International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 03 (MAY-JUNE, 2016)

# Detection and Mitigation of Flooding Attack in WIMax Network

**Pratibha Jadon**
Department of Computer Science & Engineering
Sagar Institute of Research & Technology, Bhopal, India
pratibha_jadon10@yahoo.com

***Abstract—*** Wimax is a descriptor that means worldwide ability for Microwave Access (Wimax). Wimax is predicated on Wireless Metropolitan space networking standards developed by the IEEE 802.16 group. Wimax facilitate the broadband services anytime in wireless setting, where needed. Worldwide ability for Microwave Access may be a new communication technology that passage the fissure between fastened and mobile access and provide constant to each varieties of user. In today's situation such mobile broadband services and applications are extremely necessitate as its offers freedom to the subscribers to be connected where they're at a viable price with important amenities like increasing information measure whereas accessing kind of mobile and roaming devices. The primitive edition of WiMAX is predicated on IEEE 802.16 and is specially designed for fastened and roaming access, that is advances to support movability and quality supported IEEE 802.16e, additionally called Mobile WiMAX. Wireless is additional susceptible to the within and out of doors attack because of absence of any clear line of defense. in conjunction with several attacks, such networks are significantly additional susceptible to denial of service attacks additionally called flooding. Route request flooding attack is one in all the DDoS attack. Same are going to be possible on WiMax network throughout choice of SS to transfer the packet to the BS. Recent analysis has discovered that DoS attacks can easily be launched via injecting.

***Keywords—*** BS, DoS, DDoS, IEEE802.16, flooding, PMP, RREQ, Wi-Fi, WiMax

## I. INTRODUCTION

Wimax is an acronym meaning Worldwide Interoperability for Microwave Access (Wimax). Wimax is based on Wireless Metropolitan Area Networking (WMAN) standards developed by the IEEE 802.16 group. Wimax facilitate the broadband services anytime in wireless environment, wherever required. Originally the WiMax (IEEE 802.16) standard was designed to transport Non-Line-Of-Sight (NLOS) connectivity to the subscriber to Access Point (base station) up to the cell radius of 3-10 km. Wimax network systems can deliver up to 40 Mbps per channel capacity. This is adequate bandwidth to support hundreds of businesses network having T-1 Channel speed as well as provides connectivity to the thousands of home users (residences) via DSL (Digital Subscriber Line) Connection simultaneously. A broad industry association the WiMax Forum has started certifying to the broadband wireless products for interoperability and compliance with a standard. WiMax technology already has been incorporated in notebook computers and PDAs (Personal Digital Assistant) to deliver high speed mobile Internet services on-demand in any place. Wimax is the next generation of wireless technology deliberated to facilitate high speed mobile Internet access to the large array of devices including notebook PCs, smart-phones etc. It makes possible the delivery of last mile wireless broadband access as an alternative to cable and Digital Subscriber Line (DSL). IEEE 802.16 is a standard for wireless broadband access network. IEEE 802.16 (WiMax) are covered longer distance (transmission range) than other wireless network like Wi-Fi or WLAN (IEEE802.11) with serving more stylish and enhanced Quality of-Service (QoS) support through MAC level. Various application and service types can be used in 802.16 networks and the MAC layer is designed to support this convergence. As always, security is an essential prerequisite for the success of every communication technology[12]. Wireless communications are by nature more vulnerable to a number of different attacks such as man-in-the-middle, DoS and replay. In the case of WiMAX -which was initially constructed with respect to a protocol for wired environments-, the security provision is rather inefficient as wireless and wired realms enjoy very different threat models. Moreover, with each version of the standard new improvements were added but at the same time new threats emerged. For instance, lower frequencies (and as a result NLOS communication) introduced in IEEE 802.16-2004 reduce the hardware implementation complexity and the physical placement constraints for an attacker. Similarly, mesh mode is by definition insecure as it assumes the trustworthiness of all nodes of the network. Moreover, the support for mobility facilitates aggressors to launch attacks from virtually anywhere within the network. The relay station feature, introduced in the 802.16j-2009, announces a new element on the network, but with it, another target of possible attacks is added. The latest version of this standard added enhancement in the security mechanisms that include encrypted control messages and a new version of the Privacy and Key Management protocol (PKMv3). However, since this version is very recent and there are no published works to report on the robustness of its security features so far, it will be excluded from this survey. For the same reason attacks against the 802.16j amendment are left out.

Nevertheless, it is true that the rest of the amendments of the standard, despite the constant security improvements, maintain a considerable number of security inefficiencies, exposing the user and the network to a significant number of threats. Worldwide Interoperability for Microwave Access (WiMAX) is a new communication technology that conduit the fissure between fixed and mobile access and offer the same to both types of user. In today's scenario such mobile broadband services and applications are highly necessitate as its offers freedom to the subscribers to be connected wherever they are at a viable cost with significant amenities like increasing bandwidth while accessing variety of mobile and roaming devices. The primitive edition of WiMAX is based on IEEE 802.16 and is specially designed for fixed and roaming access, which is advances to support portability and mobility based on IEEE 802.16e, also known as Mobile WiMAX. Wireless (especially MANET) is more vulnerable to the inside and outside attack due to absence of any clear line of defense [24]. Along with many attacks, such networks are particularly more vulnerable to denial of service (DoS) attacks also known as flooding. Route request flooding attack is one of them DDoS attack. Same will be possible on WiMax network during selection of SS to transfer the packet to the BS. Recent research has discovered that DoS attacks can easily be launched via injecting alevolent management frames into the WiMax based on the PKM-RSP and ARQ-Reset message are used to launched DoS attacks. There is urgent requirement to evaluate the DDoS attack and develop an efficient prevention mechanism for the WiMax network. In this article we have surveyed the WiMax network and its future perspective and also proposed a novel approach to defend against the blow of flooding attack in WiMax network. Rest of the paper organized as follow, section 2 describes countermeasure and treat of WIMax, and section 3 describes the proposed algorithm as security aspect. Section 4 discusses the obtained results of the proposed system; finally section 5 gives the conclusion of this paper.

## II. Literature Survey

The previous work in field of WiMax Network is discussed in this section. Each and every author is provides their valuable contribution. The main goal of the proposed system is to detect the Denial of Service (DoS) attack in WiMax Network. The proposed work has been tested under NS-3.18 network simulator Countermeasure of WIMAX. IEEE has defined two layers for WiMax in IEEE 802.16 DRAFT. Both the layers have some designing flaws that have to be a security hole in the WiMax network. According to author [frm_ref2], Security threats may occur in both the PHY and the MAC layers [22]. The attacker attacks with Radio Frequency (RF) channel for PHY layer threats. For MAC layer threats, the attackers spoof, modify and reply the MAC layer messages. In this paper, we concentrate only on MAC layer issues. The following sub-sections discuss the PHY layer security threats and MAC layer security threats along with counter measures. A PHY layer security issues[6], [22]and [24]: Scrambling and jamming are the two possible threats in PHY layer. For scrambling, the attackers will scramble the uplink slots of other MS's by their own data and make it unreadable for BS. Jamming at the physical layer is a kind of denial-of-service (DoS) attack that uses intentionally interfering radio communication by introducing the noise to disrupt the reception of messages in both uplink and downlink. B. MAC layer security issues in PMP Network the causes of MAC layer security issues are due to certain un-encrypted MAC management messages. The major security issues in PMP network is DoS/Reply attacks during MS Initial network entry. DoS/Reply attacks during MS Initial network entry - When the MS enter into the network, it scans the downlink channel and synchronizes with it. In the downlink, BS announces the range of initial ranging code for MS. The MS selects any one of the ranging code and sends it to BS for initial ranging. The BS responds to the successful reception of ranging code by Ranging Response (RNG-RSP) message. The RNG-RSP message is used to nullify the offsets of frequency, time and power used by the MS. Then the MS goes for SBCREQ and other procedures as shown in Fig.1 The message flows before SA-TEK are un-encrypted nature. So the attacker can decode the MAC messages, modify and re-send it to BS or MS. The security issues during initial network entry are:

1. RNG-RSP vulnerability
2. Auth-Request and Invalid vulnerability and
3. Rogue BS.

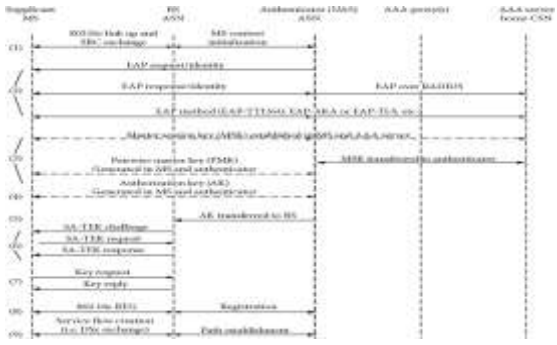

Figure 1. PKMv2 Procedure during Initial Network Entry [2,3]

In RNG-RSP vulnerability, the attacker modifies the RNGRSP message and sets the status as failed, then re-sends it to MS. So the MS goes for initial ranging again. If the attacker continuously sets the RNG-RSP status as failed, the MS cannot access the network. This leads to the DoS attack. Whereas [1, 26] has talking about

specialized DoS attack i.e. Signaling attack. Author uses the term "Signaling attack" instead of DoS, The targets of most denial of service (DoS) attacks so far are wire line endpoints, whose prevalence provides vast opportunities for an attacker to explore and launch new at-tacks. As the roll-out of nation-wide wireless data net-works continues, we expect more types of DoS attacks will start targeting wireless networks. Currently, third generation (3G) wide-area wireless net-works based on the CDMA2000 [27] and UMTS [28] standards are widely deployed. As of December 2005, there were over 300 million CDMA subscribers worldwide [27]. Emerging 3G data standards, like EDGE, HSUPA, HSDPA and Evolution-Data Optimized (EV-DO), promise to deliver broadband mobile Internet services with peak rates of 2.4 Mbps and 14.4 Mbps, respectively. The number of data subscribers is projected to reach a billion before 2010. As the number of data-capable wire-less endpoints escalates, they will become susceptible targets of new DoS attacks in the near future. In the article author has dogged about a novel DoS types attack phrase signaling attack, which seeks to overload the control plane of a 3G wireless network using low-rate, low-volume attack traffic, based on some of the aforementioned 3G-specific vulnerabilities. Unlike conventional DoS attacks that focus on the data plane, the signaling attack creates havoc in the signaling plane of a 3G network by repeatedly triggering radio channel allocations and revocations. To accomplish this, an attacker first sends a low-volume pack-et burst to a mobile. If the mobile does not currently have a radio channel, the network will allocate a new one to complete the data transfer. After an inactivity timeout, the radio channel is torn down to recycle it back for others' use and help preserve the mobile energy that will other-wise be wasted on maintaining the channel. Immediately after the channel release, the attacker sends another low-volume packet burst to the mobile so as to trigger another radio channel establishment. By repeatedly doing so at appropriately timed periods, this can generate a consider-able number of signaling operations. As detailed in Section 2, each channel establishment/release requires the RNC and BS to process more than 20 signaling messages. Launching this against large number of mobiles can easily introduce an excessive amount of signaling messages. The potential damage includes (1) overloading of RNC and BS, leading to reduced system performance, (2) denial of ser-vice to legitimate signaling messages due to congestion in the signaling paths, and (3) shortening of the mobile battery life. Modern Denial of Service attacks produce intrusive traffic (high volume) while in signaling attack can be exploit producing with generating less volume of traffic at slower rate as compared to DoS. Hence, signaling attack can efficiently dodge by applying modern intrusion detection/prevention approach especially via the mechanism of flooding-based DoS attacks detection. To understand the damage caused by the signaling at-tack, suppose that a 3G wireless network has inactivity timeout set to 5 s 1 and that an attacker generates a 40-byte packet burst (e.g., a TCP/IP packet with zero payloads). Experiments shows that if an attacker sends packet bursts in interval of 5 seconds or large than only 64 bits per second traffic volume has been produced by the attacker, which is undetectable by volume-based recognition systems. In other experiments, suppose if attacker is use a cable modem having 1.5 Mbps uplink bandwidth capacity then it can concurrently attack approximately 24 K mobiles, a number that is sufficient to bring down a wireless network infrastructure.

### 2.1 Modes of DoS Attack in WIMax

Author [3] has describes the types of DoS attack in WiMax- DoS attacks based on Ranging Request/Response (RNG- REQ/RNG-RSP) messages The RNG-REQ message is the first message sent by a SS to BS requesting transmission time, power, and frequency and burst profile information before joining the network. This initial message is not encrypted nor verified for authentication which makes it vulnerable to interception and modification to the least effective settings for the SS leading to degrading or denying the service to the SS. The RNG-RSP message is the message that the BS responds with to the RNGREQ message from the SS. The BS uses this message to change the up and downlink channels of the SS, transmission power level, fine-tune the settings of the transmission link and terminating the communications with the SS. Like the RNG-REQ, this message is neither encrypted nor authenticated and is exposed to alteration. For example, the SS transmitting power can be set to its maximum to quickly drain its battery [8]. DoS attacks based on Mobile Neighbor Advertisement (MOB_NBR-ADV) message The MOB_NBR-ADV message is sent from the BS to announce properties of neighboring BSs to its SSs that are about to perform a handover. Similarly, this message is neither encrypted nor authenticated and could, if forged, lead to inefficient or incorrect handovers [8]. Dos Attacks based on Fast Power Control (FPC) message **-** The FPC message is used by the BS to the make the SS quickly adjust its transmission power. Also, without an authentication mechanism, the FPC message is exposed to torture DoS attack [8]. DoS attacks based on Authorization-invalid (Auth-Invalid) message - The Auth-Invalid message is sent from the BS to the SS when the Authorization Key (AK) expires or the BS cannot verify the Hash-based Message Authentication Code/Cipher-based Message Authentication Code (HMAC/CMAC) properly. Since it is not protected by HMAC, it can be altered to invalidate a legitimate SS [8]. DoS attacks based on Reset Command (RES-CMD) message - The RES-CMD message in sent from the BS to the SS to reinitialize its MAC state machine when it is not responding properly or is

malfunctioning. It is protected by HMAC; however, it is still vulnerable to DoS attacks [8].

## III. PROPOSE ALGORITHM

Propose system is providing the solution against DoS (flooding) attack in WiMax network.

Proposed algorithm has been divided into 2 segments-

1. Setting up WiMax Scenario in NS-3.18. In which 5 SS and 1 BS has been setup.
2. Exploiting DoS attack in WiMax-
   To achieve these two scenarios has been consider –
   a. MAC layer DoS attack by modifying RNG-RS function design initialization of the SS onto BS.
   b. Transport Layer- Excessive number of small packets has fired towards BS continuously.

### A) Algorithm for Setting Up DoS Scenario in NS-3 WIMax

Proposed System has focused on two mode of DoS effect-

1. DoS using RNG-REQ

```
DoS: SSLinkManager::SendRangingRequest (uint8_t uiuc,
uint16_t allocation Size)
{
Do all steps as per the IEEE 802.16 draft (AS PER NS-3);
}
if (m_waitForRngRspEvent.IsRunning ())
{
Simulator::Cancel (m_waitForRngRspEvent);
}
m_rangingStatus = (WimaxNetDevice::RangingStatus)
rngrsp.GetRangStatus ();
NS_ASSERT_MSG (m_rangingStatus==
WimaxNetDevice::RANGING_STATUS_CONTINUE ||
m_rangingStatus ==
WimaxNetDevice::RANGING_STATUS_ABORT
|| m_rangingStatus ==
WimaxNetDevice::RANGING_STATUS_SUCCESS,
GOTO DoS;
```

### B) By sending zero payload TCP/UDP packet

```
a. For TCP
tcpClient[i].SetAttribute ("MaxPackets", UintegerValue
(2000));
tcpClient[i].SetAttribute ("Interval", TimeValue
(Seconds (0.1)));
tcpClient[i].SetAttribute ("PacketSize", UintegerValue
(24));

b. For UDP
udpClient[i].SetAttribute ("MaxPackets", UintegerValue
(2000));
udpClient[i].SetAttribute ("Interval", TimeValue
(Seconds (0.1)));
udpClient[i].SetAttribute ("PacketSize", UintegerValue
(24));
```

Proposed system has assumed that the probability of get comprise (or inherent suspicious) node of SS is more than the BS. It does not mean that BS can't be compromise but in most cases the SS can easily be compromised or an attacker by nature to disrupt the operation of WIMax SO that here the detection method has been applied on the BS itself using profile reputation of SS by statistical method of number of packet (initialization packet i.e. RNG_REG) related to back off timer-

```
if (no_RNG_REG > 10 && Backoff_Timer !=EXPIRE)
{
  Mark [ss] = DIRTY
}
If else (packet_size[tcp/udp]
== size [min_header_len] || [DATA=0]
{
  Mark [ss] = DIRT
}
else
{
   Mark [ss] = HEALTHY;
  }
```

## IV. RESULTS AND DISCUSSION

### Performance metrics

Following routing protocols has been used to evaluate the performance of routing in WIMax Network on NS-3 test bed.

1. Mobility Models- Various mobility are popular for simulation, Random Waypoint Mobility Model is more accurate for wireless scenario. Propose system has adopted the same.
2. Evaluation Metrics -Followings standardized metrics will be used for evaluations.
   a. Packet Delivery Ratio
   b. Throughput
   c. Packet Loss
   d. End-to-End Delay
   e. Routing Overhead

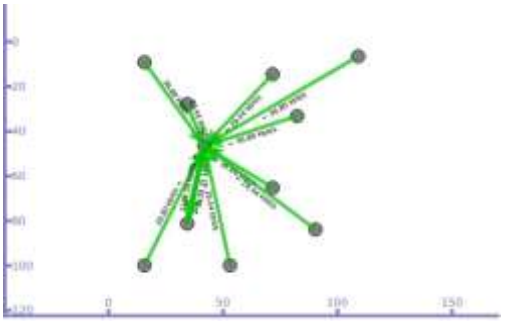

Figure 2. Simulation with 10 SS nodes during exploitation of Flooding in WIMax

Before outlining the results obtained, first insight the parameters of evaluation f WIMax as mentioned above. In this we are discussion the throughput of WIMax. Throughput – For detecting Flooding (DoS) scenario throughput has been set as benchmark for evaluating the normal WIMax to flooded WIMax. Figure 3 has shown

the throughput of 5 SS (simulation has been set to randomly select the nSS/2 nodes) nodes in normal scenario in WIMax.

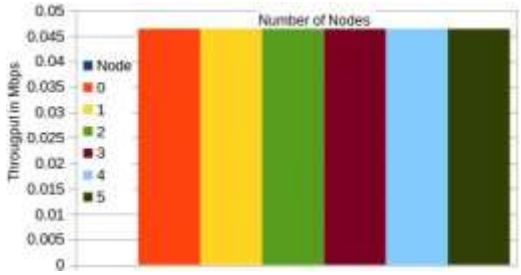


Figure 3. Throughput in normal wimax operation with 5 SS

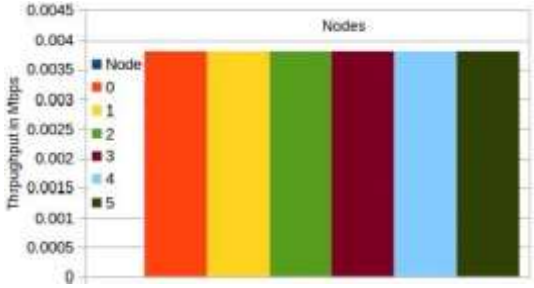


Figure 4 Throughput in Flooded wimax operation with 5 SS

Whereas figure 4 shows the flooded scenerio exploited by node 1,2,4 on wimax. Obtained results shows that the throughput has been decreses utp 10 mbps due to denial of service attack on WiMax BS nodes.

## V. Conclusion

In this article the impact of flooding attack has been analyzed under WIMax network. For beetr approximation we have set the attacking scenario in NS-3 as mentioned in proposed algorithm. Obtained results shows that the DoS Global internet is increasingly pervasive; and wireless networks are a future communication platform to access internet freely and with low cost. WiMax is future network to access the remote services with high speed. Due this reason security is the major concern for better shielding of communication from suspicious attack. DoS, DDoS and flooding are the major and simple deployable weapon to jam the network. In this article we have surveyed the WiMax network and its related current research domain. This article contains all the beneficial information about WiMax technology.

## References

[1]. Farid Benbadis, Damien Lavaux and Laurent San "Overview and Optimization of Flooding Techniques in OLSR", IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011.

[2]. SalehYousefi ,Mojtaba Mazoochi and Saeed Bashirzadeh "Architecture for Large Scale Deployment of WiMAX Networks", IEEE, International Conference on Communications and Mobile Computing, 2009.

[3]. Ayesha Altaf, Rabia Sirhindi and Attiq Ahmed "A Novel Approach against DoS Attacks in WiMAX Authentication using Visual Cryptography", IEEE, The Second International Conference on Emerging Security Information, Systems and Technologies, 2008.

[4]. IEEE Std. 802.16-2004. Copyright IEEE 2004.

[5]. IEEE Std. 802.16e/D12,"IEEE Standard for Local and Metropolitan Area Networks, part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE Press, 2005.

[6]. Kaveh Pahlavan, Prashant Krishnamurthy, " Principles of Wireless Networks: A unified Approach", Pearson Education, Prentice Hall PTR, 2002.

[7]. Anmin Fu, Yuqing Zhang, Zhenchao Zhu, Qi Jing and Jingyu Feng "An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network", Elsevier, computers & security 31 (2012) 741e749.

[8]. Haidar Safa and Farah Abu Shahla "A Policy-Based Trust-Aware Adaptive Monitoring Scheme to enhance WiMax QoS", Elsevier, Computer Networks 55 (2011) 2465–2480, 2011.

[9]. Std 802.16-2004 standard for local and metropolitan area networks part 16: Air interface for fixed broadband wireless access systems. Technical report, 2004.

[10]. IEEE Std 802.16e-2005 standard for local and metropolitan area networks part 16: Air interface for fixed and mobile broadband wireless access systems amendment 2: Physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1. Technical report, 2005.

[11]. IEEE Std 802.16-2009 standard for local and metropolitan area networks part 16: Air interface for fixed and mobile broadband wireless access systems, Revision of IEEE Std 802.16-2004 Technical report, 2009.

[12]. Constantinos Kolias, Georgios Kambourakis and Stefanos Gritzalis "Attacks and Countermeasures on 802.16: Analysis and Assessment", IEEE, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1, FIRST QUARTER 2013.

[13]. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Available at: http://standards.ieee.org/getieee802/download/802.11n-2009.pdf

[14]. Data-Over-Cable Service Interface Specifications, Baseline Privacy Plus Interface Specification. Available at: http://www.cablelabs.com/specifications/CM-SP-BPI+-C01-081104.pdf

[15]. 802.16-2001, I.S. IEEE Standard for Local and Metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. Availiable at: http://standards.ieee.org/ getieee802/download/802.16-2001.pdf.
[16]. 802.16-2004, I.S. IEEE Standard for Local and Metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. Availiable at: http://standards.ieee.org/getieee802/download/802.16-2004.pdf.
[17]. 802.16e-2005, I.S. IEEE Standard for Local and Metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. Availiable at: http://standards.ieee.org/getieee802/download/802.16e-2005.pdf.
[18]. 802.16j-2009, I.S. IEEE Standard for Local and Metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems. Available at: http://standards.ieee.org/getieee802/download/802.16j-2009.pdf
[19]. 802.16m-2011, I.S. IEEE Standard for Local and Metropolitan area net-works Part 16: Air Interface for Fixed Broadband Wireless Access Sys-tems. Available at: http://standards.ieee.org/findstds/standard/802.16m-2011.html.
[20]. D. Levine, G. Kessler, Denial of service attacks, in: Computer Security Handbook, fourth ed., John Wiley & Sons, 2002 (Chapter 11).
[21]. Zhang Shengli, Liew S C, Lam P P. Hot topic: Physical layer network coding. In: Proceedings of the Annual International Conference on Mobile Computing and Net-working (Mobi Com). Los Angeles, CA, USA, 2006: 358-365.
[22]. Katti S, Gollakota S, Katabi D. Embracing wireless interference: Analog network coding. In: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (Sig Comm). Kyoto, Japan, 2007: 397-408.
[23]. Charles D, Jain K, Lauter K. Signatures for network coding. Int. J. Inf. Coding Theory, 2009, 1(1): 3-14.
[24]. Dong Jing, Curtmola R, Nita-Rotaru C. Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks. In: Proceedings of the ACM Conference on Wireless Network Security (WiSec). Zurich, Switzerland, 2009: 111-122.
[25]. H. Du, J. Liu, J. Liang, Downlink scheduling for multimedia multicast/broadcast over mobile wimax: connection-oriented multistate adaptation, IEEE Wireless Communications (2009) 72–79.
[26]. Patrick P.C. Lee, Tian Bu and Thomas Woo "On the detection of signaling DoS attacks on 3G/WiMax wireless networks" , Elsevier, Computer Networks 53 (2009) pp. 2601–2616, 2009.
[27]. UMTS, Release 5. 3G Partnership Project.
[28]. CDMA Development Group. http://www.cdg.org
[29]. Christoforos Ntantogian, Christos Xenakis and Ioannis Stavrakakis "A generic mechanism for efficient authentication in B3G networks", Elsevier, computers & security 29 (2010) 460–475.
[30]. X. Zhao, Y. Dong, H.-T. Zhao, Z. Hui, J. Li, C. Sheng, A real-time congestion control mechanism for multimedia transmission over 3G wireless networks, in: Proceedings of the 12th IEEE Int'l Conf. on Communication Technology, 2010, pp. 1236–1239.
[31]. W. Chen, J. Yu, F. Pan, Optimal priority-based call admission control scheme for QoS provisioning in heterogeneous wireless networks, Journal of Networks 6 (2) (2011) 319–329.
[32]. Zhiwei Li, Di Pu, Weichao Wang and Alex Wyglinski "Forced Collision: Detecting Wormhole Attacks with Physical Layer Network Coding", IEEE, TSINGHUA SCIENCE AND TECHNOLOGY ISSNll10 07- 0 214ll05/09llpp50 5-5 19, Volume 16, Number 5, October 2011.
[33]. Dimitrios Koukopoulos "Instability behaviour of heterogeneous multimedia networks under dynamic adversarial attacks", Elsevier, Mathematical and Computer Modeling 57 (2013) 2671–2684.