Securing Bandwidth Request Messages in Wimax

Kaushik Adhikary[#1], Rajinder Kumar[#2] , Amit Kumar[#3]
[#1, #3] Deptt. of CSE, MMU, Mullana, India
[#2] Cyber Security Research Centre, PEC, Chandigarh, India

ABSTRACT
Privacy, confidentiality and authentication are the issues which are been focused by the security sublayer which is defined in the IEEE 802.16 standard. WiMAX which is the Wireless Interoperability for Microwave Access is the latest technology for Wireless Communication. It has been developed to replace DSL/fibre cable. It has been developed to provide 'last mile' broadband connectivity to home or business location. The IEEE 802.16 has many flaws in its security which has led to various vulnerabilities. One of the vulnerability which has been detected by us is the bandwidth request messages. This paper analyses the attacks which can be carried on the bandwidth request messages, its effect on the performance and the suitable solution to counter this attack.

Keywords
WiMAX, PKM, Bandwidth Request Message, denial-of service attack

1. INTRODUCTION
WiMAX is the latest wireless technology that has been developed. It was formed by the WiMAX forum in June 2001. It has been developed to deliver broadband access service and backhaul services to residential and enterprise customer at economical rates. It is similar to Wi-Fi [1] but has higher speed, has greater range and can cater a large number of users. As Wi-Fi refers to the interoperable implementation of IEEE 802.11 Wireless LAN standard similar to this WiMAX [2] refers to the interoperable implementation of the IEEE 802.16 standard. Wireless technology because of its open medium and unstoppable range is vulnerable to various attacks. Earlier technologies of Wireless have been found to have much vulnerability. For instance, unauthorized users, man-in-the-middle attacks, and key analysis are found in Bluetooth. User authentication, auditing, and nonrepudiation are the security services which it lacks. Due to the weakness of its WEP (Wired Equivalent Privacy) protocol Wi-Fi faces many security problems. They are easily attacked by brute force attacks, dictionary attacks, and algorithmic attacks since WEP keys are static, rather short, and shared among devices. And the result of Leak of WEP keys leads to eavesdropping, message modification, and masquerading. Repetition in key stream generation is caused by short initialization vectors (IVs). Attackers easily analyze this. The weakness of authentication process causes replay attacks and man-in-the-middle attacks. Due to the open medium traffic analysis, access point is easily compromised. Session hijacking is also possible during handover process. Denial-of-service attack is also a big risk. IEEE Standard 802.11 mitigates some of the problems, but the standard faces compatibility problem with existing Wi-Fi devices. Very few studies have been carried out on the security aspects of the IEEE 802.16 standard as it is a new standard. IEEE 802.16 uses Privacy and Key Management Protocol that provides privacy and authentication. In WiMAX above the Physical layer lays the Security Layer. The Key Refreshment mechanism is provided in the Privacy and Key Management Protocol [3]. Current researches have shown that IEEE 802.16 is still prone to attacks.

2. PROBLEM IDENTIFICATION
2.1 Spoofing of bandwidth request messages
Using Bandwidth Request messages, an SS may ask and obtain channel resources; requests can be aggregate (containing an absolute value) or differential (containing the difference from current assignment). Aggregate requests are sent in the unscheduled time period where each SS can transmit using a contention technique. As bandwidth Requests are included into unauthenticated frames, they might be forged by an attacker. Pretending to be some other station and requesting very limited channel resources, the attacker can send false aggregate requests and as a result, the BS will update the schedule and communicate it with the following UL-MAP and DL-MAP.

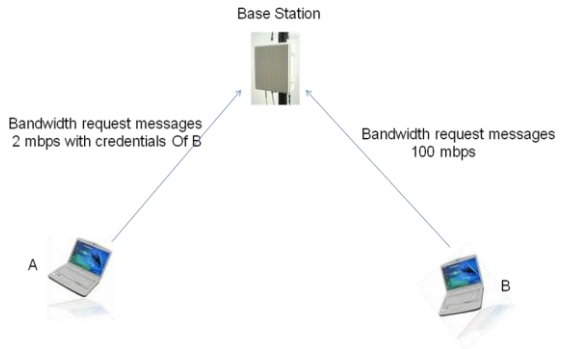

Fig 1: Spoofing of Bandwidth Request messages

The possibility of having a centralized resource allocation to distinguish several service classes, according to the credentials of the user is one of the most interesting features that distinguish *IEEE 802.16* from *IEEE 802.11* as said [4]. An authorized SS of the network can reduce the resources allocated to its neighbors with this attack with the aim of having more resources disposable to itself [as shown in fig 1]. The victim stations will not have the chance to issue some new valid requests, if the attack is repeated at every time interval.

2.2 Miscellaneous attacks

During the analysis of the protocol, other possible attacks have emerged which we briefly cite them in this subsection:

- On the initial TEK authentication, a downgrade attack is possible. Before negotiating the encryption keys, the security capabilities are sent by SS to BS over an insecure connection and these include the kind of crypto functions to be used to cipher the data packets. In order to convince the BS and the attacked SS to agree on an insecure crypto algorithm, an attacker could send a spoofed message containing weaker capabilities, since there is no authentication. It is unclear how this race condition may be solved since the standard doesn't specify a correct behavior for the BS upon reception of two valid answers for the same request.
- With the new PKMv2 RSA authentication, SS can authenticate with BS in *IEEE 802.16e* [5]. The BS has to sign the reply messages with its public key in this new authentication type. If flooded with false requests, the BS may be victim of a denial of service attack using all its resources to evaluate digital signatures since public key encryption and signature is a computationally heavy operation.
- A power save mode is introduced to support mobile limited resource devices in *IEEE 802.16e* [6]. A SS will communicate to the BS that it will buffer messages for the SS after entering into sleep mode. In the Bandwidth request, the SS can set the sleep mode and uplink sleep control messages that are not authenticated. With the identifier of victim SS, the attacker can send the Bandwidth request and uplink sleep control message and the BS will stop transmitting messages to that SS, so performing a denial of service attack.
- To produce denial of service attacks [7], more management frames are sent in clear, unauthenticated, that could be used by an attacker. For instance, to desynchronize clocks or to force the SS to repeat network entry or authentication, CMP-CLK messages, Auth Invalid messages or RNG-RSP messages can be used [8].

In the Figure 2 client request 20 Mbps to the server and is granted.

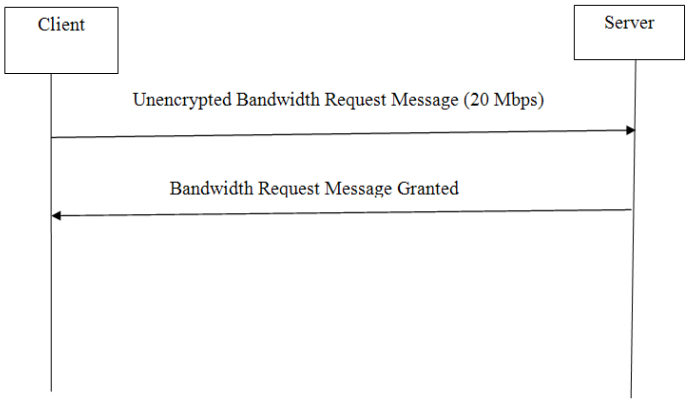

Fig 2: Client-Server unauthenticated bandwidth request message

In the Fig 3, attacker using the credentials of the client, the attacker request 2 Mbps to the server and is granted since the bandwidth request message is not authenticated. This results in denial of service for the client.

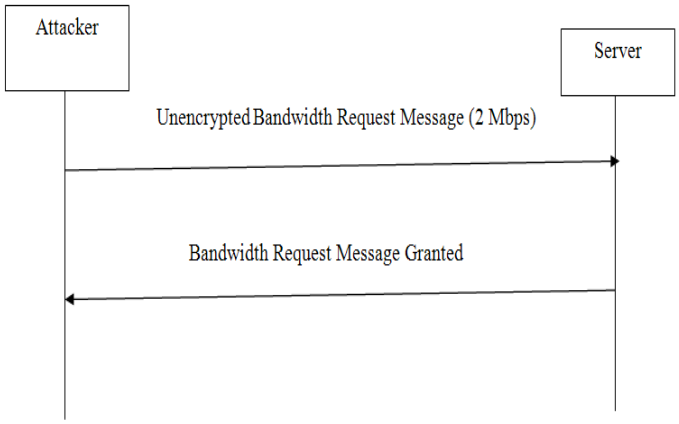

Fig 3: Attacker-Server unauthenticated bandwidth request message

3. PROBLEM SOLUTION

In Fig 4 using the authentication mechanism, the client encrypts bandwidth request messages with its private key and sends it to the server. The server decrypts the message with client public key and is authenticated. Server grants 20Mbps to the client.

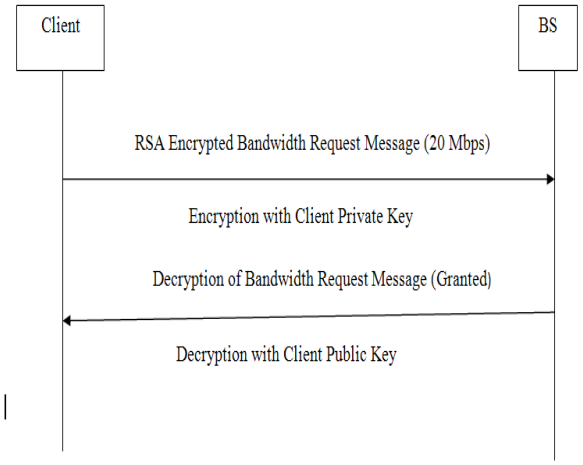

Fig 4: Client-Server authenticated bandwidth request message

In Fig 5 using the authentication mechanism, the attacker encrypts bandwidth request messages with its private key and sends it to the server. The server decrypts the message with client public key and is unauthenticated. Server denies 2 Mbps.

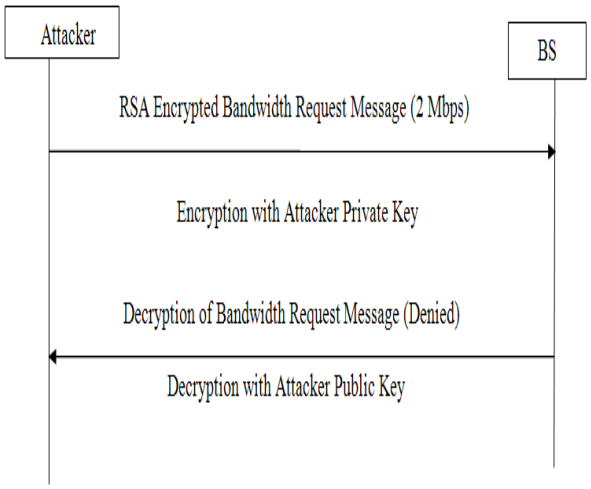

Fig 5: Attacker-Server authenticated bandwidth request message

4. RESULTS

In Figure 6, for both the cases i.e. with authentication and without Authentication, we considered the actual value of bandwidth as 20, 40, 60, 80, 100 bits /sec.

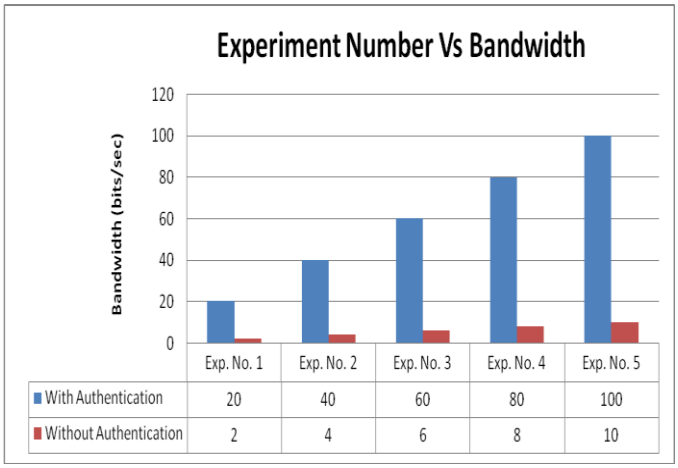

Fig 6: Experiment Number Vs Bandwidth

In below graphs we have shown the performance of client in both the cases i.e. with authentication and without Authentication.

Data Delivery Ratio can be calculated as the ratio between the number of data that are sent by the source and the number of data that are received by the sink.

In the Fig 7, it is shown that with authentication the data delivery ratio is high compared to without authentication.

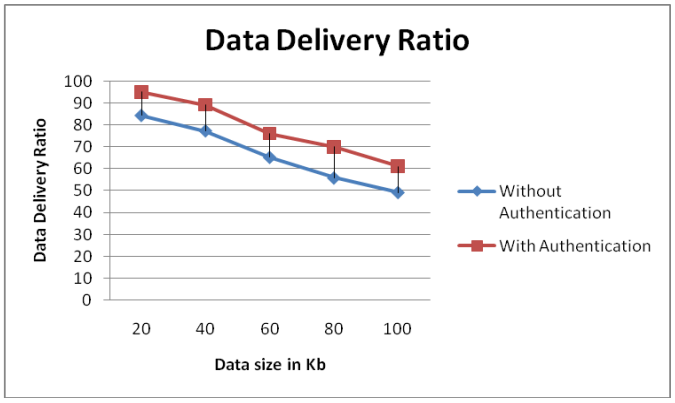

Fig 7: Data Delivery ratio comparisons between with and without authentication

Time delay is the time taken for a data to reach its destination.In Fig 8, it is shown that time dalay in case of with authentication is low as compared to without athentication.

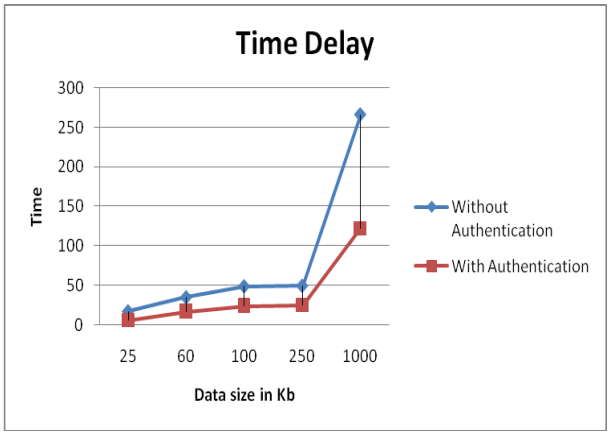

Fig 8: Time Delay comparison between with and without authentication

Throughput is the average number of successful data that can be sent in a given time. In Figure 8, it is shown that throughput in case of with authentication is high compared to without authentication.

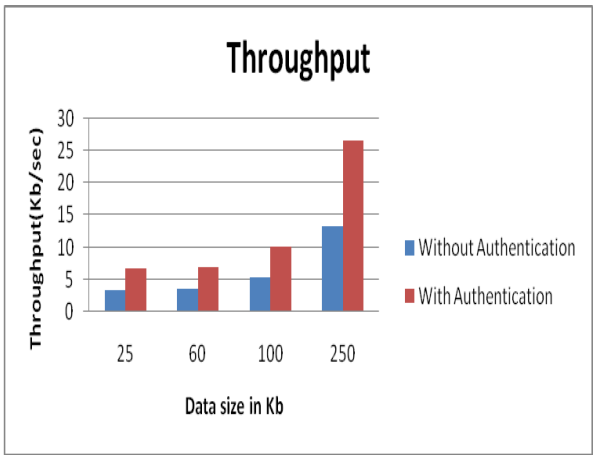

Fig 9: Throughput comparisons between with and without authentication

Cost estimation is the cost incurred while sending a data. In Figure 9, the cost for sending data is less in with authentication compared to without authentication.

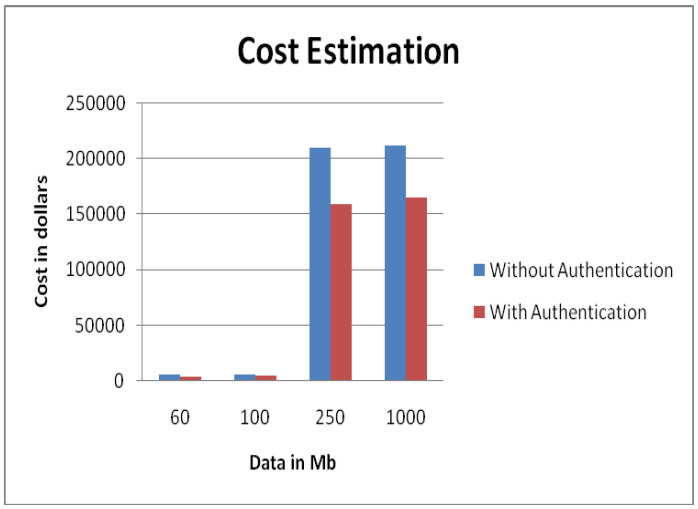

Fig 10: Cost estimation comparisons between with and without authentication

5. CONCLUSION AND FUTURE WORK

Features like strong authentication, key refreshment, and strong encryption algorithms are provided in Privacy and Key Management Protocol of IEEE802.16.IEEE 802.16 standard uses strong encryption algorithm such as Advance Encryption Standard (AES) and Data Encryption Standard (3DES).In IEEE802.16 standard Subscriber Stations are also require to authenticate a Base Station. The most of IEEE 802.16 standard are under development. The proposed mobility and coverage area in IEEE 802.16e standard will generate more problems in its security protocol. Therefore, we need to pay more attention to the security issues of those standards, which are under amendment and still not be approved as standard.Secure roaming in PKMv2 is also requires more attentions. Multicasting is another issue in the new standard, which requires revision in security protocol of IEEE 802.16 to facilitate the multicast functions.

6. LIMITATION

The security mechanisms defined in the IEEE Std 802.16 were focused by us. We considered only when the standard operates in PMP mode in our analysis. Our study is limited to the current information because the standard is new and some amendments have not been deployed yet.

7. REFERENCES

[1] Hunglin Zhou, Wi-Fi Task Group Current Status, http://lee-1.com/hlchou/ 1 WiFi_ TaskGroup_ Meeting_ok.ppt

[2] WiMAX FAQs,http://www.unwiremycity.com/archives /2005/09/wimax _faqs 1I.html

[3] IEEE 802.11, Wireless Local Area Networks (WAN's), The student reports, The Hebrew University of Jerusalem

[4] The Extensible Authentication Protocol, From Wikipedia, the free encyclopedia
[5] WiMAX Technology,www.hifn.com/docs/WiMAX _AB_1.4.pdf
[6] JunHyuk Song, Yong Chang, Privacy Sublayer Clean Up, http://www.ieee802.org/ 16/tge/contrib/C80216e-04 521rl.pdf
[7] Fabian Andre Perez, Security in Current Commercial Wireless Networks: A Survey, http://www.csociety.org/perez/WirelessSurvey.pdf
[8] G. Schafer, A. Festag, H. Karl, Current Approa-ches to Authentication in Wireless and Mobile Communications Networks, http://www.tkn.tu-berlin.de/ publications/papers/ tkno 1_002.pdf