A COUNTERMEASURE FOR FLOODING ATTACK IN MOBILE WiMAX NETWORKS

Deva Priya and Pradeep Kumar

Department of CSE, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India.

ABSTRACT

Worldwide Interoperability for Microwave Access (WiMAX) is a new communication technology that conduits the fissure between fixed and mobile access and offers the same Quality of Service (QoS) to both types of users. Generally, WiMAX is more vulnerable to the inside and outside attacks due to the absence of any clear line of defense. The Mobile Subscriber Stations (MSSs) selected to transfer the packets to the Base Station (BS) are vulnerable to Denial of Service (DoS) attacks like flooding. Recent research has discovered that DoS attacks can easily be launched by injecting malevolent management frames into the WiMAX network based on the Privacy and Key Management- ReSPonse (PKM-RSP) and Automatic Repeat ReQuest (ARQ)-Reset messages. In this paper, an algorithm is proposed to mitigate the flooding attacks and enhance the security level in the network.

KEYWORDS

WiMAX, Threats, Flooding attack, Authentication, Flood count.

1.INTRODUCTION

WiMAX, Worldwide Interoperability for Microwave Access is a telecommunications technology that offers transmission of wireless data via a number of transmission methods. The WiMAX technology offers around 72 Mbps without any need for cables. It is based on IEEE 802.16 standard, usually known as Broadband Wireless Access (BWA) networks. WiMAX Forum was formed to encourage compliance and interoperability of the WiMAX IEEE 802.16 standard. It offers last mile broadband access as a substitute to conventional cable and DSL lines. Existing technologies such as Digital Subscriber Line (DSL), cable and fixed wireless are overwhelmed by expensive installs, problems with loop lengths, upstream upgrade issues, line-of-sight restrictions and poor scalability.

WiMAX is the next stage to broadband as well as a wireless world, extending broadband wireless access to new locations and over longer distances. It considerably reduces the cost of bringing broadband to new areas. It offers greater range and bandwidth than the other available or forthcoming broadband wireless technologies such as Wireless Fidelity (WiFi) and Ultra-wideband (UWB) family of standards. It provides a wireless alternative to wired backhaul and last mile deployments that use Data over Cable Service Interface Specification (DOGS1S) Cable modems, DSL, T-carrier and E-carrier (Tx/Ex) systems and Optical Carrier Level (OC-x) technologies. New organizations as well as individuals adopt broadband, whereas those already using broadband depend and demand better services with added benefits. To support this

DOI:10.5121/ijcsa.2014.4508

exceptional new demand, WiMAX has emerged as a feasible solution because of its inherent features that hold great promises for the future of wireless communications.
There has been a lot of excitement about WiMAX and the impact that this standard based wireless network technology has on the broadband access market. This hype has generated great expectations and the industry has responded with exceptional aggression and commitment towards taking broadband to the next level with WiMAX. 802.16-2004 or 802.16d referred as fixed WiMAX was developed by a third party. This standard lacks mobility. Some amendments were made to 802.16d and it was referred as 802.16e. 802.16e introduced mobility and is known as mobile WiMAX. Figure 1 shows the WiMAX architecture.

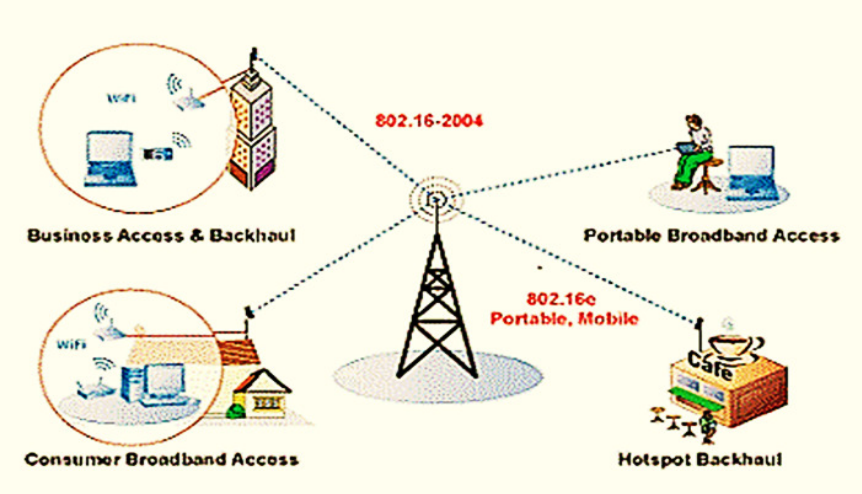

Figure 1. WiMAX Architecture

The general initiative of metropolitan area wireless networking as envisioned by 802.16 begins with fixed wireless. A backbone of Base Stations (BSs) is connected to a public network and each BS carries hundreds of fixed Mobile Subscriber Stations (MSSs) which can be both public hot spots and fire-walled enterprise networks.

Later in the development cycle of 802.16e, WiMAX encourages mobile wireless technology specifically wireless transmissions directly to mobile end users. This is similar in function to the General Packet Radio Service (GPRS) and the one time Radio Transmission Technology (RTT) offered by mobile phone companies.

The Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) are the two types of duplexing mechanism followed by IEEE 802.16.

Downlink-MAP (DL-MAP) and Uplink-MAP (UL-MAP) are used to describe the contents of Downlink (DL) and Uplink (UL) respectively and also the timing in both transmissions [1]. In TDD, the MSSs are provided with time slots for transmission and the BSs with the DL schedules. In FDD, both UL and UL are simultaneous processes.

The privacy issues are dealt by the Privacy Sublayer (PS) in the Medium Access Control (MAC) layer. The PS is based on two main components, an encapsulation protocol for providing packet data encryption and Privacy and Key Management (PKM) protocol for providing secure distribution of the keying material and authorized access to connection between BS and SS.

The two main goals of WiMAX are

- To provide maximum security to the wireless networks
- To provide the network with access control

In [2], various requirements that a WiMAX protocol should satisfy to provide high security are discussed. Following features are to be considered for ensuring security in a network.

Confidentiality

When sensitive data is transferred through the WiMAX network, it should ensure that the data is available only to authorized users. If this confidentiality is not maintained, security of the standard is not guaranteed.

Authenticity

Mutual authentication should be provided to ensure authenticity. This mutual authentication mechanism should ensure that the data sent by the user is received without any modification. It should not be possible for intruders to insert false information into the original data. The data should be accessible only by authenticated users.

Integrity

The standard must ensure that the shared key should not be tampered or altered by the intruder. The data should not be tampered while in transit by an intruder. This property is as important as authentication.

Access Control

The standard should ensure that only authorized users should access the network by connecting to it and receive desired services.

1.1.How WiMAX Works?

The backhaul of the WiMAX is based on the typical connection to the public wireless networks by using optical fibre, microwave link, cable or any other high speed connectivity. In few cases such as mesh networks, Point-to-Multipoint (PMP) connectivity is also used as a backhaul. Ideally, it uses Point-to-Point (P2P) antennas as a backhaul to join subscriber sites to each other and to BSs across long distances.

A WiMAX BS serves MSSs using Non-Line-of-Sight (NLOS) or Line-of-Sight (LOS) PMP connectivity which is referred to as the last mile communication. Ideally, WiMAX uses NLOS PMP antennas to connect residential or business subscribers to the BS. A WiMAX Customer Premises Equipment (CPE) typically serves a building using wired or wireless Local Area Network (LAN).

1.2.Layered Architecture

The WiMAX/802.16 is a layered architecture consisting of two main layers:

- Physical (PHY)layer
- Medium Access Control (MAC) layer

Both the layers are vulnerable to attacks of their own kind. In the PHY layer the bits are transmitted as equal length sequenced frames. This layer is subjected to attacks like jamming and scrambling. The MAC layer is connection oriented with two types of connections:

- Management connections
- Data transport connections

This layer experiences attacks like Man-In-The-Middle (MITM), DoS and eavesdropping. Figure 2 shows the layers of IEEE 802.16 protocol. The important part of this layered architecture is the sublayer system. The standard defines the Services Access points (SAPs). The MAC layer consists of three sublayers they are

- Convergence Sublayer (CS)
- Common Part Sublayer (CPS)
- Privacy Sublayer (PS)

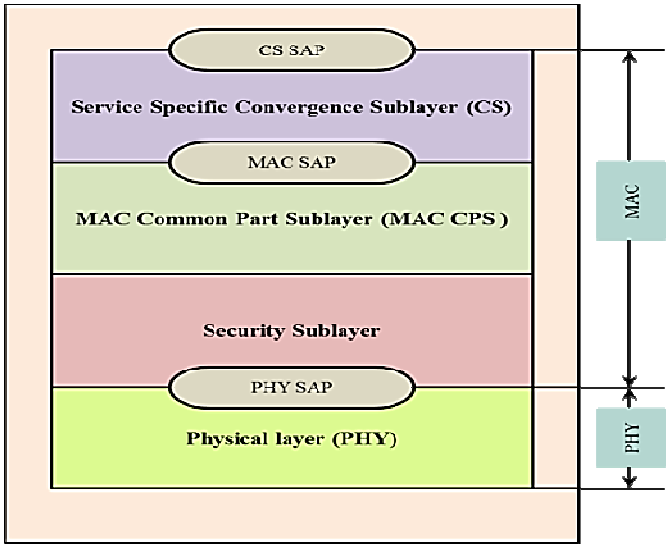

Figure2. WiMAX Layered Architecture

Convergence Sublayer (CS)

The service specific CS maps higher level data services to the MAC layer service flows and connections. There are two types of CSs:

- Asynchronous Transfer Mode (ATM) CS which is designed for ATM network

- Service packet CS is designed to support Ethernet, P2P, both IPv4 and IPv6 internet protocols and Virtual Local Area Network (VLAN) [3].

Common Part Sublayer (CPS)

The CPS is the core of the standard. The CPS defines the rules and mechanisms for system access, connection management and bandwidth allocation. Functions like UL scheduling, bandwidth request and grant, Automatic Repeat Request (ARQ) and connection control are also defined here. Communications between the CS and the MAC CPS are done by MAC Service Access Point (MAC SAP).

Privacy Sublayer

There are two main protocols in this sublayer:

- Encapsulation protocol for encrypting packet data across the fixed BWA.
- PKM for providing secure distribution of keying data from the BS to the MSS [4].

2.THREATS IN WiMAX

Some of the common threats in WiMAX are discussed below.

Jamming

Radio Frequency (RF) jamming is seen in all wireless networks. This attack is due to the overwhelmed interference of the RF signal into the spectrum range used by the system. This denies the service of the wireless nodes that are in the range of the RF signals. This jamming attack is a DoS attack.

Scrambling

Scrambling is due to the interference of the RF signal during the transmission of the management signals. As this attack is seen for a short period of time, it is difficult to detect when compared to jamming attack. It leads to overall degradation of the system.

Man-In-The-Middle (MITM)

MITM attacks occur when an adversary deceives a MSS to appear as a legitimate BS while simultaneously deceiving a BS to appear as a legitimate MSS. This allows an adversary to eavesdrop and corrupt data communications.

Denial of Service (DoS) Attack

It is the most harmful and dangerous attack which can be launched on any layer of BWA network. When authorized users are not provided requested services within a defined maximum waiting time, it means that a DoS violation has occurred. DoS attacks target availability by preventing communication between network devices or by preventing a single device from sending or receiving traffic, where availability ensures that authorized users can access the data, services and network resources from anywhere anytime. This type of attack will invoke unnecessary state transitions.

Eavesdropping

Eavesdropping occurs when an adversary uses a WiMAX traffic analyzer within the range of a BS and/or SS/MS. The adversary may monitor management message traffic to identify encryption ciphers, determine the footprint of the network or conduct traffic analysis regarding specific WiMAX nodes.

Flooding Attack

Flooding attacks occur when a network or service becomes heavy with packets, initiating incomplete connection requests that it can no longer process genuine connection requests. In data flooding attack, the attacker gets into the network and sets up paths between all the nodes in the network. Once the paths are established, the attacker injects an immense amount of useless data packets into the network which are directed to all the other nodes in the network. These immense unwanted data packets congest the network. Any node that serves as destination will be mounted with useless and unwanted data.

Blackhole Attack

In the blackhole attack, the intruder takes hold of a particular routing node and makes it to drop all its packets. If the attacker drops only selective packets and keeps forwarding the rest of the packets, then the attack is called as grayhole attack. Black hole attack results in extensive use of time and energy by the selected node in the WiMAX network.

In [5], a confidence level based prediction mechanism to predict the prevalence of black hole attack is proposed which eliminates the vindictive nodes.

Wormhole attack

In wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attackers is known as a wormhole. The wormhole attack is particularly dangerous in ad hoc networks, in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node.

3.AUTHENTICATION IN WIMAX

As explained in [6], the authentication method supported by the MSS is determined by the encapsulation protocol. The encapsulation protocol consists of data encryption algorithm, the data authentication algorithm and Traffic Encryption Key (TEK) encryption algorithm. The authentication and authorization by the MSS is defined by the PKM protocols. It also describes the periodic re-authorization, reception and renewal of key material.

IEEE 802.6 supports two versions of PKM protocols: MSS authentication is provided by PKMv1 and mutual authentication by PKMv2. The Security Association (SA) is a set of security parameters of the connection.

3.1.Vulnerabilities Analysis

The various vulnerabilities in IEEE 802.16 are discussed in [7].

Unauthenticated Messages

Most of the messages in IEEE 802.16 are integrity protected by either a Hash based Message Authentication Code (HMAC) or Cipher based Message Authentication Code (CMAC). In WiMAX security architecture there is no common key authentication used to secure the broadcast messages. There are certain messages which do not contain any common key, where these messages will become a threat.

Unencrypted Management Communication

In WiMAX management messages are still sent in the clear. The consequential risk is outlined in this section. When a MSS performs initial network entry, it negotiates communication parameters and settings with the BS. Here, a lot of information like security negotiation parameters, configuration settings, power settings, mobility parameters, vendor information and capabilities of the MSSs are exchanged. Currently the complete management message exchange in the network entry process is unencrypted and the above mentioned information can be accessed just by listening on the channel.

3.2.Shared Key in Multicast and Broadcast Service

The multicast and broadcast service offers the possibility to distribute data to multiple MS with one single message. This saves cost and bandwidth. Broadcasted messages in IEEE 802.16e are encrypted symmetrically with a shared key. Every member in the group knows the key and can decrypt the traffic. Message authentication is based on the same shared key.

4.RELATED WORK

In [8], various threats to wireless networks are discussed. It proposes a solution to eliminate the threats by using a strong encryption technique with intrusion prevention system. The PHYlayer is more vulnerable to threats than the MAC layer

As described in [9], 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 the messages. Anyone with a properly placed radio receiver can catch an authorization message, modify and retransmit it. There is no digest used to prove that the message is not modified. To overcome these attacks, PKM is used.

In [10], key space vulnerability due to insufficient key size is discussed. To protect the keying materials from attack, a solution is proposed that increases the number of bits for both the keys.

Network performance can be degraded if the attacker sends spoofed messages to the BS and make it believe that the MSS has weaker security algorithm. [11].

The threats that arise from WiMAX authentication scheme are discussed in [12]. WiMAX supports unilateral device level authentication which can be implemented in a similar way as WiFi MAC filtering based on the hardware device address. Therefore, address sniffing and spoofing makes a MSS masquerade attack possible. In addition, the lack of mutual authentication makes a MITM attack from a rogue BS possible. However, a successful MITM attack is difficult because of the Time Division Multiple Access (TDMA) model in WiMAX.

The attacker and the legitimate BS must transmit at the same time using a much higher power level to "hide" the legitimate signal. Various attacks in the authentication phase and the key material exchange phase are discussed. The process in the authentication phase can be interrupted by an intruder by obtaining the authorization reply message and sending false request message to the BS. This overloads the BS and it does not respond to the messages from the MSS. This is called as replay/DoS attack. In the data encryption phase, the MSS requests the key material (TEKs). The MSS periodically sends key request messages referring to one of its valid Security Association Identifiers (SAIDs). An attacker captures the TEK messages and replays them to gain information needed to decrypt the data traffic. This attack can be mitigated by increasing the length of the sequence number so that a satisfactory amount of TEK sequence numbers can be generated and transmitted within the longest validity duration of the Authentication Key (AK).

In [13], the Rogue BS or Relay Station (RS) attack is discussed. It is one of the most common attacks on wireless authentication protocols. A malicious node impersonates a legitimate BS or RS node with fake credentials and tries to convince a joining RS or MSS to connect with it. Alternately, an attacker may try to compromise a legitimate BS or RS to get control over it. IEEE 802.16j uses PKMv2 to counter possible rogue BS attack by using mutual authentication. However, there is an implicit assumption in PKMv2 that BS is always trustworthy. PKMv2 does not provide any protection to detect and counter the attack from a compromised BS. Moreover, the distributed security mode in Mobile Multihop Relay (MMR) WiMAX networks also makes rogue RS attack possible. This is because the authentication procedure between RS nodes is not performed by a centralized server but is based on the trust between nodes. If one node is compromised, its trust with other nodes is also compromised.

In [14], a cross-layered mechanism is proposed which provides a secured transfer of data as well as avoids retransmission. This work proposes a novel energy-conserved, fault-tolerant, intrusion-less clustering mechanism that ensures security at the group heads in a region.

5.FLOODING ATTACK

By flooding a server or host with connections that cannot be completed, the flooding attack eventually fills the host's memory buffer. Once this buffer is full no further connections can be made and results in a DoS attack. The malicious node steams excessive amount of false packets into the network that clog the network and deplete the available network bandwidth for communication among other nodes in the network.

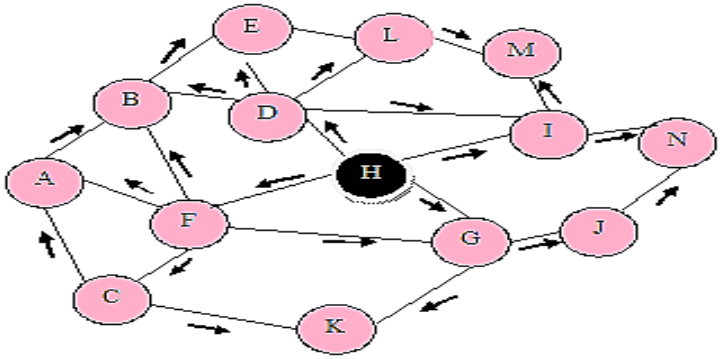

Figure 3. Flooding attack

A legitimated user will not be able to use the network resources for valid communication. The goal of flooding attack is to exhaust the network resources like bandwidth and to consume a node's resources like computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. Due to limited availability of resource constraints, resource consumption owing to flooding reduces the throughput of the network [15].

Flooding is possible in almost all on-demand routing protocols, even in the secure on-demand routing Secure Routing Protocol (SRP), Secure Ad hoc On-Demand Distance Vector (SAODV), Authenticated Routing Ad hoc Network (ARAN), Ariadne etc.

Depending on the type of packets used to flood the network, flooding attack can be categorized into different categories. In Route REQuest (RREQ) flooding attack, the attacker selects IP addresses which do not exist in the networks as destination addresses. Then it successively creates a bulk of RREQ messages with maximum Time-To-Live (TTL) value for these void IP addresses. The whole network will be filled with RREQ packets sent by the attacker. As these destination addresses are invalid, no node sends Route REPly (RREP) packets for these RREQs and the reverse routes in the routing table of the intermediate nodes will be occupied for longer time and gets exhausted soon (Figure 3).

A threshold can be set and the node sending more requests (above threshold) within a certain time interval can be declared as vindictive.

5.1. Flood Count (FC) based solution for Flooding attack

As stated earlier, a threshold can be set to restrict a node from sending more number of packets in a particular time interval. The proposed algorithm is applicable for a topology with a source, a destination and more than one intermediate node. The reason is given below.

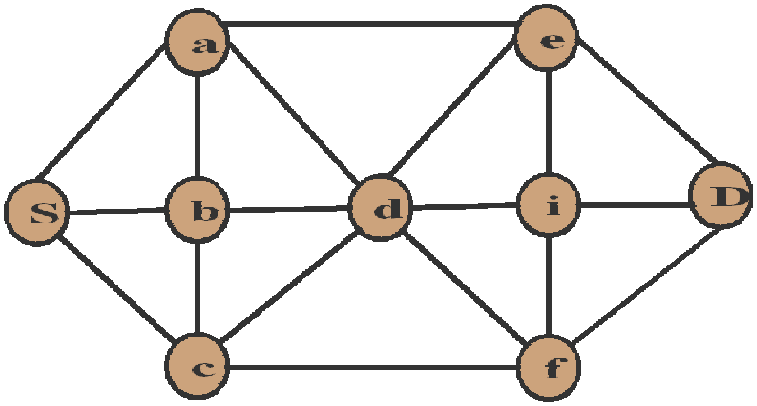

Figure 4. Example

In Figure 4, let 'S' be the source and 'D' be the destination respectively. Let 'i' be an intermediate node with respect to which the observations are made.

Let the total number of nodes in any network be 'n'.Within a short time period say, 't', node 'i' can receive packets from source 'S' and 'n - 3' (leave S, D, i) intermediate nodes. In the figure, there are 6 intermediate nodes. To be more clear, any intermediate node can be involved 'n - 3' times in forwarding the packets to 'i'. For example, a packet originating from 'S' can reach 'i' through 'd'.

1. S - **a - d - i** - D
2. S - c - **b - d - i** - D
3. S - a - b - **c - d - i** - D
4. S - a - **e - d - i** - D
5. S - c - **f - d - i** - D

From the above listed paths, it is understood that, any intermediate node say 'd', may be involved atmost 'n - 3' times in forwarding packets to another intermediate node or the destination. The nodes preceding the node 'd' may be any one of the nodes - a, b, c, e, f, S (other than the 'D, i and d'). The algorithm is given in Figure 5.

The above discussion was made to make a correct choice of the limit say, FLOOD_COUNT. For each node, HOP_COUNT and FLOOD_COUNT are computed and stored dynamically. If node 'i' comprehends a node with HOP_COUNT = 0, then it identifies it as the source and sets the FLOOD_COUNT to 'n - 3' for that node (Figure. 4).

When a source 'S' transmits a packet, its FLOOD_COUNT is set to 'n -3', while intermediate node gets '1'. This is done so as to ensure that no node acts as a source more than once in time 't'.

```
initialize( )

begin
```

```
Source sends RREQ to all the neighbours for each intermediate node 'i'
   HOP_COUNT = 0
   FLOOD_COUNT = 0
end for
end

Algorithm Flood ( )
begin
initialize( )
for each intermediate node 'i'
    if ( 'i' generates and sends a packet and is the Source)
        Set FLOOD_COUNT [i] += n - 3
   else if ('i' forwards a packet and is an intermediate node)
          Set FLOOD_COUNT [i] += 1
          HOP_COUNT [i] +=1
   end if
   if ( FLOOD_COUNT [i] ≤ (n - 3) and 'i' is an intermediate node ||FLOOD_COUNT [i]
= (n - 3)  and 'i' is the source node S)
          Flooding has not occurred.
   else if ( FLOOD_COUNT [i] > (n - 3))
          Flooding has occurred.
          'i' is a malicious node.
   end if
end for
Choose the path with the least total FLOOD_COUNT
Send packets along the chosen path.
end
```

Figure 5. Flood Count based Algorithm for Flooding attack

Initially,

$$\text{FLOOD COUNT} = \begin{cases} 1, \text{for intermediate node} \\ n - 3, \text{for S} \end{cases}$$

Finally,

$$\text{FLOOD COUNT} = \begin{cases} \leq n - 3, \text{for intermediate nodes} \\ = n - 3, \text{for S} \\ > n - 3, for\ malicious\ nodes \end{cases}$$

If there is only one intermediate node, then the FLOOD_COUNT will become '0'. There are chances for the 'S' to be the malicious node. A scenario with a single intermediate node is very rare and hence can be ignored.The TOTAL_FLOOD COUNT for a path with 'n' nodes is given by,

$$\text{TOTAL FLOOD COUNT} = \sum_{i=1}^{n} \text{FLOOD COUNT}$$

6.PERFORMANCE ANALYSIS

This section describes the parameters (Table 1) and performance metrics used in the simulations. The system was simulated using ns2.

The performance of the network degrades when the network is flooded with RREQs. In the Flood Count (FC) based prediction technique, the malicious nodes are eliminated thus avoiding further floods, thus yielding better results (Figure 6 to 8).

Table 1. 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
Queue Length	50
Simulation Duration / Start time / Stop time	250 ms / 20 ms / 100 ms
Modulation Scheme	OFDM_QPSK
Frame Duration	0.020 ms

The Flood Count (FC) based algorithm yields better results. The PDR of the network is improved after applying the FC algorithm as shown in the figure (Figure 6).

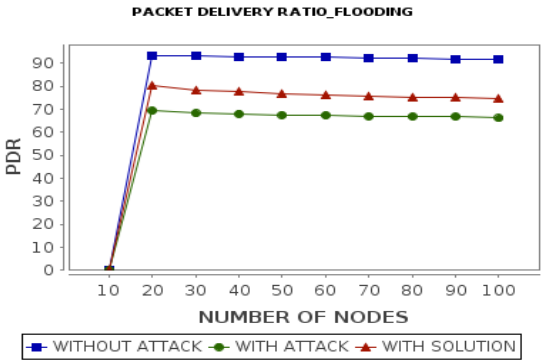

Figure 6. Packet Delivery Ratio

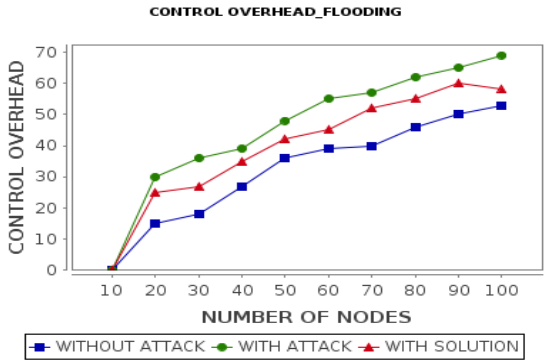

Figure 7. Control Overhead

Control overhead is the ratio of total number of control packets transmitted and the number of data packets expected to be received. The control overhead involved in overcoming the flooding attack is tolerable (Figure 7).

Similarly, the throughput of the system does not deteriorate after the application of FC algorithm as shown in Figure 8.

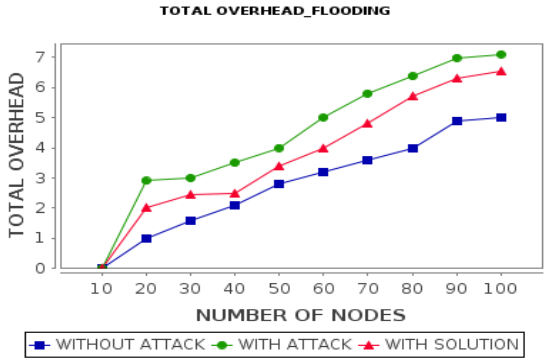

Figure 8. Throughput

7.CONCLUSION

This work mainly focusses on flooding attacks in mobile WiMAX. It is obvious that the prediction mechanism yields better results in terms of throughput, control overhead and Packet

Delivery Ratio (PDR) when paths without malicious nodes are selected for transmission. In the future, this prediction method can be employed in other multicasting protocols with some modifications.

REFERENCES

[1] Thamilarasu, Geethapriya, Sumita Mishra, and Ramalingam Sridhar, "A cross-layer approach to detect jamming attacks in wireless ad hoc networks", In Proceedings of the Military Communications Conference, MILCOM 2006, pp. 1-7, 2006.

[2] Wei-min, Lang, Wu Run-Sheng, and Wang Jian-qiu, "A Simple Key Management Scheme based on WiMAX", In Proceedings of the International Symposium on Computer Science and Computational Technology, ISCSCT'08, vol. 1, pp. 3-6, 2008.

[3] Aslan, Mahmoud NasreldinHeba, Magdy El-Hennawy, and Adel El-Hennawy, "WiMAX security", 2008.

[4] Sakib, AKM Nazmus, and Mir Md Saki Kowsar, "Shared key vulnerability in IEEE 802.16e: Analysis & solution", In Proceedings of the 13th International Conference on Computer and Information Technology (ICCIT), pp. 600-605, 2010.

[5] Barbeau, Michel, "WiMAX/802.16 threat analysis", In Proceedings of the 1st ACM International workshop on Quality of Service &Security in Wireless and Mobile Networks, pp. 8-15, 2005.

[6] Priya, M. Deva, M. L. Valarmathi, S. Aishwarya, and K. Jaya Bharathi, "A Countermeasure for Black Hole Attack in Mobile WiMAX Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol. 2, No. 3, pp-0964, 2013.

[7] Saeed, Nuha, and MahfuzaMunira, "WiMAX security analysis", PhD diss., Department of Electrical and Electronic Engineering, 2011.

[8] Hasan, Jamshed, "Security Issues of IEEE 802.16 (WiMAX)", In Proceedings of the Australian Information Security Management Conference, pp. 71, 2006.

[9] Liu, Fuqiang, and Lei Lu, "A WPKI-based Security Mechanism for IEEE 802.16e", In Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2006, pp. 1-4, 2006.

[10] Sikkens, Bart, "Security issues and proposed solutions concerning authentication and authorization for WiMAX (IEEE 802.16e)", In Proceedings of the 8th Conference on IT Enschede University of Twente, 2008.

[11] Maccari, Leonardo, Matteo Paoli, and Romano Fantacci, "Security analysis of IEEE 802.16." In Proceedings of the International Conference on Communications, ICC'07, pp. 1160-1165, 2007.

[12] Deininger, Andreas, ShinsakuKiyomoto, Jun Kurihara, and Toshiaki Tanaka, "Security vulnerabilities and solutions in mobile WiMAX", International Journal of Computer Science and Network Security, Vol. 7, No. 11,pp. 7-15, 2007.

[13] Huang, Jie, and Chin-Tser Huang, "Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations", In Proceedings of the International Conference on Communications (ICC), pp. 1-5, 2011.

[14] Priya, M. Deva, J. Sengathir, and M. L. Valarmathi, "ARPE: An Attack-Resilient and Power Efficient Multihop WiMAX Network", International Journal on Computer Science and Engineering, 2010.

[15] Refaei, M. Tamer, Vivek Srivastava, Luiz DaSilva, and Mohamed Eltoweissy, "A reputation-based mechanism for isolating selfish nodes in ad hoc networks", In Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous 2005, pp. 3-11, 2005.