A Study on Evaluation of DoS Attacks in WiMAX Networks

K. Saranya,[1] M.A.Dorairangaswamy[2]

[1] PhD Research Scholar, Bharathiar University, Coimbatore.
[2] Professor, Department of Computer Science, ASIET, Kalady.

---***---

Abstract: *Security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment whereas early research effort assumed a friendly and cooperative environment and focused mainly on problems such as wireless channel access and Multi-hop routing. Recent wireless research indicates that the WiMAX presents a larger security problem than conventional wired and wireless networks. Denial of Service (DoS) attacks has become a problem for users of computer systems connected to the Internet. Different mechanisms have been proposed to countermeasure the routing attacks against WiMAX. However, these mechanisms are not suitable for WiMAX resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. In this paper, the different schemes for handling the DoS attacks are investigated and studied.*

Keywords: *WIMAX, Security attacks, DoS, Attack modes.*

1. INTRODUCTION

In a WIMAX, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. A WIMAX is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. In a WIMAX, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. In a mobile ad hoc network, routers act as hosts as well as packet-forwarding routers. The nodes in WIMAX themselves are responsible for dynamically discovering other nodes to communicate. While such networks have potential commercial viability, the main deployment of WIMAXs is still mainly for disaster-relief emergencies and military expeditions in hostile terrains. Such applications involving information-retrieval and data sensitive transactions require some level of cyber security to be provided to users. One of the most common forms of security breaches is the Denial-Of-Service (DoS) attack. A DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function. These attacks are launched against server resources or network bandwidth by preventing authorized users from accessing resources. They pose threats to larger websites such as Amazon and eBay. The effect of these attacks varies from temporarily blocking service availability to permanently distorting information in the network. DoS attacks can target a client computer or a server computer. For example, an attack may target a system by exhausting limited wireless resources such as bandwidth, storage space, battery power, CPU, or system memory. In this paper, we look into various vulnerabilities in WIMAXs, the DoS attack scenarios and methods for detection and prevention of DoS attacks.

2. SECURITY ISSUES AND VULNERABILITIES IN WIMAX NETWORKS

A WIMAX is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. Due to self-organize and rapidly deploy capability, WIMAX can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other security-sensitive applications. WIMAXs are a unique class of wireless multi-hop network comprising of autonomous mobile nodes. This causes the network topology to be dynamically changing, which gives rise to a wide range of characteristics such as transient links, unpredictable resource availability and complex route maintenance. In addition, nodes in WIMAXs have limited battery life, which is expended by packet transmission and reception. Although security threats exist in both wired and wireless networks, the inherent nature of wireless networks such as WiMAX's results in them being more vulnerable to attacks. In the following, we describe how some of these WIMAX features cause the network to be more susceptible to threats.

- Nodes in WIMAXs do not have any central base station to coordinate the transmission and authentication of packets. Thus, the delivery of data packets from source to destination nodes in the network is dependent on the cooperation of the (intermediate) nodes in the network.

- The wireless channel in WIMAXs is a shared broadcast medium, where as in wired scenarios channel can be configured to provide dedicated access to any particular user group. Therefore, nodes in wireless networks are often subject to interference (whether deliberate or not) from neighboring nodes.

- The mobility of the nodes in the network also increases the challenge of node authentication, because nodes can easily venture into and out of the network.

Because WiMAX have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the WiMAX.

2.1 Lack of secure boundaries

The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network. In the wired network, adversaries must get physical access to the network medium, or even pass through several lines of defense such as firewall and gateway before they can perform malicious behavior to the targets. However, in the mobile ad hoc network, there is no need for an adversary to gain the physical access to visit the network: once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks.

The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service.

2.2 Threats from Compromised nodes inside the network

In the previous subsection, we mainly discuss the vulnerability that there is no clear secure boundaries in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This Vulnerability can be viewed as the threats that come from the compromised nodes inside the network. Since mobile nodes are autonomous units that can join or leave the network with freedom, it is hard for the nodes themselves to work out some effective policies to prevent the possible malicious behaviors from all the nodes it communicate with because of the behavioral diversity of different nodes. Furthermore, because of the mobility of the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to different node in the network, thus it is very difficult to track the malicious behavior performed by a compromised node especially in a large scale ad hoc network. Therefore, threats from compromised nodes inside the network are far more dangerous than the attacks from outside the network, and these attacks are much harder to detect because they come from the compromised nodes, which behave well before they are compromised.

A good example of this kind of threats comes from the potential Byzantine failures encountered in the routing protocol for the mobile ad hoc network. We call it a Byzantine failure when a set of nodes are compromised in such a way that the incorrect and malicious behavior cannot be directly detected because of the cooperation among these compromised nodes when they perform malicious behaviors. The compromised nodes may seemingly behave well; however, they may actually make use of the flaws and inconsistencies in the routing protocol to undetectably destroy the routing fabric of the network, generate and advertise new routing information that contains nonexistent link, provide fake link state information, or even flood other nodes with routing traffic. Because the compromised nodes cannot be easily recognized, their malicious behaviors are prone to be ignored by other nodes. Therefore Byzantine failure is very harmful to the mobile ad hoc network.

2.3 Lack of centralized management facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems. Now let us discuss this problem in a more detailed manner. First of all, the absence of centralized management machinery makes the detection of attacks a very difficult problem because it is not easy to monitor the traffic in a highly dynamic and large scale ad hoc network. It is rather common in the ad hoc network that benign failures, such as path breakages, transmission impairments and packet dropping, happen frequently. Therefore, malicious failures will be more difficult to detect, especially when adversaries change their attack pattern and their attack target in different periods of time. For each of the victims, because it can only observe the failure that occurs in itself, this short-time observation cannot produce a convincing conclusion that the failure is caused by an adversary. However, we can easily find from a system point of view that the adversary has performed such a large amount of misbehaviors that we can safely conclude that all of the failures caused by this adversary should be malicious failure instead of benign failure, though these failures occur in different nodes at different time. From this example we find that lack of centralized management machinery will cause severe problems when we try to detect the attacks in the ad hoc network.

Second, lack of centralized management machinery will impede the trust management for the nodes in the ad hoc network. In mobile ad hoc network, all the nodes are required to cooperate in the network operation, while no security association (SA2) can be assumed for all the network nodes. Thus, it is not practical to perform an a priori classification, and as a result, the usual practice of establishing a line of defense, which distinguishes nodes as trusted and non-trusted, cannot be achieved here in the mobile ad hoc network. Third, some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure.

2.4 DOS ATTACK

Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the WIMAX. A routing table overflow attack and sleep deprivation attack are two other types of the DoS attacks. In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node. The traditional intent and impact of DoS attacks is to prevent or impair the legitimate use of computer or network resources. Regardless of the diligence, effort, and resources spent securing against intrusion, Internet connected systems face a consistent and real threat from DoS attacks because of two fundamental characteristics of the Internet:

- The Internet is comprised of limited and consumable resources.
- Any system can be compromised and attacked if the IP address is recognized.

2.5 Use of Denial of Service

Denial of Service attacks were first used to “have fun”, get some kind of revenge from system operators or make complex attacks possible, such as blind spoofing on services. IRC servers were also often targeted after one got insulted on a channel. At this time networks and Internet uses were “confidential”, and those attacks had very limited impact. With time and as the Internet gets more and more used as a communication channel, hacktivism becomes more and more popular. Geopolitical situations, wars, religious concerns, ecology, any motive is then good to launch attacks on companies, political organization or even national IT infrastructures. A more recent use of Denial of Service is linked to online gaming. Many servers have been victims of such attacks, generated by unhappy gamers who lost lives or their favorite weapon during game. But the very use of Denial of Service today is definitely extortion. More and more enterprises rely on their IT infrastructure. Mail, critical data and even phone are handled by the network. Very few companies can survive without their main communication channel. Furthermore the Internet is also a production tool. Search engines and gambling web sites, as an example rely entirely on their connectivity to the network.

2.6 Permanent Denial of Service attacks

A permanent denial-of-service (PDoS), also known loosely as phlashing is an attack that damages a system so badly that it requires replacement or reinstallation of hardware. Unlike the distributed denial-of-service attack, a PDoS attack exploits security flaws which allow remote administration on the management interfaces of the victim's hardware, such as routers, printers, or other networking hardware. The attacker uses these vulnerabilities to replace a device's firmware with a modified, corrupt, or defective firmware image—a process which when done legitimately is known as flashing. This therefore "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced. The PDoS is a pure hardware targeted attack which can be much faster and requires fewer resources than using a botnet in a DDoS attack. Because of these features, and the potential and high probability of security exploits on Network Enabled Embedded Devices (NEEDs), this technique has come to the attention of numerous hacker communities.

2.7 ATTACK SCENARIOS

The DoS attacks that target resources can be grouped into three broad scenarios. The first attack scenario targets Storage and Processing Resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider. Consider the case where a node continuously sends an executable flooding packet to its neighborhoods’ and to overload the storage space and deplete the memory of that node. This prevents the node from sending or receiving packets from other legitimate nodes. Neighborhood watch and monitoring can prevent the occurrence of such events by gradually excluding such malicious nodes.

The second attack scenario targets energy resources, specifically the battery power of the service provider. Since mobile devices operate by battery power, energy is an important resource in WIMAXs. A malicious node may continuously send a bogus packet to a node with the intention of consuming the victim's battery energy and preventing other nodes from communicating with the node. The use of localized monitoring can help in detecting such nodes and preventing their consequences.

The third attack scenario targets bandwidth. Consider the case where an attacker located between multiple communicating nodes wants to waste the network bandwidth and disrupt connectivity. The malicious node can continuously send packets with bogus source IP addresses of other nodes, thereby overloading the network. This consumes the resources of all neighbors that communicate, overloads the network, and results in performance degradations.

3. RESEARCH ACHIEVEMENTS

S. Zhong, J. Chen and Y.R. Yang[4] specifies that Mobile ad hoc networking has been an active research area for several years. How to stimulate cooperation among selfish mobile nodes, however, is not well addressed yet. In this paper, we propose Sprite, a simple, cheat-proof, credit based system for stimulating cooperation among selfish nodes in WiMAX. The system provides incentive for mobile nodes to cooperate and report actions honestly. Compared with previous approaches, our system does not require any tamperproof hardware at any node. At a high level, the basic scheme of our system can be described as follows. When a node receives a message, the node keeps a receipt of the message. Later, when the node has a fast connection to a Credit Clearance Service (CCS), it reports to the CCS the messages that it has received/forwarded by uploading its receipts. The CCS then determines the charge and credit to each node involved in the transmission of a message, depending on the reported receipts of a message.

Two main issues:

- Since there is no tamper-proof hardware at any node and the charge and credit are based on the reports of the selfish nodes, a selfish node (or even a group of colluding node) may attempt to cheat the system to maximize its expected welfare.

- A node should receive enough credit for forwarding a message for another node, so that it can send its own messages with the received credit, unless the resource of the node itself is extremely low. This is the incentive perspective of the system

S. Marti, T.J. Giuli, K. Lai and M. Baker[5] describes techniques that improves throughput in an Ad Hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. The paper uses a Watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes. Two extensions to the Dynamic Source Routing Algorithm (DSR) to mitigate the effects of routing misbehavior: the watchdog and the pathrater. The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through theses nodes. The DSR is divided into two main functions:

- Route Discovery

- Route Maintenance

We implement the watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node. For the watchdog to work properly, it must know where a packet should be in two hops. The path rater, run by each node in the network, combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. One of the main advantages of this technique is that DSR with the watchdog has the benefit that it can detect misbehavior at the forwarding level and not just the link level.

A possible disadvantage is that there are chances of ambiguous collisions between the nodes and also the limited transmission power of the nodes can be quite limiting factors for this approach

S. Buchegger and J.Y.L Boudec[6] identifies that Mobile ad-hoc networking works properly only if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. The paper proposes a protocol, called CONFIDANT, for making misbehavior unattractive; it is based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. The detailed implementation of CONFIDANT in this paper assumes that the network layer is based on the Dynamic Source Routing (DSR) protocol.

The CONFIDANT protocol works as an extension to a reactive source-routing protocol for mobile ad-hoc networks. CONFIDANT consists of the following components, as shown in Figure 1: The Monitor, the Reputation System, the Path Manager, and the Trust Manager. The components are present in every node. Each node monitors the behavior of its next-hop neighbors. If a suspicious event is detected, the information is given to the reputation system. If the event is significant for the node, it is checked whether it has occurred more often than a predefined threshold, which is high enough to distinguish deliberate malicious behavior from simple coincidences such as collisions.

L. Buttyan and J. Hubaux[1] specifies that in military and rescue applications of WiMAX, all the nodes belong to the same authority; therefore, they are motivated to cooperate in order to support the basic functions of the network. In this paper, they consider the case when each node is its own authority and tries to maximize the benefits it gets from the network. More precisely, we assume that the nodes are not willing to forward packets for the benefit of other nodes. This problem may arise in civilian applications of WiMAX. In order to stimulate the nodes for packet forwarding, we propose a simple mechanism based on a counter in each node.

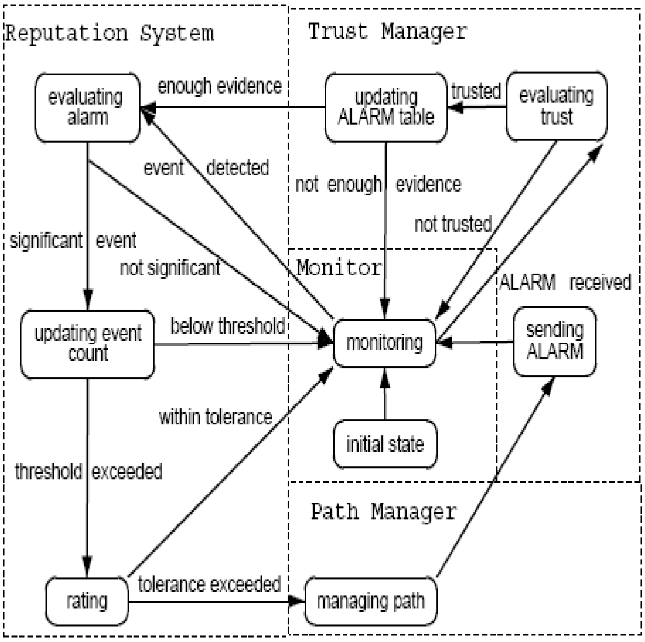

Fig.1. Trust Architecture

However, with the progress of technology, it will soon be possible to deploy WiMAX for civilian applications as well. Examples include networks of cars and provision of communication facilities in remote areas. In these networks, the nodes typically do not belong to a single authority and they do not pursue a common goal. In addition, these networks could be larger and could have a longer lifetime, and they could be completely self-organizing, meaning that the network would run solely by the operation of the end-users. In such networks, there is no good reason to assume that the nodes cooperate. Indeed, the contrary is true: in order to save battery power, the nodes tend to be selfish. An approach to alleviate this problem is based on a trusted and tamper resistant hardware module, called security module, in each node and cryptographic protection of packets. As opposed to the node itself, the security module cannot be tampered with by the user. One can think of the security module as a smart card (similar to the SIM card in GSM phones) or as a tamper resistant security co-processor. Our design ensures that while the user can still modify the behavior of the node (but not the security module), she cannot gain any advantages by doing so. Thus, tampering with nodes is uninteresting, and should happen only rarely. Even though a tamper resistant module is present in the node, still the node may bypass the security module. The implementation of the security module requires additional computational and communication overhead.

V. Gupta, S. Krishnamurthy, and M. Faloutsos[15] analyzes attacks that deny channel access by causing pockets of congestion in WiMAX. This paper focuses on the properties of the medium access control (MAC) protocol which enable such attacks. Several different traffic patterns that an intelligent attacker might generate in order to cause denial of service are investigated. The fundamental cause that DoS at MAC layer can take place is the capture effect and unfairness in media access. End-to-End authentication scheme fails in preventing an attack by two colluding nodes. Traffic patterns generated by an attacking node, its location in the network, availability of other compromised nodes, availability of routing information are key factors in determining the efficacy of the DoS.

This paper assumed that a malicious node would not tamper with the MAC protocol. However, MAC protocol should be made robust so that the effect of tampering is identified and not propagated. Such a scheme may need support in the form of corroboration from the neighbors. Many of the attacks that have been simulated are possible even when end-to-end authentication is enforced for each flow in the network. One of the possible ways of preventing unchecked flows is by the assignment of capabilities to nodes. The assignment of capabilities to node is not addressed in this proposed technique and may be considered as a limitation in this paper.

4. DISCUSSIONS AND SUMMARY

The classification among the proposed techniques in WIMAX for detecting and preventing the DoS attacks can be composed using the parameters given in Table1. Most of the techniques used by the different schemes use a distributed and a cooperated environment. But the most important thing is the reasons the architecture to be configured in distributed manner. As the nature of WIMAX is so open, attacks source can be generated from any nodes within the WIMAX itself or nodes of neighboring networks. Unfortunately, this network lacks in central administration. S. Zhong, J. Chen and Y.R. Yang[4] addresses this issue by providing a Credit Clearance Service(CCS). L. Buttyan and J. Hubaux[1] specifies the use of a security module which provides efficient protection from tampering of nodes by unauthorized sources.

S. Marti, T.J. Giuli, K. Lai and M. Baker[5] addresses the use of a Watchdog and a Pathrater for malicious activity detection but it is not flexible and scalable in all possible cases of malicious activity. S. Buchegger and J.Y.L Boudec[6] proposes a CONFIDANT protocol which includes trust relationships among a number of entities. It follows a distributed and a cooperative architecture. All attacks type of wired networks is possible in WIMAX. WIMAX has also several typical of attacks, which are not available in the traditional wired network, such as selfish attack, black hole attack, sleep deprivation attack and others type of attacks. V.Gupta, S. Krishnamurthy, and M. Faloutsos[15] provides the solution for the above mentioned issues and provides protection from congestion of network as a result of DoS attacks but it also lacks centralization. Table 1 shows the summary of the classification of these WIMAX techniques and methodologies.

5. CONCLUSION

In this study, we try to inspect the security issues in the WiMAX, which may be a main disturbance to the operation of it. Due to the open media nature, the WiMAX are much more prone to all kind of security risks and the most important of those is denial of service. As a result, the security needs in the WiMAX are much higher than those in the traditional wired networks. We discuss some typical and dangerous vulnerability in the WiMAX, most of which are caused by the characteristics of the WiMAX such as constantly changing topology, open media and limited power. These vulnerabilities may lead to serious security attack known as Denial of Service attack. We then discuss some Denial of service characteristics and the various attack scenarios. Finally we introduce the current security solutions for the WiMAX. We start with the discussion on the security criteria which acts as a guidance to the security-related research works in this area. Then we talk about the DoS attack scenario that threatens the current WiMAX. In the end, we discuss several security techniques that can help protect the WiMAX from disruption of services due to Denial of service attacks. During the survey, we also find some points that can be further explored in the future, so that WIMAX can be further improved to handle, detect and prevent the DoS attacks.

REFERENCES

[1] L. Buttyan and J. Hubaux, "Stimulating cooperation in self-organizing WiMAX," ACM/Kluwer Mobile Networks and Applications (MONET), August 2003.

[2] M. Baker, E. Fratkin, D. Guitierrez, T. Li, Y. Liu and V. Vijayaraghavan, "Participation incentives for ad hoc networks," http://www.stanford.edu/~yl31/adhoc (2001).

[3] D. Barreto, Y. Liu, J. Pan and F. Wang, "Reputation-based participation enforcement for adhoc networks," http://www.stanford.edu/~yl314/adhoc (2002).

[4] S. Zhong, J. Chen and Y.R. Yang, "Sprite: A simple, cheat proof, credit-based system for mobile ad-hoc networks," Technical Report 1235, Department of Computer Science, Yale University (2006).

[5].S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating routing misbehavior in WiMAX," In Mobile Computing and Networking, September 2000, page 255–265.

[6] Tran S. Buchegger and J.Y.L Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation Of Noes — Fairness In Distributed Ad-hoc NeTworks," In Proc. Of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, IEEE 2004, page 226–236.

[7] J. Broch, D. Maltz, and D. Johnson, "Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks", In Proc. of IEEE Workshop on Mobile Computing, June 1999.

[8] P. Michiardi and R. Molva, "Making greed work in WiMAX," Technical report, Institut Eur´ecom (2002). [9] A. Kuzmanovic and E.W. Knight, "Low-Rate TCP-Targeted Denial of Service Attacks," SIGCOMM'03, August 25-29, 2003.

[10] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy efficient communication protocol for wireless micro-sensor networks", In Proc. of IEEE Hawaii Int. Conf. on System Sciences, pages 4-7, January 2000.

[11] M.K. Denko, "An Incentive-Based Service Differentiation in WiMAX", In Proc. IEEE International conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2005), pp. 197-204, August 2005, Montreal, Canada.

[12] M.K. Denko, "A Localized Architecture for Detecting Denial of Service (DoS) Attacks in Wireless Ad Hoc Networks", In Proc. IFIP INTELLCOMM'05, Montreal, Canada.

[13] A. Habib, M. H. Hafeeda, and B. Bhargava, "Detecting Service Violation and DoS Attacks", In Proc. of Network and Distributed System Security Symposium (NDSS), 2003.

[14] M. Just, E. Kranakis, and T. Wan, "Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks", In Proc. Of ADHOCNOW'03, Montreal, Canada.

[15] V. Gupta, S. Krishnamurthy, and M. Faloutsos, Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks. In Proc. Of MILCOM, 2002.