ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

A Countermeasure for Black Hole Attack in Mobile WiMAX Networks

M. Deva Priya, Dr. M.L.Valarmathi, S. Aishwarya, K. Jaya Bharathi

***Abstract* - Mobile WiMAX has drawn much attention due to its benefits. Nevertheless, security is a challenge and has to be ensured. The attacker may make use of parts of unencrypted management messages and acquire information about the type of traffic, nodes involved, timing and so on. This work discusses about the attacks prevalent in mobile WiMAX and a prediction mechanism to foreknow the prevalence of Black hole attack, an attack in the network layer. This mechanism eliminates the vindictive nodes and provides better results in terms of Packet Delivery Ratio (PDR), Throughput, Control and Total overheads.**

Index Terms - Black hole attack, Confidence Level (CL), WiMAX.

I. INTRODUCTION

The WiMAX (Worldwide Interoperability for Microwave Access) is a broadband wireless access system which is based on IEEE 802.16 wireless MAN air interface standard, developed and promoted by the WiMAX Forum [1].

The role of the WiMAX Forum is to define profiles using the broad range of 802.16 available options to address certification of implementations and to define additional mechanisms for networking such as user-network mutual authentication, integration with other kinds of wireless access technologies (WiFi/802.11, 2G/3G/4G cellular) and transfer of security and quality of service state information during handovers.

Manuscript received March, 2013

***Deva Priya. M**, Assistant Professor, Department of CSE, Sri Krishna College of Technology, Coimbatore, Tami Nadu, India.*
***Dr. Valarmathi M. L.**, Associate Professor, Department of CSE, Government College of Technology, Coimbatore, Tami Nadu, India.*
***Aishwarya. S,** PG Scholar, Department of CSE, Sri Krishna College of Technology, Coimbatore, Tami Nadu, India.*
***Jaya Bharathi. K,** PG Scholar, Department of CSE, Sri Krishna College of Technology, Coimbatore, Tami Nadu, India.*

WiMAX offers high throughput, great coverage, flexible Quality of Service (QoS) support and extensive security. In an ideal condition, WiMAX offers a bit rate of upto 75 Mbps [2], within the range of 50 km and for mobile stations with a maximum data rate of upto 70 Mbps compared to 802.11a with 54 Mbps upto several hundred meters, EDGE (Enhanced Data Rates for Global Evolution) with 384 kbps to a few kms, or CDMA2000 (Code-Division Multiple Access 2000) with 2 Mbps for a few kms.

WiMAX is a Fixed Wireless Access (FWA) network suitable for broadband services on areas without adequate cable infrastructure. This system is based on the Orthogonal Frequency Division Multiplexing (OFDM) and realizes broadband data transmission by using a radio-frequency range of 2-11 GHz and 10-66 GHz. An important feature of an OFDM system is the possibility of successful communication even under non-line-of-sight (NLOS) propagation condition. WiMAX uses adaptive modulation which is dependent on the Signal-to-Noise ratio (SNR).

Originally line-of-sight transmission was supported in the 10 G Hz to 66 G Hz range. Two amendments were published. The first amendment, the IEEE 802.16c standard defines profiles of typical implementations. The second amendment, the IEEE 802.16a standard [3] consists of control enhancements, introduction of mesh mode and support of additional frequencies. Together they added transmission in the 2 G Hz to 11 G Hz range, non-line-of-sight, and licensed or unlicensed service.

A major update was published in 2004 as the IEEE 802.16d standard. It is a consolidation and an improvement of the IEEE 802.16 standard and the amendments 802.16c and 802.16a. An amendment to IEEE 802.16d has been drafted as the IEEE 802.16e. It defines additional mechanisms to support mobile subscribers at vehicular speed and data authentication.

IEEE 802.16 Working Group has embarked on the development of a new amendment of the IEEE 802.16 standard (i.e., IEEE 802.16m) as an advanced air interface to meet the requirements of the International Telecommunication Union – Radio communication / International Mobile Telecommunications (ITUR/IMT) - advanced for fourth-generation (4G) systems as well as the next-generation mobile network operators. The IEEE 802.16m is suitable for both green-field and mixed deployments with legacy mobile stations (MSs) and Base Stations (BSs).The backward compatibility feature allows smooth upgrades and an evolution path for the existing deployments. It enables roaming and seamless connectivity across IMT-advanced and IMT-2000 systems through the use of appropriate interworking functions. In addition, the IEEE 802.16m system utilizes multihop relay architectures for improved coverage and performance.

A. Modes of operation

The IEEE 802.16 standard supports PMP (Point-To-Multipoint) and Mesh-mode topologies. The IEEE 802.16 standard published in 2002 defined the air interface for fixed PMP broadband wireless access networks. PMP mode comprises of a BS (Base station) that communicates with different SSs (Subscriber Stations). Each BS broadcasts to a group of SSs. In Mesh mode, SSs directly establish a link between each other, where one of the communicating SS acts as a host.

B. Features of WiMAX

WiMAX is a wireless broadband solution that offers a rich set of features with a lot of flexibility in terms of deployment and services. Some of the salient features that deserve emphasizing are:

- Types of Service - WiMAX can provide two forms of wireless service. i.e, Non-line-of-sight and Line-of-sight.
- OFDM-based physical layer.
- Very high peak data rates - The peak PHY data rate can be as high as 74Mbps when operating using a 20MHz wide spectrum. Using a 10MHz spectrum operating using TDD scheme with a 3:1 downlink-to-uplink ratio, the peak PHY data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively.
- Scalable bandwidth and data rate support - A WiMAX system may use 128, 512, or 1,048-bit FFTs based on whether the channel bandwidth is 1.25MHz, 5MHz, or 10MHz, respectively.
- Adaptive Modulation and Coding (AMC)
- Link-layer retransmissions - Automatic Retransmission Requests (ARQ) at the link layer for connections that require enhanced reliability.
- Support for TDD and FDD.
- Flexible and dynamic per user resource allocation.
- Support for advanced antenna techniques - beam forming, space-time coding, and spatial multiplexing.
- Quality-of-service support - support a variety of applications, including voice and multimedia services and offers support for Constant Bit Rate, Variable Bit Rate, Real-Time and Non-Real-Time traffic flows, in addition to best-effort data traffic to a large number of users, with multiple connections per terminal, each with its own QoS requirement.
- Robust security - Incorporates Advanced Encryption Standard (AES) and a robust privacy and key-management protocol are available. Includes Extensible Authentication Protocol (EAP), Cipher-based Message Authentication Code (CMAC) and Hashed Message Authentication Code (HMAC) based control message protection schemes.
- Support for mobility.
- IP - based architecture.
- Access - Supports the service in the remote rural areas.
- Versatility - support different services like Voice over IP and especially Triple play.
- Connectivity - Connections in different medium available in the market called subscriber units like, cell phone, Net books, iPods, etc and is accessible in a multiple ways by using Wi-Fi access point, Ethernet ports also support WiMAX connectivity, while telephone jacks are a convenient way to access this WiMAX service.

C. IEEE 802.16 e – Mobile WiMAX

There are two main classes of WiMAX systems called fixed WiMAX and mobile WiMAX.

Fixed WiMAX is targeted for providing fixed and nomadic services, while mobile WiMAX provides portable and (simple and full) mobile connectivity. Mobile WiMAX offers a wireless solution to link fixed and mobile broadband networks through a broadband radio access technology and an advanced architecture defined by the standard [5][6].

In the IEEE 802.16e standard, three basic types of handovers are specified for portability and simple/full mobility of users: Hard Handover (HHO), Macro Diversity Handover (MDHO), and Fast Base Station Switching (FBSS). HHO is mandatory in WiMAX systems.

Other two types of handover are optional. IEEE 802.16e uses Extensible Authentication Protocol (EAP) as an authentication procedure and key management for link layer security as well as an RSA-based authentication procedure. Due to the flexibility and ability to interact with Authentication, Authorizing and Accounting (AAA) infrastructures, it is very likely that EAP will become the de facto authentication method for 802.16e access control [4].

In fact, all OFDM-based, mobile broadband access technologies that have been developed exploit, enhance, and expand fundamental concepts that were originally utilized in mobile WiMAX.

D. IEEE 802.16 j – Multi-hop relay based WiMAX

The new task group IEEE 802.16j-2009 standard [1] of IEEE 802.16 air interface for broadband wireless access was officially established in March 2006. In order to support the mobile multi-hop relay specification, mesh mode is removed from the IEEE 802.16 -2009 standard. The mobile stations communicate with a base station through an intermediate relay station. Multi-hop relay station is an optional deployment that may be used to provide additional coverage. The Relay Station may be fixed or may be mobile. The relay station may act as a Base Station and has its own physical cell identifier.

E. WiMAX MAC Layer

MAC layer of WiMAX consists of 3 sub-layers: Convergence Sublayer, Common part Sublayer and Privacy Sublayer. The Convergence Sublayer was introduced to support better interface with existing protocols of upper layers such as IP, ETHERNET, ATM and potential future technologies. Currently it can operate with the IP and ETHERNET protocols.

F. Security Services

The ultimate goals of the security solutions for WiMAX is to provide security services, such as authentication, confidentiality, integrity, authentication, nonrepudiation, anonymity and availability to mobile WiMAX users. There is no single mechanism that will provide all the security services in WIMAXs. The common security services are described below.

- *Availability* - Availability is concerned with the (unauthorized) upholding of resources. Availability ensures the survivability of network services despite various attacks.

- *Confidentiality* - Confidentiality ensures that certain information is only readable or accessible by the authorized party. Transmission of sensitive information such as military information requires confidentiality.

- *Integrity* - Integrity guarantees that the authorized parties are only allowed to modify the information or messages. It also ensures that a message being transmitted is never corrupted.

- *Authentication* - Authentication ensures that the access and supply of data is done only by the authorized parties. It is concerned with assuring that a communication is authentic.

- *Non repudiation* - Non repudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver.

- *Scalability* - Scalability is not directly related to security but it is a very important issue that has a great impact on security services. Security mechanisms should be scalable to handle the network.

II. ATTACKS IN WiMAX

This section lists some of the attacks seen in mobile WiMAX due to the lack of encryption of management messages.

A. Bandwidth spoofing

In bandwidth spoofing, the attacker grabs the available bandwidth, by sending unnecessary BW request messages to BS [7]. To solve this problem, the radio resource management in the BS should check the Local Policy Function (LPF) and then allocate bandwidth only if the MS is necessarily

provisioned. This new recommendation is based on QoS model suggested by the WiMAX forum [5].

An SS obtains channel resources using Bandwidth Request messages. Bandwidth requests are included into unauthenticated frames and hence can be forged by an attacker. The attacker can send false aggregate requests pretending to be some other station and requesting very limited channel resources and the BS will update the schedule and communicate it with through UL-MAP and DL-MAP [8],[9].

B. Unencrypted management messages

IEEE 802.16-2004 does not provide any data authenticity for management messages [10],[11]. The complete management communication between MS and BS is unencrypted. If an adversary listens to the traffic, he can collect information about both instances. Mobile WiMAX includes some unauthenticated messages [12]. Their forgery can interrupt communication. Adversary can also listen to important network information from these unencrypted frames. Some important management frames lack the authentication of their origin.

IEEE 802.16e-2005 and IEEE 802.16-2009 provide integrity protection for certain unicast management messages by appending a unique digest to protect against malicious replay or modification attacks. This digest is not added to IEEE 802.16 multicast and initial network entry management messages.

For symmetric traffic encryption, the multicast and broadcast service in IEEE 802.16e shares keying material with all group members. The group members can forge messages or even distribute their own traffic keying material, thus controlling the multicast and broadcast contents [10],[12]. In addition, [10] discuss about various messages that are not encrypted, leading to attacks.

As with all wireless systems, digest integrity protection cannot be applied to management messages sent to multiple recipients (i.e., multicast transmissions), and initial network entry management messages cannot leverage integrity protection because nodes must first be authenticated to create the unique digest. Management messages are susceptible to eavesdropping attacks as they are sent in the clear to facilitate network operations. Furthermore, information sent between a BS and SS before security associations have been negotiated, is insecure and unauthenticated. An attacker may misuse RNG-REQ message, changing some fields randomly and send it to BS in large number to waste the resources of the network [13].

During handover, when a MS performs initial network entry [14], it negotiates communication parameters and settings with the BS, a lot of information is exchanged like security negotiation parameters, configuration settings, mobility parameters, power settings, vendor information, MS's capabilities, etc. Since the management messages are unencrypted, an attacker can access them by listening to the channel. IEEE 802.16m supports full encryption and authentication for management messages, but it has not been integrated into many vendor solutions. Critical threats are eavesdropping of management messages, BS or MS masquerading, management message modification and DoS attack.

The spoofed message may contain false message about the security capabilities of the legitimate SS. For instance, the attacker may degrade a MS, by informing the BS that the SS supports low security capabilities or has no security capabilities. In this situation, if the BS supports this kind of SS, the communication between the SS with the serving BS will not be encrypted. As a result, the attackers can wiretap and tamper all the information transmitted.

Eavesdropping of management messages is a critical threat for users and a major threat to a system. For example, an attacker could use this vulnerability to verify the presence of a victim at its location before committing an offence. Additionally, it might be used by a competitor to map the network. The masquerading threat of the BS or SSs is enabled when authentication weaknesses are present.

C. Encryption in WiMAX

Most of the management messages defined in IEEE 802.16e are integrity protected. This is done by a Hash based Message Authentication Code (HMAC) or alternatively by a Cipher based Message Authentication Code (CMAC). However, some messages are not authenticated. This introduces some vulnerability. A couple of management messages are sent over broadcast management connection. In WiMAX security architecture, since there is no

common key which can be used as the authentication of broadcasted management messages, the authentication of these messages is difficult. Furthermore, a common key would not completely protect the integrity of the message as MSs sharing the key can be generated by unauthenticated BS.

WiMAX MAC layer encrypts only data messages not management messages. It checks the SA associated with the current connection and acquires the initialization vector (IV). The MPDU plaintext payload is encrypted by employing the generated MPDU IV and the authenticated TEKs. To indicate that the payload in the MPDU is encrypted, it sets Encryption Control (EC) field of the MAC header to 1.Here, 2 bit encryption key sequence is used to indicate which TEK is used. Finally it updates the CRC field in accordance with changes in both the payload and MAC header [17].

A lot of security concerns should be provided, so future work is needed in this area to secure the communication and countermeasure the security threats/attacks [16].

D. Message Flooding

The attacker floods either the BS or SS with messages such that the overall performance of the network falls. An attacker constantly sends messages in order to keep the destination of the messages busy processing or rejecting them [18]. A distributed flooding DoS attack is a huge challenge for all the wireless broadband networks, as this attack can bring down an entire network or consume the network bandwidth to a great extent.

E. Rogue Base Station

A rogue BS confuses the MSs of the network by acting like a legitimate BS. Mesh routers or APs are compromised by the attackers using sniffers. In IEEE 802.16, the BS is compromised by reprogramming a device with the hardware address of another legitimate device. The hardware address can be obtained by intercepting the management messages of IEEE 802.1 using sniffers. WMN and IEEE 802.11 nodes use Probe request frames to discover a wireless network and the AP respond with Probe response frame. The clients select the AP that provides the strongest signal to it. Identity theft and Rogues BS are specific techniques of masquerading.

The attacker can spoof a flood of probe request frames, thus increasing the number of nodes searching for wireless network and overload the AP or wireless mesh router. The attacker can spoof the de-authentication message on behalf of the target node to stop it from using the network resources. The same vulnerability exists in IEEE 802.16, where the adversary eavesdrop the authentication message between the node and the BS, and then replays this message many times to the BS, creating DoS for the target node [19],[20].

F. DOS (Denial of Service)

If a SS sends a lot of false authorization requests to a BS, the BS will use all its resources to calculate whether the certificate is right [22]. WiMAX uses mutual authentication to protect from forgery attacks, but the authorization process is still vulnerable because there is no way to ensure integrity of messages [21].Anyone with a properly placed radio receiver can catch an authorization message, modify and retransmit it. DoS attacks take place as authentication operations trigger the execution of long procedures. A MS can be flooded with a high number of messages to authenticate. Due to low computational resources, the MS will not be able to handle a large amount of invalid messages, rendering the DoS attack successful [15].

G. Man-in-the-middle vulnerabilities

The attacker intercepts messages during communication establishment or a public key exchange and then retransmits them, tampering the information contained in the messages, so that the two original parties still appear to be communicating with each other. In a man-in-the-middle attacks, the intruder uses a program that appears to be the (Access Point) AP to SS and appears to be the SS to AP [23].

The attacker intrudes into the communication between the endpoints on a network to inject false information and intercept the data transferred between them [24]. A man-in-the-middle attack is successful, when the attacker impersonates each endpoint to the satisfaction of the other.

Although WiMAX can prevent MITM attack through rogue BS by using PKMv2, it is still vulnerable to MITM attack. This possibility is due to the vulnerabilities in initial network entry procedure.

It is known that WiMAX standard does not provide any security mechanism for the SSBC negotiation parameters.

H. Replay attack

In the mesh mode, 802.16 is also vulnerable to a replay attack in which an attacker maliciously resends valid frames that the attacker has intercepted in the middle of forwarding (relaying) process [25].

I. Water Torture attack

In wireless world some threats are generic; IEEE 802.16 is not an exception. A classic threat arises from the water torture attack, in which an attacker sends a series of frames to drain the receiver's battery. In addition, attacker with a properly positioned RF receiver can intercept messages sent through wireless, and thus a confidentiality mechanism in the design is required [26].

J. Scrambling attack

Scrambling is a sort of jamming, but for short intervals of time and targeted to specific frames or parts of frames. Scramblers can selectively scramble control or management information with the aim of affecting the normal operation of the network. The problem is of greater amplitude for time sensitive messages, which are not delay tolerant, such as the channel measurement report requests or responses [27]. Present security mechanisms do not address well in IEEE 802.16a Mesh modes network, which leads to new security threats, such as the trustworthiness of the next hop mesh node. Introducing mobility in IEEE 802.16e standard makes the attacker's life comfortable. As the physical location of the attacker is not an issue, management messages are more vulnerable than in IEEE 802.11. Therefore, it is necessary to maintain a secure connectivity while a mobile SS shifts between BSs.

III. NETWORK LAYER VULNERABILITIES

The network layer DoS attacks in WMN can be

- *Black hole attack* - The attacker creates forged packets to impersonate a valid mesh node and subsequently drops packets. The attracting packets involve advertising low-cost or quickest routes [30].
- *Grey hole attack* - The malicious node selectively forwards the packets to the destination node [33].
- *Wormhole attack* - The attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network [28].
- *Flooding attack* - The attacker transmits a flood of packets toward a target node in order to congest the network and degrade its performance [29],[31].

In the sections that follow, Black hole attack is discussed in detail with a solution to overcome it. A scenario in which a Routing REQuest (RREQ) is broadcast and Routing REsPonses (RREPs) are collected is simulated using ns-2. The malicious nodes are found and eliminated in the initial phase, thus enforcing a secured path from the source to the destination.

A. Black hole attacks

In Black hole attack, a malicious node sends fake routing information using its routing protocol, and advertises itself as having the shortest path to the destination, even though the route is spurious, with the intention of intercepting packets. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way the attacker will always reply to the RREQ, intercept data packets and retain them. The malicious node absorbs all the traffic going toward the target node [32]. Everything is made possible as the management information is unencrypted.

When the route is established, the malicious node either drops the packets or forwards them to unknown address. A Black hole attack is a kind of denial-of-service attack, where a malicious node attracts all packets by falsely claiming an optimum route to the destination and absorbing them without forwarding them to the destination. However, the attacker runs the risk that neighbouring nodes will monitor and expose the on-going attacks. There is a more subtle form of these attacks, when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing.

Once the attack has been injected, its impact in the network communication and the running applications must be evaluated. This impact may, for instance, may lead to the failure of a particular application, degrade network communications, isolate nodes or create routing loops. This work concentrates on route discovery information alone (Fig. 1).

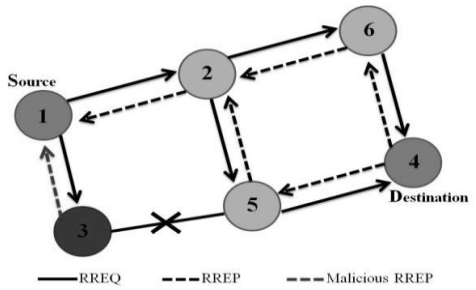

Fig. 1: Black hole attack

In Fig. 1, Node 1 is the source node and node 4 is the destination node. Node 3 is a malicious node which replies makes a false response stating that it has the shortest route to the destination node. Therefore Node 1 erroneously starts sending data packets to Node 3. A malicious node probably drops or consumes the packets. This suspicious node can be regarded as a Black hole. As a result, Node 3 misroutes the packets easily and the network operation is hindered.

B. Confidence Level (CL) based Solution for Black hole attacks

The source node broadcasts the RREQ and then waits for 't' seconds. If a node is a Black hole, it will not forward the packet to other nodes. Instead it will drop/ modify the packet. A normal node, on the other hand will forward the packet and receive an acknowledgement. In other words, the CONFIDENCE_LEVEL of a node is increased if the node is involved in forwarding the data. The algorithm is given in Fig. 2.

The number of acknowledgements received by a node in a particular time interval is the CONFIDENCE_LEVEL of that node. It should be kept in store, so as to identify the malicious node. In case of a vindictive node, the number of acknowledgements received will be zero.

If more than one route has the same TOTAL_CONFIDENCE_LEVEL, then the path with the highest AVERAGE_CONFIDENCE_LEVEL is chosen for the next transmission. The basic idea is to select the next hop node with the highest CONFIDENCE_LEVEL.

For a node,

$$\text{CONFIDENCE\_LEVEL} = \sum_{i=1}^{n} \text{ACKNOWLEDGEMENT} \quad (1)$$

i.e the number of acknowledgements received in the time period $1 \leq i \leq t$.

For a path with 'n' nodes,

$$\text{TOTAL\_CONFIDENCE\_LEVEL} \sum_{i=1}^{n} \text{CONFIDENCE\_LEVEL} \quad (2)$$

of 'n' nodes along the path.

In case, two or more paths have the same CONFIDENCE_LEVELs, then the one with the minimum HOP_ COUNT is chosen.

$$\text{AVERAGE\_CONFIDENCE\_LEVEL} = \frac{\text{TOTAL\_CONFIDENCE\_LEVEL}}{\text{HOP\_COUNT}} \quad (3)$$

Equation (3) gives the AVERAGE_CONFIDENCE_LEVEL of a path. The value varies with the HOP_COUNT. The path which involves less number of hops may contribute a higher average value and involve less time.

In case the CONFIDENCE_LEVEL of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and it is eliminated and all the nodes are intimated.

Initially, the source takes the initiative of finding the number of hops to each node. This is maintained in the routing table and is updated dynamically after each transmission.

One important factor that has to be considered here is that, a malicious node will send RREP immediately before any other legitimate node. In such a case, the time taken for response will be very less. The source may rely on this node and forward packets through this node. This can be overcome by setting a THRESHOLD_TIME, before which no responses will be accepted.

$$\text{THRESHOLD\_TIME} = \Delta t \quad (4)$$

'Δt' is based on the minimum number of hops required to reach the destination from the source.

```
initialize( )        // Initialization
begin
for each intermediate node 'i'
  Set CONFIDENCE_LEVEL [i] = 0
  Set HOP_COUNT [i] = 0
end for
end

begin     // Algorithm Black_hole( )
initialize ( )
Source sends RREQ to all the neighbors and waits for RREP.
Find the minimum HOP_COUNT mandatory to reach the destination from the former transmission. Find 'Δt'.
for each intermediate node 'i' for time 't'
    if ('i' sends a RREP before 'Δt')
        Drop node 'i' and declare it to be malicious.
    end if
    Find the HOP_COUNT[i] for each path.
    if 'i' receives an acknowledgement along a path
       Update the CONFIDENCE_LEVEL [i]
    end if
end for

Source gets the RREPs.
for each intermediate node 'i'
  if (CONFIDENCE_LEVEL [i]  = = 0)
     Drop node 'i' and declare it to be malicious.
  end if
end for

for each node 'i' on the path
  Next hop node = Node with Maximum Confidence level.
  Find the Total and Average CONFIDENCE_LEVELs.
  Choose the path with the highest average CONFIDENCE_LEVEL.
  if (more than one path is available with the same value)
       Choose the path with the least HOP_COUNT.
  end if
 end for
Send packets along the chosen path.
End
```

Fig. 2: Confidence Level based prediction algorithm for Black Hole attacks

IV. PERFORMANCE ANALYSIS

This section describes the parameters (Table. I) and performance metrics used in our simulations.

Table I: Simulation parameters

Parameter	Value
Number of nodes	50
Packet size	1000
Data rate	100 Mbps
Traffic Type	CBR
Mobility model	Random way-point
Queuing policy	Drop Tail
Simulation Duration	250 ms
Queue Length	50
Start time	20 ms
Stop time	100 ms
Modulation Scheme	OFDM_QPSK
Frame Duration	0.020 ms

In case of Black hole attacks, the Confidence Level based prediction mechanism yields better results when compared to the attacked scenario. The following graphs show the performance of Confidence Level based mechanism (Fig.3 to Fig.6).

The Confidence Level based mechanism yields a better PDR and Throughput when compared to an attacked network. The solution does not degrade the performance.

Similarly, the Control and Total overheads are less when compared to a network with Black hole attacks.

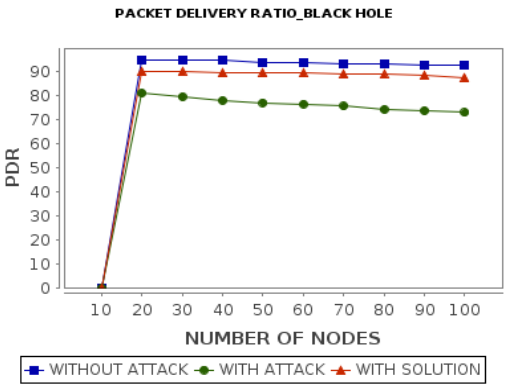

Fig. 3: Packet Delivery Ratio for Black Hole attack

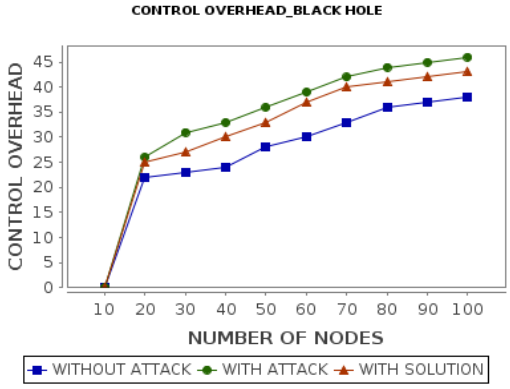

Fig. 4: Control Overhead for Black Hole attack

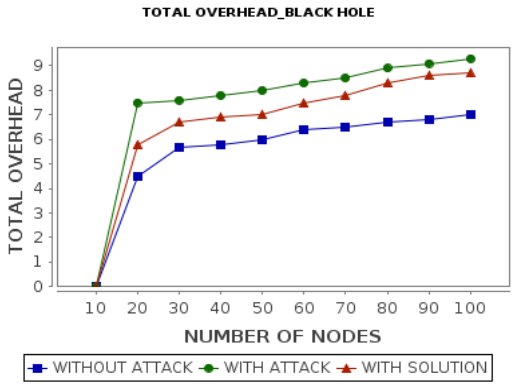

Fig. 5: Total Overhead for Black Hole attack

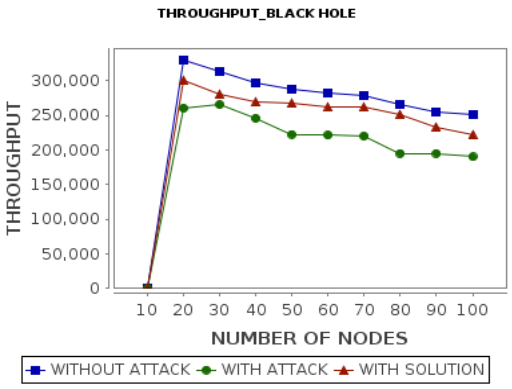

Fig. 6: Throughput for Black Hole attack

V. CONCLUSION

This work mainly focused on the Black hole in mobile WiMAX. It is obvious that the prediction mechanism yields better results when paths without malicious nodes are selected for transmission. This prediction method can be employed in multicasting protocols with some modifications.

REFERENCES

[1] "IEEE standard for local and metropolitan area networks: Part 16: Air Interface for Broadband Wireless Access Systems," IEEE Std 802.16- 2009, pp. 1 - 2080, 2009.

[2] "WiMAX Forum, WiMAX System Evaluation Methodology V2.1," pp. 230, 2008.

[3] "LAN MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society. Local and metropolitan area networks - Part 16: Air interface for fixed broadband wireless access systems - amendment 2: Medium access control modifications and additional physical layer specifications for 2-11 GHz," IEEE Standard 802.16a-2003, 2003.

[4] "IEEE C802.16m-07/029, Mobility Sensitive Master Key Derivation and Fast Re-authentication for 802.16m," 2007.

[5] Eklund, C. , Marks, R.B. , Stanwood, K.L. , Wang, S., "IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access," *IEEE Communications Magazine*, Vol. 40, No. 6, pp. 98 - 107, 2002.

[6] "IEEE P802.16Rev2/D2, DRAFT Standard for Local and metropolitan area networks," Part 16: Air Interface for Broadband Wireless Access Systems, pp. 2094, 2007.

[7] Huang, J., Huang, C-T.," Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations," *In Proceedings of IEEE International Conference on Communications*, 2011.

[8] Maccari, L., Paoli, M., Fantacci, R., "Security analysis of IEEE 802.16," *In Proceedings of International Conference on Communications proceedings*, 2007.

[9] Adhikary, K., Kumar, R., Kumar, A., "Securing Bandwidth Request Messages in WiMAX," *International Journal of Computer Applications*, Vol. 33, No. 3, pp. 1-5, 2011.

[10] Naseer, S., Younus, M., Ahmed, A., "Vulnerabilities Exposing IEEE 802.16e Networks To DoS Attacks:A Survey," *In Proceedings of Ninth IEEE ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, pp. 344 - 349, 2008.

[11] Deininger, A., Kiyomoto, S., Kurihara, J., Tanaka, T., "Security Vulnerabilities and Solutions in Mobile WiMAX," *International Journal of Computer Science and Network Security*, Vol. 7, No. 11, 2007.

[12] Bakthavathsalu, K. , Sampalli, S. , Qiang Ye, "Management Frame Attacks in WiMAX Networks: Analysis and Prevention," *In Proceedings of Seventh International Conference On Wireless And Optical Communications Networks (WOCN)*, pp. 1 -7, 2010.

[13] Shojaee, M. , Movahhedinia, N. , Ladani, B.T., " Traffic Analysis for WiMAX Network under DDoS Attack," *In Proceedings of Second Pacific-Asia Conference on Circuits, Communications and System (PACCS)*, Vol. 1, pp. 279 - 283, 2010.

[14] Chee, J., Ming Teo, "Improving Security in the IEEE 802.16 Standards," *In Proceedings of International Conference on Information Technology: New Generations (ITNG)*, pp. 408 - 412, 2011.

[15] Maru, S., Brown, T.X., "Denial of Service Vulnerabilities In the 802.16 Protocol," *In Proceedings of The Fourth International Wireless Internet Conference* (WICON 2008), pp. 1 - 9, 2008.

[16] Kahya-Abbaci, N., Ghoualmi, N., "A New Classification Based on IEEE 802.16 for Wireless Access," *Journal of Data Processing*, Vol. 2, No. 1, pp. 32 - 38, 2012.

[17] Nirwan Ansari, "WiMAX Security: Privacy Key Management," *In Proceedings of Sendai International*

Workshop on Network Security and Wireless Communications, 2007.

[18] Parish, D. J., Aparicio-Navarro, F. J., "Misbehaviour metrics in WiMAX networks under attack," *PGNeT*, 2010.

[19] Barbeau, M., Robert, J.M., "Rogue-Base Station Detection in WiMAX/802.16 Wireless Access Networks," *Annals of Telecommunications*, Vol. 61, No. 11-12, pp.1300-1313, 2006.

[20] Shon, T., Choi, W., "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions," *In proceeding of First International Conference on Network-Based Information Systems*, 2007.

[21] Qayyum, J., Lal, M., Khan, F., Imad, M., "Survey & Assessment of WiMAX, its security threats and their solutions," *International Journsal of Video & Image Processing and Network Security* , Vol. 11, No. 3, pp. 36-47, 2011.

[22] Liu, F., Lu, L., "A WPKI-based Security Mechanism for IEEE 802.16e," *In Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1 - 4, 2006.

[23] Han, T., Zhang, N., Liu, K., Tang, B., Liu, Y., "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions," *In Proceedings of 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 828 - 833, 2008.

[24] Khan, A.S., Fisal, N., Hussain, S., "Man-in-the-Middle Attack and Possible Solutions on WiMAX 802.16j," *In Proceedings of International Conference on Recent and Emerging Advance Technologies in Engineering*, 2009.

[25] Bogdanoski, M., Latkoski, P., Risteski, A., Popovski, B., "IEEE 802.16 Security Issues: A Survey," *In Proceedings of 16th Telecommunication Forum TELFOR 2008*, 2008.

[26] Hasan, J., "Security Issues of IEEE 802.16 (WiMAX)," *In Proceedings of 4th Australian Information Security Management Conference*, 2006.

[27] Jung, J., Jeung, J., Lim, J., "Control Channel Hopping for Avoidance of Scrambling Attacks in IEEE 802.16 Systems," *In Proceedings of Military Communications Conference*, pp. 1225 - 1230, 2011.

[28] Santhanam, L., Nandiraju, D., Nandiraju, N., Agrawal, D.P., "Active cache based defense against DoS attacks in Wireless Mesh Network," *In Proceedings of the 2nd IEEE International Symposium on Wireless Pervasive Computing (ISWPC 2007)*, 2007.

[29] Nait-Abdesselam, F., "Detecting and avoiding wormhole attacks in wireless ad hoc networks," *IEEE Communication Magazine*, Vol. 46, No. 4, pp. 127-133, 2008.

[30] Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, J., Nygard, K., "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," *In Proceedings of International Conference on Wireless Networks*, pp. 1 - 7, 2003.

[31] Khan, S., Loo, K-K., Naeem, T., Khan, M.A., "Denial of Service Attacks and Challenges in Broadband Wireless Networks," *International Journal of Computer Science and Network Security*, Vol. 8, No. 7, pp. 1 - 6, 2008.

[32] Deng, H., Li, W., Agrawal, D.P., "Routing Security in Wireless ad hoc Networks," *IEEE Communication Magazine*, Vol. 40, No. 10, pp.70-75, 2002.

[33] Abel, V.S., "Survey of Attacks on Mobile Adhoc Wireless Networks," *International Journal on Computer Science and Engineering*, Vol. 3, No. 2, pp. 826 - 829, 2011.