the source receives an ACK segment or until the maximum number of segment retransmissions is reached. If an attacker launches a jamming attack and disrupts the segment, the source of the segment will never receive the ACK segment. At this moment, the transport layer will send a Connection Reset (RST) segment in order to close the connection.

Under a jamming attack, there would be:

- A high number of segments sent, with the same sequence number, from the same source.
- A difference between the numbers of segments sent and the number of ACK segments received.
- An increase in the number of RST segments sent.
- An increase in the value of the backoff period for an individual source.
- An average increase in the Round Trip Time (RTT) value for the same couple source-destination.
- A difference between the number of received SYN segments and the number of received FIN segments.
- An increase in the number of SYN segment retransmissions from the same source.

V. CONCLUSION

Despite all efforts taken with security, WiMAX still presents vulnerabilities. More research focused on this area is needed. In this paper, we have conducted an analysis of the threats that a WiMAX network may face and highlighted the estimated misbehaviour metrics that may vary on the network performance, according to these attacks. Our main objective is to develop an intrusion tolerance system, focused on WiMAX. With this work we have established the first step in our objective, which is to identify the possible attacks and determine the appropriate threshold for detecting such attacks. Ongoing work focuses on the study of the metrics in a real scenario.

REFERENCES

[1] IEEE Standard for Local and metropolitan area networks, Air Interface for Broadband Wireless Access Systems, P802.16, 2009.

[2] Siddharth Maru and Timothy X Brown, "Denial of Service Vulnerabilities In the 802.16 Protocol", 2008. WICON.

[3] Sen Xu, Manton Matthews and Chin-Tser Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", 2006. ACM SE'06.

[4] David Johnston and Jesse Walker, "Overview of IEEE 802.16 Security", 2004. IEEE.

[5] Alefiya Hussain, John Heidemann and Christos Papadopoulos, "A Framework for Classifying Denial of Service Attacks", 2003. SIGCOMM'03.

[6] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar, "A Cross-layer Approach to Detect Jamming Attacks in Wireless Ad hoc Networks", 2006. MILCOM.

[7] Juan Li and Sven-Gustav Häggman, "Performance of IEEE802.16-2004 based system in jamming environment and its improvement with link adaptation", 2006. PIMRC'06.

[8] Evren Eren, "WiMAX Security Architecture – Analysis and Assessment", 2007. IEEE.

[9] Lang Wei-min, Wu Run-sheng and Wang jian-qiu, "A Simple Key Management Scheme based on WiMAX", 2008. IEEE.

[10] Karen Scarfone, Cyrus Tibbs and Matthew Sexton, "Guide to Security for WiMAX Technologies (Draft)", 2009. NIST Special Publication 800-127.

[11] Tao Han, Ning Shang, Kaiming Liu, Bihua Tang and Yuan'an Liu, "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", 2008.