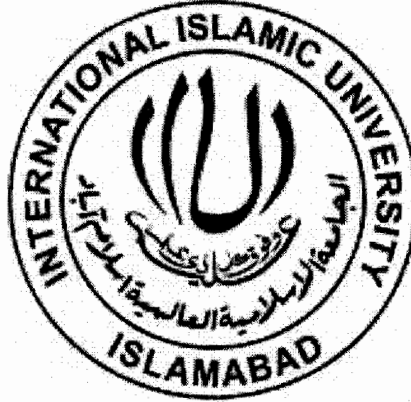


**Secure Mechanism for Handling Targeted Attacks in
Infrastructure based Wireless Mesh Networks**

708153



**THESIS SUBMITTED FOR PARTIAL REQUIREMENT OF MASTER OF
SCINECES IN COMPUTER SCIENCE**

BY

REHAN SHAFI

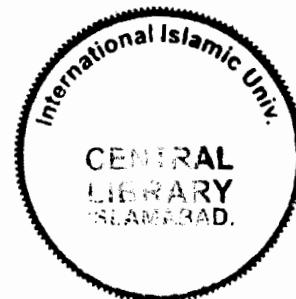
568-FBAS/MSCS/F09

SUPERVISED BY

PROF. DR. MUHAMMAD SHER

**DEPARTMENT OF COMPUTER SCIENCE,
FACULTY OF BASIC AND APPLIED SCIENCES
INTERNATIONAL ISLAMIC UNIVERSITY, ISLAMABAD
PAKISTAN**

2011



Accession No TH8153

M. S. Hill
M.D.

MS
621.38215
RES

wireless communication systems

International Islamic University, Islamabad

Dated: -----

Final approval

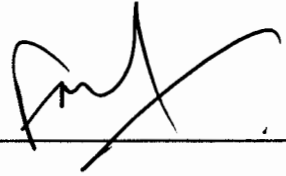
It is certified that we have examined the thesis titled "Secure Mechanism for Handling Targeted Attacks in Infrastructure base Wireless Mesh Networks" submitted by Rehan Shafi, Registration No. 568-FBAS/MSCS/F09 and found as per standard. In our judgment, this research project is sufficient to warrant its acceptance by the International Islamic University, Islamabad for the award of MS Degree in Computer Science.

Committee

External Examiner

Dr. Farrukh Aslam Khan

Associate Professor,
Department of Computer Science,
National University of Computer
and Emerging Sciences (FAST-NUCES),
Islamabad,



Internal Examiner

Dr. Muhammad Zubair


Assistant Professor,
Department of Computer Science and
Software, Engineering, International
Islamic University, Islamabad



Supervisor

Prof. Dr. Muhammad Sher

Chairman and Professor
Department of Computer Science and
Software, Engineering, International
Islamic University, Islamabad


19-8-11

ABSTRACT

Infrastructure based Wireless mesh networks allow heterogeneous types of networks to be connected at a time through wireless mesh routers. Since the nodes of every network have different processing power, bandwidth, amount of energy etc. so this situation can lead to targeted attacks. An Internet connected node can easily generate flood over a node of sensor network in order to handle these types of attacks a new secure authentication mechanism has been introduced that works when a potential of attack is detected. Furthermore the secure mechanism has been proposed that authorizes the nodes of the wireless mesh network to demand data according to their capacity by using pull data traffic control mechanism. Initially solution has been applied on mesh routers to discourage targeted attacks and application of solution on an individual node has been investigated that lies in between a node and mesh router.

DECLARATION

I hereby declare that this work, neither as a whole nor as a part has been copied out from any source. It is further declared that I have conducted this research and have accomplished this thesis entirely on the basis of our personal efforts and under the sincere guidance of my supervisor Prof. Dr. Muhammad Sher. If any part of this project is proved to be copied out from any source or found to be reproduction of some other project, I shall stand by the consequences. No portion of the work presented in this dissertation has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

REHAN SHAFI

568-FBAS/MSCS/F09

A Dissertation submitted to the
Department of Computer Science
International Islamic University Islamabad
As a partial fulfillment of requirements for the award of
The degree of
MS in Computer Science

This thesis is dedicated to my father, who taught me that the best kind of knowledge to have is that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time

ACKNOWLEDGEMENTS

All praise to Almighty Allah who has all the names, and who needs no name the most generous, considerate, and compassionate who has blessed mankind with this verdict to think, explore, to learn and discover the hidden secrets of this universe and helped me to broaden the veils of my thought and enabling me to get through the difficulties indulged during this project. Also admiration to our beloved Prophet Muhammad (PBUH) who is always a great source of inspiration of divine devotion and dedication to me.

I would cordially pay my special appreciations and whole heartedly considerations to my reverend supervisors Prof. Dr Muhammad Sher for his endless support, guidance and coordination while conducting this project. I owe him a great respect and honor and I am privileged to work under their supervision. It was their efforts, courage, moral support and endeavoring attitude that helped me to get through any problem or difficulty during each step of this project.

I would also like to pay my gratitude to all my respected teachers making me capable of what I am today due to their guidance and help. Thanking Dr. Muhammad Zubair, Mr. Shahzad Ashraf, for their views which helped me in improving the proposal, also Mr. Bilal Shah and Mr. Mehmood for providing the managerial and administrative support.

Thanking my friends for always being there for me whenever I needed them for their help, generosity and moral support. Special thanks to Mr. Waqas Nasar, Mr. Zia ur Rehman, Mr. Nisar Tiwana, Mr. Aslam Khan, Mr. Muhammad Sarfraz, Mr. Awais Akhtar, Mr. Safdar Raza, Mr. Qamar ul Islam and Mr. Arman Shafi.

I also owe a special thanks and gratitude to Mr. Zeeshan Shafi Khan for supporting me in working on this idea and accompanying me with the material for study which I needed during this research.

Finally my beloved parents and family who deserve the credit more than I could ever express for always being completely supportive to me. They have been a constant

source of advice, love and devotion to me. From moral to financial they have been blessing me with all the support that I needed up till now in my life.

I express my countless appreciation to all the people who have helped me during achieving this MSCS degree and hope to have this honor that they would walk along me through out my life.

REHAN SHAFI

568-FBAS/MSCS/F09

TABLE OF CONTENTS

1. Introduction	1
1.1 WMNs Architecture.....	2
1.1.1 Infrastructure Base WMNs.....	2
1.1.2 Client WMNs.....	3
1.1.3 Hybrid WMNs.....	4
1.2 WMNs Design Factors.....	4
1.3 Characteristics of WMNs.....	6
1.4 Application Scenarios.....	7
1.4.1 Community and Neighborhood Networking.....	7
1.4.2 Broadband Home Networking.....	8
1.4.3 Enterprise Networking.....	8
1.4.4 Metropolitan Area Network.....	9
1.4.5 Building Automation.....	9
1.4.6 Health and Medical System.....	10
1.5 Capacity of WMNs.....	10
1.5.1 Physical Layer.....	10
1.5.2 MAC Layer.....	11
1.5.3 Network Layer.....	12
1.5.4 Transport Layer.....	13
1.5.5 Application layer.....	14
1.6 Network Management.....	14
1.6.1 Mobility Management.....	15
1.6.2 Power Management.....	15
1.6.3 Network Monitoring.....	15
1.7 Security.....	16
1.7.1 DoS Attacks in WMNs.....	16
1.7.2 Distributed DoS attacks.....	18
1.7.3 Selfish backbone devices.....	18
1.7.4 Deprivation attack on a Node.....	19
1.7.5 Effects of DoS attacks.....	19
1.8 Pull Data Mechanism.....	21
1.9 Presence Service.....	22

2. LITERATURE SURVEY	24
2.1 Security Issues in Mesh Networks	24
2.2 Presence Service.....	31
2.3 Pull Data Option.....	33
2.4 WMNs in OmNet++.....	34
3. PROBLEM DEFINITION	36
3.1 Problem Scenarios.....	37
3.1.1 Scenario 1.....	37
3.1.2 Scenario 2.....	38
3.1.3 Scenario 3.....	38
4. SOLUTION AND METHODOLOGY	40
4.1 Presence Subscription Process	40
4.2 Authentication Process.....	42
4.3 Pull Data Options	45
4.3.1 Periodic Pull Data Traffic	46
4.3.2 Pull Data Traffic (Pull Message).....	47
4.3.3 Pull Data Traffic (Multiple Pull).....	47
4.3.4 Pull Data Traffic (Pull at Middle).....	48
4.4 Solution Scenarios.....	49
4.4.1 Wireless Mesh Router Detects a Targeted Attack.....	49
4.4.2 Receiver Detects a Targeted Attack	52
4.4.3 Middle Node of Multi-hop WMN Detects a Targeted Attack	53
4.5 Chapter Summary.....	55
5. IMPLEMENTATION AND RESULTS.....	57
5.1 Authentication Process with Spoofed and Zombie Detect.....	57
5.2 Pull Data Traffic Control (Periodic).....	60
5.3 Pull Data Option Control (Periodic Rule Change).....	62
5.4 Pull Data Option Control (Pull Message)	63
5.5 Pull Data Option Control (Multiple Pull).....	65
5.6 Pull Data Option Control (Pull at Middle).....	66
5.7 Presence Check (Scenario 1).....	68
5.8 Presence Check (Scenario 2).....	70
5.9 Presence Check (Scenario 3).....	72
5.10 Delay in Simple Ticket based Authentication.....	74

5.11	Delay in Image Ticket based Authentication	75
5.12	Delay in the Presence Check.....	76
5.13	Overall Delay Comparison.....	77
5.14	Chapter Summary.....	78
6.	CONCLUSION AND FUTURE WORK.....	79
6.1	Conclusion	79
6.2	Future Work	80
	REFERENCES.....	81

LIST OF FIGURES

Figure 1.1: Infrastructure/Backbone WMNs.....	2
Figure 1.2: Client WMNs.....	3
Figure 1.3: Hybrid WMNs	4
Figure 1.4: Presence Architecture	22
Figure 3.1: Targeted Attack Scenario	37
Figure 3.2: Distributed Targeted Attack Scenario	38
Figure 3.3: Flooding Attacks on Intermediate Node.....	39
Figure 4.1: Presence Sequence Diagram.....	41
Figure 4.2: Authentication Process	42
Figure 4.3: Pull data option Sequence Diagram.....	46
Figure 4.4: Description of Scenario I.....	50
Figure 4.5: Implementation of Scenario I	51
Figure 4.6: Implementation of Scenario II.....	53
Figure 4.7: Description of Scenario III	54
Figure 4.8: Implementation of Scenario III.....	55
Figure 5.1: Implementation of Spoofed and Zombie Detects	58
Figure 5.2: Authentication Process	59
Figure 5.3: Pull Data Option Periodic.....	61
Figure 5.4: Pull Data Option Periodic rule Change	63
Figure 5.5: Pull Data Option Control (Pull Message).....	64
Figure 5.6: Pull Data Option Control (Multiple Pull)	66
Figure 5.7: Pull Data Option Control (Pull at Middle)	67
Figure 5.8: Pull Data Option Control (Pull at Middle)	69
Figure 5.9: Presence Check (Scenario 1).....	70
Figure 5.10: Presence Check (Scenario 2).....	71

Figure 5.11: Presence Check (Scenario 3)71

Figure 5.12: Delay in Simple Ticket Based Authentication..... 74

Figure 5.13: Delay in Image Ticket based Authentication..... 75

Figure 5.14: Delay in Presence Check76

Figure 5.15: Overall Delay Comparison 77

Chapter 1

1. Introduction

Wireless Mesh Networks (WMNs) have become an emerging technology in the Next Generation Networks (NGN). WMNs are dynamically configured and organized, and the nodes establish the ad-hoc network automatically maintain the connectivity of the mesh networks. There are two types of nodes in the WMNs, mesh clients and mesh routers. WMNs have the additional capabilities and function to maintain the mesh systems other than the traditional routing capabilities of wireless router. The same coverage can be achieved with less transmission power by using the multi-hop communication. Mesh routers contain multiple wireless interfaces that may consist of different network technologies.

Wireless Mesh Networks (WMNs) are gaining lot of researcher's as well as users' attention because of their easy deployment and many other advantages. There are so many applications of WMNs including military networks, enterprise networking [1], metropolitan area networking, broadband home networking, transportation systems, building automation, health and medical sciences, emergency response system [2], efficient support for real time applications [3], security and surveillance systems [4] etc.

Wireless Mesh Routers (WMR) form the backbone of the WMNs [5]. When a new node appears in the network, it broadcasts its address and network capabilities. The close-by WMRs will receive the broadcast and update their list by adding the new node. When any device turns off or disappears, mesh routers will update their list accordingly. Due to this

continuous adjustment, mesh routers create fault tolerant and robust networks. We can say that there is no problem of single point failure in the whole network.

1.1 WMNs Architecture

Wireless mesh networks can be categorized into three types on the basis of their architecture.

1.1.1 Infrastructure based WMNs

In the infrastructure based WMNs the mesh router provides an infrastructure for the clients which is based on the different type of radio technologies. The mesh routers work as backbone for the clients.

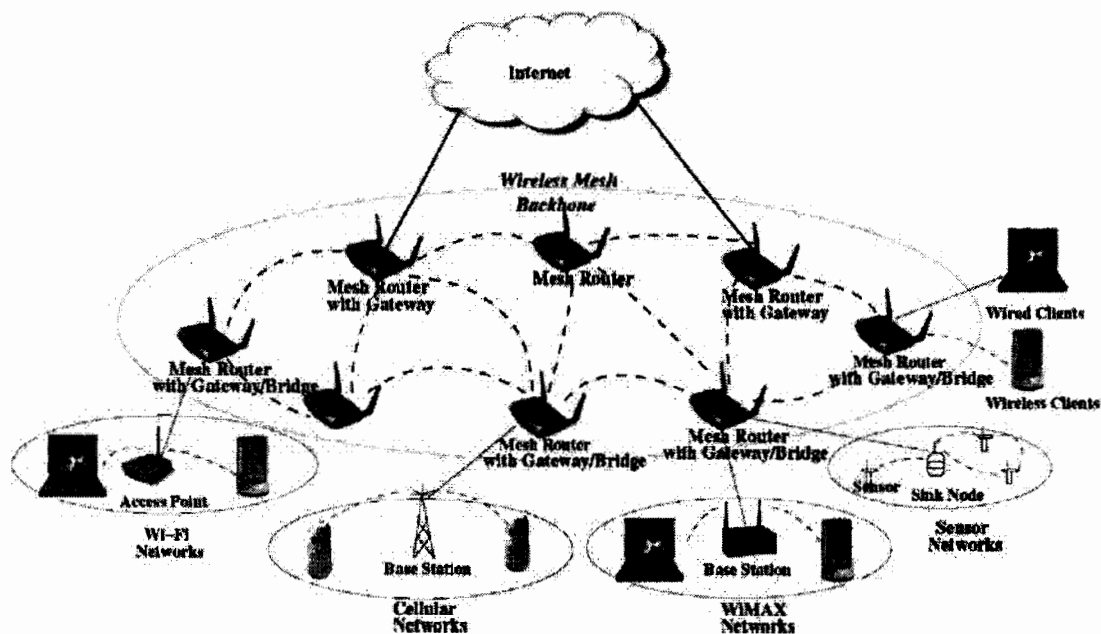


Fig 1.1: Infrastructure/Backbone WMNs

The main characteristic of the mesh routers are that they configure and organize themselves automatically. By the use of gateway/bridge the mesh routers can connect to the internet and it can be integrated with traditional wireless network. If a client has Ethernet interface then it can connect and communicate to the wireless mesh network directly by using the Ethernet link. If the clients have different radio technologies then they have to contact with their base station which have the Ethernet connection to mesh routers [1].

1.1.2 Client WMNs

In client meshing the client devices have peer-to-peer connection with each other. The network consists of client nodes those are responsible to perform self-configuration, routing functionality as well as providing the applications to the end users. The mesh router is not required for client meshing and all the clients must have the same type of radio technologies. We can say that the client WMNs are similar to simple ad-hoc network. The requirements of the end users increased as compared with the infrastructure base WMNs because of some extra functionality like routing and self-configuration [1].

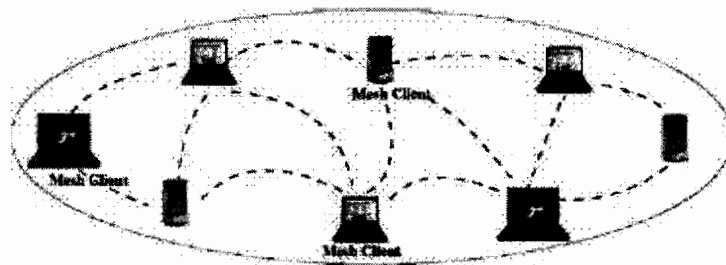


Fig 1.2: Client WMNs

1.1.3 Hybrid WMNs

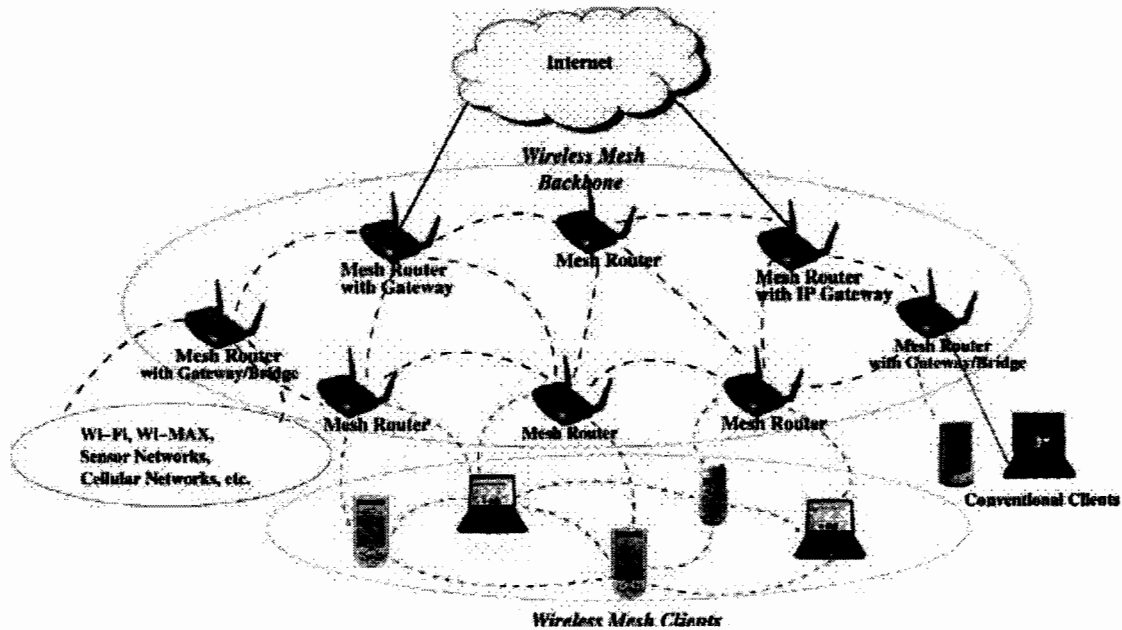


Fig 1.3: Hybrid WMNs

It is the combination of client based and infrastructure based WMNs. Mesh clients can directly communicate with other clients as well as they can connect to the network by using the mesh routers. While by using the gateways of the infrastructure the different type of networks like sensor network, WiFi, cellular etc. can be connected to the mesh routers [1].

1.2 WMNs Design Factors

These are the main factors on which the performance of the WMNs depends [1].

Radio Technologies: The flexibility and capacity of the WMNs are very crucial. To enhance the performance of the WMNs different types of advanced radio technologies are used such as self-configuring radios, software base radios and the frequency agile radios.

Mesh Connectivity: The main advantage of the WMNs is mesh connectivity. For the better mesh connectivity the network must be self-configurable and optimized algorithms are required to control the topology.

Scalability: One of the major requirements of the WMNs is scalability. If the network is not scalable then the performance of the network significantly decreases as the size of network increases. For better performance all the protocols from data link layer to application layer must be scalable.

Broadband and QoS: Most of the WMNs systems use the broadband services which require heterogeneous type of Quality of Service (QoS) requirements as compared with the typical ad-hoc networks. The performance of the WMNs is not only dependent on the end-to-end delay and fair allocation of resources. Some other factors such as aggregate throughput, ratio of the packets lost and per node throughput must be considered to enhance the QoS.

Security: There are number of security schemes for the ad-hoc networks which can be implemented on the WMNs but most of the schemes for ad-hoc networks are not too much mature for the practical implementation on the WMNs. The solutions of the typical ad-hoc networks are not much effective for the WMNs due to the internal architecture differences. That's why some optimized security schemes are required.

Ease of Use: The network should be self-configurable and autonomous as maximum as possible and design the protocol which ensure this property. There should be develop some network managements system for the better performance measurement, manage the network operations and configure the different properties and parameters of the WMNs. By combining the optimized protocols and network management system enable the rapid and secure deployment of the WMNs.

1.3 Characteristics of WMNs

- WMNs have the capability of self-configuration and self-organization and also support the ad-hoc networking.
- Infrastructure based WMNs provide the backbone of the mesh routers which support the multi-hop wireless networking.
- Mesh routers perform the functionality of routing, configuration and it also have the minimal mobility, that's why the load on the mesh clients and end user will decreases.
- WMNs are based on the wireless infrastructure that's why it provides the end user mobility easily.
- Mesh routers can connect different types of wireless and wired networks
- Mesh routers and mesh clients consumes different amount of power.
- WMNs are not separate or stand-alone system and it must well-matched with other types of the wireless networks.

1.4 Application Scenarios

Wireless Mesh Networks have variety of application domains. It covers the limitations which are present in the other wireless networks like, Wireless Sensor networks, Wireless Metropolitan Area networks, Wireless Cellular Networks and other type of Wireless Networks due to its architecture.

1.4.1 Community and Neighborhood Networking

In Community and Neighborhood networking the connection with the internet is established by using a cable or DSL and the client wireless nodes are connected with the DSL or cable modem. There are some drawbacks and limitations in this technique

- The data is shared by using the internet in the community and neighborhood networking which obviously reduces the utilization of the network resources.
- Only some area between the houses and buildings are covered with the wireless services.
- The cost of the network services increases due to the wireless services are configured on the individual basis.
- There are usually no alternative paths available for one home, so it has to communicate by using the single path with the internet and other neighboring networks

Wireless Mesh Networks overcome the most of these issues due to the flexible architecture of the mesh connectivity

1.4.2 Broadband Home Networking

In the home networking the major issue is the location of the access point. If the access point is located without the inspection of the site then there are several areas where no network converge is available. The multiple access points are also not feasible due the cost of the Ethernet cable which has the direct connection with the backhaul router or hub. Also if the user of one access point want to communicate with the user of other access point then always they communicate by using hub which is obviously most resource consuming and not efficient. Wireless Mesh Networks overcomes all these limitations for the home network users. To overcome these drawbacks in the Wireless Mesh Networks replace the access points with the wireless mesh routers. The communication will be faster and fault tolerant due the flexible architecture and extra capabilities of the mesh routers. The dead zones are cover by introducing new mesh routers or by changing the position of the mesh routers and the communication between the different nodes will be possible without going back to hub each time.

1.4.3 Enterprise Networking

This could be a small network for a office or a medium size of the network within a building or a large enterprise which is located across multiple buildings in the same area. Current WiFi networks are using for this purpose and the Ethernet cables are used to connect the various access points with router or hub which is the main reason of high cost of the enterprise level networks. Moreover the extra access point only enhance the inner speed of the network but is does not introduce extra capabilities of fault tolerant links, link congestion and other network capabilities. If the access point of the enterprise level

networks are replaced with the mesh routers then it will overcome most of these issues. As various modems are shared by all nodes so it increases the robustness of the link failure, reduces the link congestion and improves the overall performance of the network. Moreover, due to the replacement of access points with mesh routers, Ethernet links can be completely eliminated, which automatically reduces the cost of the network.

1.4.4 Metropolitan Area Network

There are various advantages of mesh-based metropolitan area networks. The transmission rate at the physical layer is more than as compared with other types of networks. The communication does not rely on the backbone. As compared with other wired networks, the wireless mesh-based MAN is a more economical option. The wireless mesh MAN covers a larger physical area as compared with other networks, so it is more scalable.

1.4.5 Building Automation

In buildings, most things like elevators, air conditioners, and other types of accessories are controlled automatically. Previously, these wired networks were used for this purpose, which is very costly and also very difficult for deployment. Currently, Wi-Fi is used for this purpose, which is more effective than wired but still costly due to Ethernet connections with the back hub. If the access points of the Wi-Fi based network are replaced with mesh routers, then it reduces the cost and it will be easier to deploy such a system due to the mesh connectivity of the wireless mesh routers.

1.4.6 Health and Medical System

In medical centers broadband networks are required to communicate data from one room to another. For this purpose high speed broadband network is required because of the heavy medical images transmission. The wired network can only cover small area and it is also not feasible in term of cost. The Wi-Fi base networks cover large area but it is also not the cost effective due to the Ethernet connections. While in the WMNs these issues are resolved. So it is more convenient to use mesh networks in health and medical systems.

1.5 Capacity of WMNs

The wireless mesh networks capacity is depends upon the various factors such as radio technologies, the architecture of network and topology as well as density, number of channels and transmission power of the nodes.

The best transmission power in the multi-hop architecture can be achieved if each node is connected with six neighborhood nodes. In case of Infrastructure based WMNs this result is highly useful.

1.5.1 Physical Layer

There are various high-speed techniques are available to capacity increase of the wireless networks. For WMNs the smart antenna and diverse antenna techniques could be used. The key issue in the WMNs is low cost and to maintain the low cost the directional antenna could be used. This technique reduces the interference between the nodes as a

result of which the capacity of the network will increase. The multiple antenna technique can also be used to enhance the capacity but the initial cost and the level complexity is high. Also for multiple antenna technique an efficient MAC layer protocol is needed.

1.5.2 MAC Layer

These are the major differences between MAC layer protocols of WMNs and the other type of wireless networks. These diversities must be kept in mind to design a MAC protocol for WMNs.

- The WMNs have the multi-hop architecture, while the other type of wireless networks have single hope communication and the routing protocol handles the transfer across multiple nodes which makes MAC and routing separate to each other. While this technique does not works well with WMNs because the multiple nodes can affect data during the transmission.
- The MAC is not centralized in case of WMNs and it handles the multipoint-to-multipoint communication. The MAC protocol has the responsibility that all the nodes must be cooperative during the communication.
- As the WMNs are self-organized system so it is responsibility of MAC protocol to have the information about the topology of the network. It will enhance the collaboration between the adjacent and multi-hop distance. The self-organized system increases the capacity of networks by the reduction of the interference between the nodes.

- Mobility is one of major factor for the MAC performance. In WMNs the network configurations are dynamically changes due to the mobility thus it will effect the performance of the MAC.

The scalability of the WMNs is depends upon the two factors. The first method is to modify the currently available MAC protocols and design new protocol to enhance the throughput when there is only one channel is available for communication. The other way is that each node can transmit data on multiple channels.

1.5.3 Network Layer

Due to the strong collaboration of the WMNs with the internet and the IP is used as network layer protocol for the WMNs as well as in the other wireless networks. However routing mechanism is different in WMNs as compare with other type of cellular and wireless networks. Thus routing protocol is the main focus area of the network layer. As there are many common features between WMNs and other types of wireless networks therefore the same routing protocol can be used for WMNs. But there are some major differences between WMNs and other types of ad-hoc networks like mobility and power constraints. The WMNs have no power constraints but the backbones which consist of the wireless mesh routers have the minimal mobility. But the client nodes require a power efficient routing protocol.

The optimized routing protocol for the WMNs must have the following features.

- Normally the performance of the routing protocol is measured by selecting the minimum hop count path, but most of time this will not accurate. So the performance metrics must be defined carefully when designing a routing protocol.

- The routing protocol must be fault tolerant. If one link fails then the system must be urgently select the alternate path to provide the smooth service.
- Load Balancing is also one of the key factors. If the congestion occurs on the one path the routing protocol must be able to share the load by allocating the alternating paths to the traffic. If Round Trip Time is used as performance metric then the It will balance load in most of the cases.
- Scalability is also a critical factor for the routing protocol of WMNs. Routing protocol must be able to reduce the end to end delay and adopting the path changes.
- There is no mobility and power constraint issue on the mesh routers that's why simple routing protocols can be designed for the mesh routers. However for mesh clients a fully functional protocol is needed.

1.5.4 Transport Layer

There are many transport layer protocols available for the ad-hoc networks. These protocols can be divided into two categories one is the TCP variant and the other are the completely new protocols. TCP variant protocols are the enhancement of the classical TCP protocol. The completely new protocols are not designed on the basis of TCP to overcome the major drawbacks of the TCP.

TCP variant protocols do not works well in the ad-hoc networks environment because it does not make any distinction between the congestion and non-congestion losses. The throughput of the network is quickly falls if non-congestion losses arise. Link failure is also one of the main drawbacks of the TCP variant protocols. In backbone of WMNs link

failure is not occurs frequently because there is no single point of failure in infrastructure. However link failure can be occurred in the mesh clients. As the mesh routers are connected with the mesh client as ad-hoc network that's why path changes are very frequent that's why TCP based protocols does not work well in this scenario.

Ad-hoc Transport Protocol ATP is specially designed for ad-hoc networks however its not best compatible with WMNs.

1.5.5 Application layer

From the applications we can estimate the requirement of the WMNs. Also we have to determine in which applications WMNs can be used what are new applications that could be developed on the basis of WMNs.

Some of the major applications of the WMNs are listed below

- WMNs have many advantages over the modems and DSL to access the internet like the easy installment, low cost and enhancement in the speed.
- WMNs can be used for the distributed sharing of the information as well as its storage. The application users can communicate with each other by using the WMNs
- By using the WMNs we can share information across different types of wireless networks e.g. Wi-Fi, Sensor.

1.6 Network Management

The smooth working of the WMNs is depends upon the many key factors.

1.6.1 Mobility Management

The call delivery and registration of the new calls are depends upon the location management while the data flow service and new connection establishment is depends upon the handoff management. The mobility management techniques which are developed for wireless or other type of ad-hoc networks can be applied to the WMNs. However the centralized approach does not give best results in WMNs due to its distributed architecture. The distributed techniques give better performance in WMNs. The performance of the MAC and routing protocols can be increased by implementing the location management.

1.6.2 Power Management

The power management is not crucial for the mesh routers because normally there is no issue of the power for them. The performance of MAC layer protocols can be decrease due the hidden nodes. MAC protocols are strongly connected to the techniques used for the power management. The performance also based on the connectivity of the networks that's why the power management is also important for the routing protocols.

As compared with mesh backbone routers, the mesh clients required the protocol which must be efficient in terms of power constraints. Like in case of sensor network power is a major issue so the MAC and routing layer protocols must be power efficient.

1.6.3 Network Monitoring

The WMNs does not have static topology, it can be change dynamically due to the wireless mesh clients. Also in case of the link failure or any wireless mesh router failure

the network topology will be change. That's why the network monitoring is very import for WMNs. There is few network management protocols are designed for the ad-hoc networks. These protocols can be used for WMNs with some enhancements. The data processing algorithm must be efficient to detect the abnormal behavior of the mesh network.

1.7 Security

There are two major types of attacks in the broadband networks, one is passive attack and the second one is the active attack. In passive attack the attacker only view and analyze the traffic and does not modify or change the information. In these attacks the transmission of the data is not normally interrupted. The second kind of attack is more severe than the passive attacks, because in active attacks the attacker can modify the information. It is hard to detect a passive attack because it does not block the actual flow of the traffic. An active attack or a denial of service DoS attack can be launched by using the information gather through the passive attacks. It is easy to make a passive attack on the WMN as compared with other wireless networks due to its multi-hop architecture. The WMN is also more susceptible to the active attack due its multi-hop and ad-hoc architecture.

1.7.1 DoS Attacks in WMNs

DoS attack is the more severe type of attack. In DoS attacks the communication of the network or of the certain node can be blocked. If a request is sent and there is no response

in the specified time then it is the possibility that the DoS attack has been launched. DoS attack can be launched on the different layers of protocol stack.

Physical Layer: At physical layer the WMN use the 2.4 GHz of frequency. The attack on the physical layer can be launched by using a signal jamming device or introducing the interference of the huge noise to disturb the actual frequency. However these types are attack are not normally launched because some dedicated devices are required to launch attack also these attacks can be detected by using radio analyzers. In WMN the attacker can launch the attack from anywhere in the network while in 802.11 the attacker must be close to the access point and 806.11 the attacker must be closer to its base station. As the WMN is consists of large geographical area that's why the physical layer attacks are easy to launch as compared with wireless networks.

Data Link Layer: As the WMN is used the common medium for the entire nodes at MAC layer that's why there is a possibility of the collision or the attack by a selfish node. In selfish attack an attacking node enhance its bandwidth, quality of service and throughput at the cost of other node and the other nodes may be deprived from the network resources. The attack detection module is available in WMN that will block or blacklist the selfish node. The other type of DoS attack which can be launched on the link layer in WMN is de-authentication attack.

Network Layer: There are more possibilities to launch DoS attacks on the network layer of the WMN due to its multi-hop architecture. The routing overhead is increasing with

increase in the hop count. DoS attack on this stage can disturb the routing functionality, decrease the performance or misuse the resources of the network. The common attacks which are launched on the network layer are flooding attack, wormhole attack and greyhole attack.

1.7.2 Distributed DoS attacks

Distributed DoS attacks are very difficult to detect that's why it is challenge in the mesh environment. The DDoS can block the activity of the entire network or it can misuse the bandwidth and network resources to interrupt the normal working. Dedicated machines called Zombie are used to create these types of attacks. Zombie is a dedicated program developed by professionals. In WMN the target of the attack will be the mesh router in most of the cases.

1.7.3 Selfish backbone devices

In WMN a selfish mesh router can create the problem by introducing some type of congestion or make it unable for the communication. The attack can be launched on the mesh router by using the sniffer. The sniffer is specialized program which analyze the traffic by launching a passive attack. The mesh routers or APs in case of 802.16 can be reprogrammed and it can use the hardware address and configuration of the legitimate user. In case of 802.11 these attacks can be launched on the base station. By the use of the sniffer the hardware addresses are extracted from the management message. And later on this information can be used for an active attack.

WMN use the probe request to search the networks in range, and the access points respond the request with the probe response message. After that the client chooses the AP with the strongest signals. In this scenario the attacker can send a spoofed flooding attack of the probe request messages which will cause the overhead on to the access point or mesh router. If the number of the probe requests exceed from the specified threshold value then it can cause the denial of service attack on that specified mesh router or access point.

1.7.4 Deprivation attack on a Node

In this type of attack the attacker target the single node or part of the network to deprive it from the use of network resources. The attacker can send spoofed flooding attack on to the specified node due to that the node will not able to receive the legitimate traffic. Normally authentication is used and the node can de-authenticate if that node does not want to use the network resources anymore.

1.7.5 Effects of DoS attacks

The result of the DoS attack depends upon the nature of the attack and it will affect the network differently depending upon the type of attack.

- The attack on a single node is launched to weaken its battery or deprive it from using the network resources. These attacks are categorized as low intensity attacks.

- The high strength attacks are launched on the specified targeted area to make the services unavailable. In case of WMN these attacks can be launched on the mesh routers.
- The highest capacity attacks are launched to bring down the complete network. The distributed flooded attacks are used to launch this type of attacks. These attacks utilize the whole bandwidth of the network or cause overflow of traffic on the gateways.

DoS attacks are categorized as severe type of attack, so some methods must be implement to prevent from them.

- To prevent the jamming and scrambling attack on the physical layer the cognitive radio technique can be implemented. It will work in mesh networks as well other types of wireless broadband networks.
- The encryption algorithms need to make more efficient because the currently used encryption techniques like DES and AES are open to eavesdropping attacks. This attack then further can be converted into DoS attack.
- The intrusion detection system must be implement to block the attacks on network layer especially in WMN.
- There must be some location detection method implemented on the mesh routers or access point to identify the flooding probe request attack from the malicious node.
- Improvement in the routing protocol is also being mandatory, especially for the mesh networks.

1.8 Pull Data Mechanism

The pull data mechanism is useful to prevent the node deprivation attack. In the pull mechanism the traffic is controlled from the server or receiver that's why it minimizes the possibilities of attack. In normal network communication the traffic is generated by the sender and it is forwarded to the server and then to the receiver while if the pull data option is used then the sender will only generates the restricted amount of traffic. It can be implemented on the server as well as on the receiver node.

If the pull data option is applied on the server then the server will guide the sender to generate the traffic. The sender will not be able to generate traffic without the server permission. The server will control the traffic according the applied pull data mechanism. If the pull data option is applied on the receiver then the sender send data to the server but receiver will only receive the specified amount of data. The receiver will send the pull request to the server and server will respond accordingly.

The classic HTTP protocol uses the TCP for the connection oriented application and UDP for the connectionless environment. In both of the cases the sender initiates the whether to use TCP or UDP. The server will respond according to the sender request. For small communication the TCP is not best suitable because of the overhead involved in the establishment of the connection. To overcome these drawbacks the Dual HTTP can be used which the combination of TCP and UDP. Sender will always send the UDP request and server will decide how to respond with the request. If the request is small and then the server reply by using the UDP. If the request will larger and take more time then the server will initiate the TCP connection. So in this case the control is on the server, the

server will take the decision which protocol will be used. By using this technique most of the drawbacks of the TCP an UDP can be covered with better performance.

Pull data option is useful to prevent DoS attacks, targeted attacks, and node deprivation attacks. It will also enhance the bandwidth utilization by blocking the malicious traffic. Different types of pull techniques can be used according to the requirements. The receiver has to communicate with the server to register its preferences or presence service can be used as an alternative.

1.9 Presence Service

To communicate the current status of a user to other users is known as presence service. The status may contain information like the current location of the user, the available devices, preferred means of communication, currently supported applications etc. Presence service contributes to change the current communication paradigm. You have information about a particular person before contacting him /her. The components of the presence service include Personal User Agent or Publisher, Watcher and Presence Server.

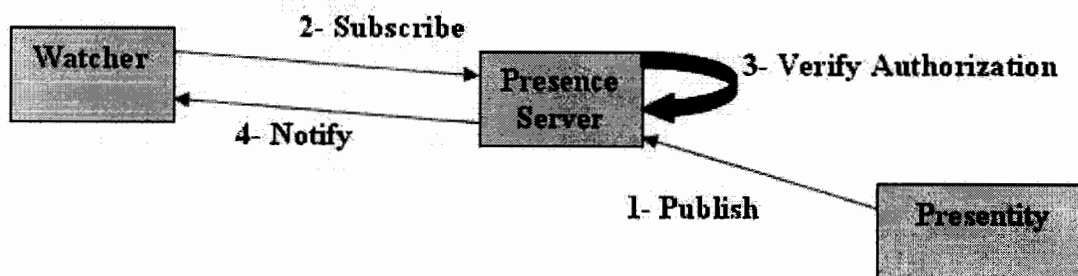


Figure 1.4: Presence Architecture

The publisher provides the information to presence server who stores it and provides it to the subscribed watchers. Subscription can be made to more than one presentity at a time known as subscription to presentity list. Presentity can set different information for different watchers at different levels. Figures below explain the subscription and publication of presence service.

Chapter 2

2 Literature Survey

We categorized our literature survey into four parts. The first part discusses the literature relevant to security issues in mesh and other networks. The second part consists of literature relevant to presence service. In third part we will discuss literature related to the pull data mechanism and the fourth part consists of the literature survey related to the WMNs implementation in the OmNet++.

2.1 Security Issues in Mesh Networks

Vinod et al. in 2007 [6] described a new protocol named QUORUM, which have the capability of calculating the end-to-end delay precisely and provides the mechanism for its integration in the flow setup to fulfill the quality of service requirements. It also provides the functionality of link quality and described how it is useful in the route selection. QUORUM is a reactive approach based protocol which finds the routes on demand. The protocol defines a metric for the intelligent routing that worked on reducing the effect of selfish or misbehaving nodes. Flow decision is based on the source and destination if anyone of them is misbehaving or causing problems then the flow is labeled as bad otherwise it considered as good. The protocol is based on the five major modules. First one is that the each node should have the capability to find the strength of the route estimation to the neighboring one-hop count nodes. The second module is the route discovery on the basis of the topology of the network. The third module calculates the end to end delay of the actual data packets. The fourth module handles the nodes which are

misbehaving in the network. The fifth and final module is for the recovery to maintain the quality of service. There will be a plenty of delay for normal flow because the QUORUM is based on the reactive approach which finds route on demand. All the processing is made when the nodes want to communicate that's why for legitimate users the technique involved reasonable amount of overhead. The simulation results obtained are not compared with any existing QoS routing protocol.

Fabian et al. in 2009 [7] developed an intrusion detection system by focusing on anomaly based detection. Authors performed experiments and conclude that the complete inspection of every packet is not reliable for the mesh devices. They used OpenLIDS which is the set of lightweight intrusion detection and anomaly detection techniques. In this mechanism first of all the packets are captured. The packets captured and the properties of the connection check the hash table to obtain the information about the client data structures and then it increment the counter. The detection process is repeated after every two seconds instead of checking all the packets. And finally the alert generation module is added, the system denies capturing the packets from the system on which the alert is generated and thus the malicious node will automatically be blocked. The experiment shows that even with less hardware capabilities of the mesh devices, it can efficiently detect the intruders. The proposed solution seems to be well designed but it is not scalable in terms of number of connection. If the number of connection increased then the performance of the system will decrease gradually. It means that this solution is only suitable for small and static of WMNs in which number of connection remains in certain limit.

Yeyan et al. in 2009 [8] proposed active cache based security with drop probability. The attack can be detected by the frequency of the number of packets sent and attack is controlled by dropping the packets by using Drop Probability (DP). The proposed solution consists of three major parts. In the first part the authors define the data structure which consists of the cache table of the fixed size to store the information of the traffic flow on the each mesh router. In second module the DoS attacks are detected by the use of the cache table, when packet arrives the signature of the packet is compared with the cache table entry on the basis of it the system take the decision. After the attack is detected then the third module is to send the alert that the attack has been launched and the packets from the malicious node are dropped. The cache table is then updated accordingly. The experiment shows that the DP technique enhances the overall performance of the solution in both normal and attacking flows. The authors used the different optimized drop probability approaches and compare the results against DoS attacks. This scheme can misclassify the legitimate bursty flow of packets as an attack and will label it as attacker. If a legitimate user is labeled as attacker then the traffic generated by that node will be dropped until its status do not changed in the cache.

Xiawang et al. in [9] 2009 designed the model for cross layer based anomaly detection system. The purposes of the model are to increase the anomaly detection rate by comparing the information from different layers in the protocol stack. Reduce false alarm rate of anomaly intrusion detection by comparing the feature of network and data link layer. Detect cross layer attack targeting different layers in the protocol. The cross layer

anomaly detection model consists of four major components data collection at data link and network layer, profile training module, anomaly detection module and alert generation module. Statistical feature from data link and network layer are collected and processed and then make the comparison with single layer based intrusion detection system with feature only from the network layer. The three types of attack probe flooding attack, greyhole attack, and blackhole attack are implemented for the data collection. Authors observed that the cross layer base intrusion detection system gives the better results as compared with the network layer base intrusion detection system. Cross layer based IDS has higher intrusion detection rate in all the three anomaly models as compared with single layer intrusion detection system. The false alarm rate is also less in the Cross layer based intrusion detection system. First of all this solution does not work well in distributed scenario and secondly real time detection is not in the scope of this solution. The overhead involved for implementation of cross layer base intrusion detection model is also ignored.

Khan et.al in 2008 [10] described the challenges for the wireless networks. Due to the difference in the topologies and types of the operations there are the possibilities of different kind of attacks from which the DoS attack is most severe kind of attack. The author concludes that the mesh networks are more susceptible for DoS attacks due to the multi-hop structural design as compared with IEEE standards 802.11 and 801.16. WMNs are more open for attacks due to its structure. WMNs are more unsecured on the network layer based attacks because of its multi-hop architecture. The DDoS can block the activity of the entire network or it can misuse the bandwidth and network resources to

interrupt the normal working. Dedicated machines called *Zombie* are used to create these types of attacks. In WMNs the target of the attack will be the mesh router in most of the cases. In WMNs a selfish mesh router can create the problem by introducing some type of congestion or make it unable for the communication. The attack can be launched on the mesh router by using the sniffer. The attacker can send spoofed flooding attack on to the specified node due to that the node will not able to receive the legitimate traffic to launch the targeted attack on a single node. The authors only discussed the threats, attacks and vulnerabilities of the wireless broadband networks but do not provide any experimental solution or results to prevent from these attacks.

Mehdi et.al in 2009 [11] have discussed the drawbacks of flooding-based technique for Mobility management in Wireless Mesh Networks (WMN) and have developed a DHT-based approach, which according to them, can overcome such limitations and provide an effective solution to the mobility management problem. Flooding technique in the wireless network raises the performance issue like broadcast storm and latency. The DHTs are based on the concept of the mapping object, the key identifier which is in the form of hash function and then distribute these keys all the nodes of the network. The DHTs only run on the backbone mesh router and it will remains transparent to the mesh clients. The changes in the topology are preserved by using the DHT. The advantages of the purposed solution are, it reduces the overhead of the flooding, and network will be more scalable. Authors tested it on the test bed by using both TCP and UDP and it gives better result then the flooding-based mobility technique in both scenarios. The solution will work only for small number of nodes and only for few metrics. All remaining

metrics on which the performance of the WMNs depends are totally ignored and solution is not implement-able in the real scenario.

Fabio et al. in 2009 [12] proposed a framework for community WMNs to detect the selfish and ambiguous behavior of the mesh routers. Each node is responsible for checking the reliability of all other nodes on the basis of direct observations on the behavior of adjacent nodes and the trust information provided by the other nodes. The architecture of the proposed solution consists of the two parts. The first one is the watchdog which is used to check the node misbehavior and the second one is the trust model on each mesh router which computes the global trust factor for all the other nodes in the network. On the basis of experimental results authors conclude that the proposed architecture has high detection rate even if most of the routers provides the negative trust values. The solution works well to identify the mesh routers with selfish behavior that drop the packets instead of forwarding. The solution is based on the number of assumptions like all the wireless links between any two nodes must be symmetric thus the solution does not work for asymmetric channels. All devices must be connected with each other with wireless medium it does not worked on the wired links. The solution only worked if all the links of the backbone used the same wireless channel, different wireless channels are not supported in the backbone.

TH 8/53

Shafi et al. in 2009 [13] have introduced a three layered architecture for IP Multimedia subsystem (IMS). In these three layers first layer is configured by the sender. Sender specifies rules for itself to protect its identity from misuse. After that an intrusion

detection system is deployed at the IMS core to cope the attack. The intrusion detection and prevention system consists of the number of components. Misuse detection to identify is there any attack or not, the priority table to maintain the priority of all the users, blacklist of the attacker nodes and the set of rules to identify the attack. Third layer is configured by the receiver to set its preferences that at what time what type of data it want to receive from which users. First of all this solution is totally designed for IMS, it has nothing to do with mesh network. Secondly how rules will be designed for intrusion detection system is not discussed in the paper. Whether it will be misuse detection system or anomaly detection system is also ignored in this paper.

Shafi et al. in 2010 [14] proposed a call back authentication mechanism for web to cellular phone SMS communication. In their paper they proposed a ticket based authentication scheme and pull data traffic control mechanism but their solution totally focuses on GSM technology and handling of SMS flood. The architecture of the proposed system consists of the three major parts. First one is SMS client, a program which sends the SMS to mobile from the internet. The second part is Token Server which is responsible for the authentication and forwards the list of authenticated user to the next tier. Third one is the CBA server which provides the service to the authenticated users. They use a ticket based scheme for security. The focus is to secure the GSM network. This paper is purely written for GSM network and attack is based on only SMS traffic. All other types to generate attacks are ignored. Secondly this paper is not focused on targeted attack.

Sharjeel et al. in 2010 [15] proposed a solution to protect the low capacity nodes from the high performance nodes. Low capacity nodes configure set of rules on mesh router. Mesh router matches each incoming request (for a particular node) with the rules specified by that particular node. If the rules contradict with the incoming request, the request is dropped else it is forwarded. Moreover authors emphasize that these rules should be configured on the router near to the attacker. The results showed a good improvement in overall security of mesh network but the authors does not specify that how these rules will be developed. Secondly what mechanism should be used to specify the rules near to the attacker is not mentioned in the paper. Theoretical results are provided just by assuming three rules but a detailed simulation is not part of this paper.

2.2 Presence Service

Jiang et al. in 2005 [16] proposed a three layer for presence service. Layer one provides network services, layer two is responsible for basic services to all users and layer three contains the policies related to personalization service. The authors proposed to add location, line status, role and availability in the presence information. To extend Call Processing Language (CPL) for presence authors defined four top level actions, five operations and a presence switch. The major focus of the authors is on presence service and call control.

Igor in 2005 [17] conducted the detailed analysis of the presence subscription when the underlying access network is UMTS. According to the author periodic subscriptions to presence by a user after a short interval of time utilizes more bandwidth at the air

interface of the UMTS. Author proposed a modified technique to reduce this load from the UMTS air interface.

Florian et al. in 2006 [18] described that instead of subscribing to presence service individually, subscription should be allowed to a Resource List Server (RLS). RLS collects the information and sends it in bundles. It reduced the number of messages thus results in efficient utilization of resources. Author also proposed that instead of providing information to subscriber after every change, the RLS should collect the information and provide it to the watcher only on demand.

Vishal et al. in 2006 [19] presented a survey on security issues in presence and proposed few solutions to solve these security issues. Authors emphasized on authentication of the watcher and presentity, authorization and access control over presence information and the integrity and confidentiality of the presence information. For authentication author proposed asserted identity, cryptographically verified identity and certificate based authentication. For data integrity and confidentiality of the presence information the author proposed the use of private and public key.

Beltern et al. in 2007 [20] presented the fully distributed platform to deploy presence service. They proposed middleware architecture consists of two layers two layers. First layers takes the intelligent decision to process and manage the presence information and the second layer is responsible for sending and receiving messages like subscribe and notify. The major emphasizes of the authors is on the management of the presence

information in order to make it more efficient. RA rules defined by the authors restrict a user to communicate with other user.

Wang et. al. in 2007 [21] presented the idea of PoC session setup using rich presence information. All the group members are invited without knowing the presence information. The server retrieved and compared the presence information and only those users are invited whose presence information matches with the request. It decreased the session setup delay and reduced the presence related SIP signaling traffic.

2.3 Pull Data Option

Michael et. al. [22] in 2000 presented a new model dual-transport HTTP, which use the combination of UDP and TCP to split the traffic on both channels. The authors stated that the classic HTTP protocol uses the TCP for the connection oriented application and UDP for the connectionless environment. In both of the cases the sender initiates the wheatear to use TCP or UDP. The server will respond according to the sender request. For small communication the TCP is not best suitable because of the overhead involved in the establishment of the connection. To overcome these drawbacks the Dual HTTP can be used which the combination of TCP and UDP. Sender will always send the UDP request and server will decide how to respond with the request. If the request is small and then the server reply by using the UDP. If the request will larger and take more time then the server will initiate the TCP connection. So in this case the control is on the server, the server will take the decision which protocol will be used. By using this technique most of the drawbacks of the TCP an UDP can be covered with better performance. The authors

do not give any method to handle the encrypted web based traffic. Also there is the requirement of the extra features in the firewall as well as in NAT devices. The solution is only works well if there is no congestion in the network.

2.4 WMNs in OmNet++

Reberto et. al. [23] worked on the enhancement of the performance for the simulation of the wireless mesh networks in omnet++. The authors presented a simulation model which focused on the allocation of the bandwidth and the control of the delays occurs at nodes that receiving packets, real time and non-real time IP flows. First they have developed a theoretical model which stated the performance of the WMN node and assume result on the basis of there observations. Then they performed the experiment and the experimental results shows that the performance is enhanced and it is very close to the theoretical values by using the UDP sources. However this system does not work well with TCP sources and the performance results are decreased.

Thomas et. al. [24] in 2009 presented a emulation framework with the name of VirtualMesh for the simulation of WMNs in omnet++. VirtualMesh combines the advantages of the real world experiment with the controlled simulation environment. The major work of the system is to redirect the packet from node to the simulation model which is responsible for its behavior in the physical medium. There are three major procedures are defined, first one is the node registration with the model. The second process is the packet sent by an external node to the virtual interface. The third process is the reception of the packet on an external node. This model provides more flexibility and

control in the simulation. However there is delay involved in the redirection of packets and processing on each node.

Chapter 3

3 Problem Definition

Infrastructure based wireless mesh network connects different types of networks with each other by using mesh routers. So on one side of a mesh router an Internet node can be connected and on the other side a sensor node may exist. So for an Internet node there are high processing speed, high bandwidth, and no battery or energy issues but for sensor node energy is a very serious issue and bandwidth is also low. Processing power of a sensor node is also very low as compared to an Internet connected high speed workstation. This situation allows the Internet connected node to launch a targeted attack on a node of sensor network.

Targeted attack can easily be launched by sending enormous number of requests to a particular receiver. For Internet connected node, generating thousands of requests per unit time is not a big issue but for a sensor node receiving and processing those requests is a big problem and it can result in expiring the battery of a sensor node. It can also cause denial of service attack on that particular sensor node.

Currently in wireless mesh networks there exists no mechanism that can handle these targeted attacks. Few intrusion detection and prevention mechanisms exist for wireless mesh networks but they mostly handle the attacks on wireless mesh routers. Handling targeted flooding attacks on a particular node is still an open issue in wireless mesh networks.

If the traffic increases from the capacity of sensor node then it will be unable to handle the request from the legitimate users. So this targeted attack is automatically converted into to DoS attack.

3.1.2 Scenario 2: Distributed Targeted Attacks

Figure 3.2 demonstrate the distributed targeted attack from multiple nodes to a single node. Multiple high capacity nodes connected with different or same mesh routers can generate huge traffic for a single low capacity attacks node. As a result of this traffic the low capacity node may be unable to handle it. It is very hard to detect the distributed targeted attacks. In the figure there are multiple internet nodes with high capacity, bandwidth, power and energy generate bulky traffic on the single sensor node.

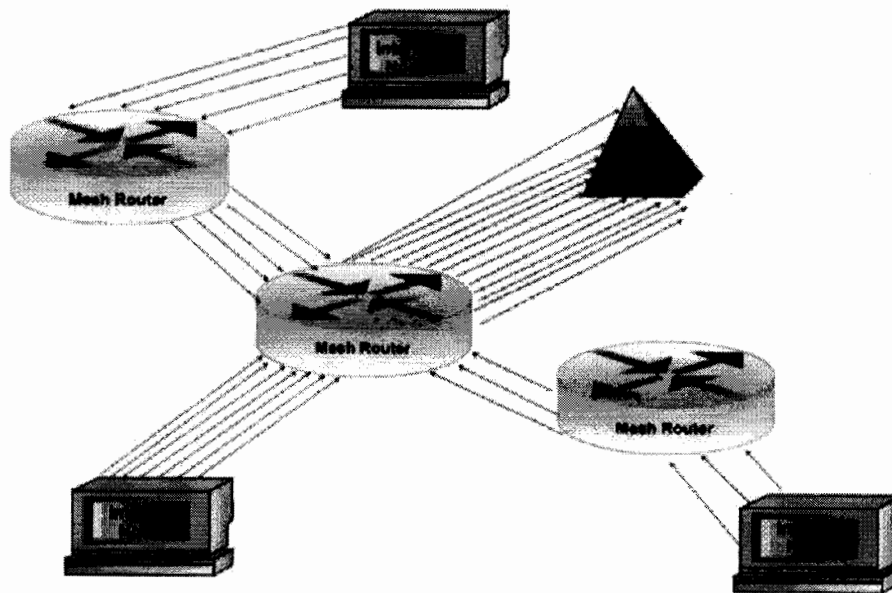


Figure 3.2: Distributed Targeted Attack Scenario

3.1.3 Scenario 3: Flooding Attack on Intermediate Node

Figure 3.3 shows the flooding attack on intermediate node from indirectly connected node. The node which is not connected with mesh router directly may generate a flooding attack to the other node which is directly connected with the mesh router. In this scenario the mesh routers are not involved in the attack that's why some mechanism is also required on every node as well to detect this type of attack. In the diagram the white node is not directly connected with the mesh router. This node forwards its traffic to the red node which is directly connected with the mesh router. Now the intermediate node is not the receiver of traffic it only works as the communication bridge between mesh router and indirectly connected node. Now the indirectly connected node may generates a targeted attack on to the directly connected node. The mesh router is not involved in this scenario so there must be some mechanism to prevent this attack.

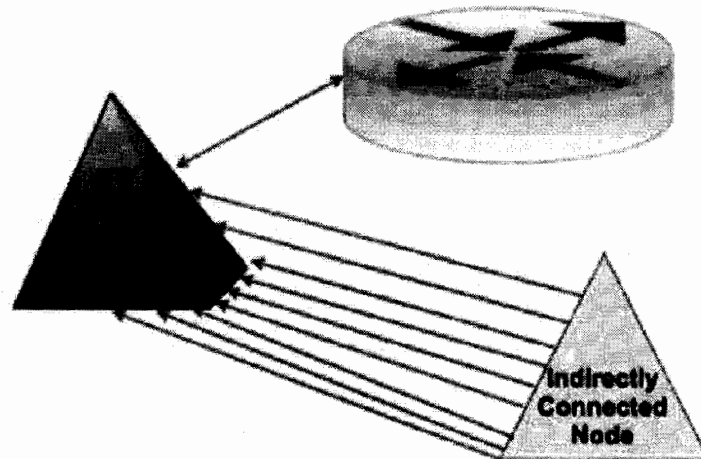


Figure 3.3: Flooding Attacks on Intermediate Node

Chapter 4

4. Solution and Methodology

In this chapter we will discuss the proposed solution and methodology. First of all we will discuss the processes involved in the solution scenarios and after that we will integrate these processes.

4.1 Presence Subscription Process

To communicate the current status of a user to other users is known as presence service. The status may contain information like the current location of the user, the available devices, preferred means of communication, currently supported applications etc.

Presence(Node, Router, Server, State)

begin

var isLive **←** State //if State=0 then node will not receive and message

//if State=1 then node is active

Node.isLive **→** Server //Node publish its Presence information to the //Presence Server

Route **→** Request(Server.Node.isLive) // Mesh Router Send Request

if Server.Node.isLive **exist**

do

//Send Presence information of the requested node to Mesh router

Response(Server.Node.isLive) **→** Router

else

return false

end

Algorithm 4.1: Presence Subscription Process

We have used only one state parameter in the presence. If the value of state is zero then node will be in inactive state and it will not accept any message. And if the state is one it means the node is up and ready to communicate.

Now in the above algorithm the four parameters are used Node which want to share its presence information, Router the mesh router which act as a watcher, Presence Server and the State the presence information of the Node.

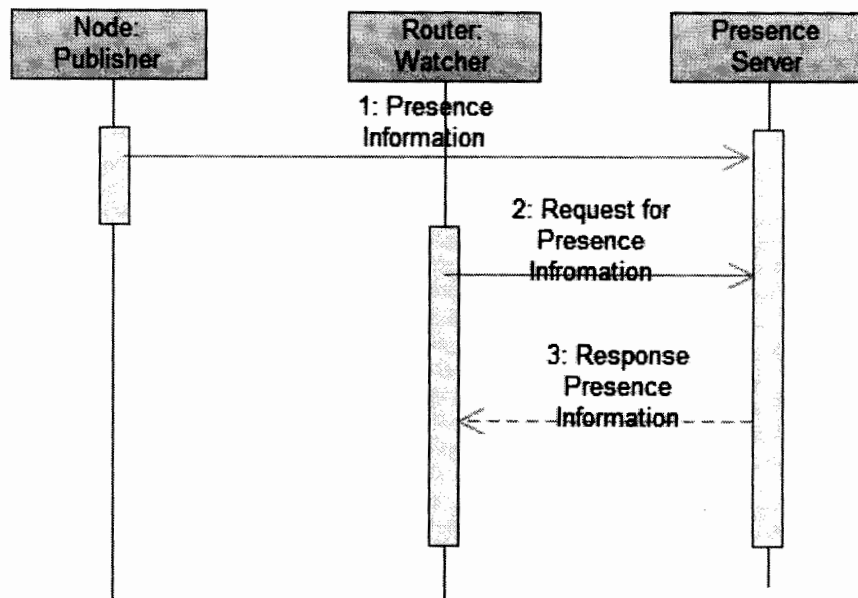


Figure 4.1: Presence Sequence Diagram

The subscriber which wants to share its presence information sends its information to the presence server. The presence server stores the presence information sent by the subscriber. The presence server has the information of all the register nodes. The mesh router sends request for the presence information of a particular user. The presence server

sends the information to the mesh router as a response. The router takes the presence information to make decisions. If presence information matched then message is forward otherwise drop all the messages.

4.2 Authentication Process

Two threshold values are configured on the wireless mesh router. First threshold value is named as normal threshold and the second threshold value is titled as abnormal threshold.

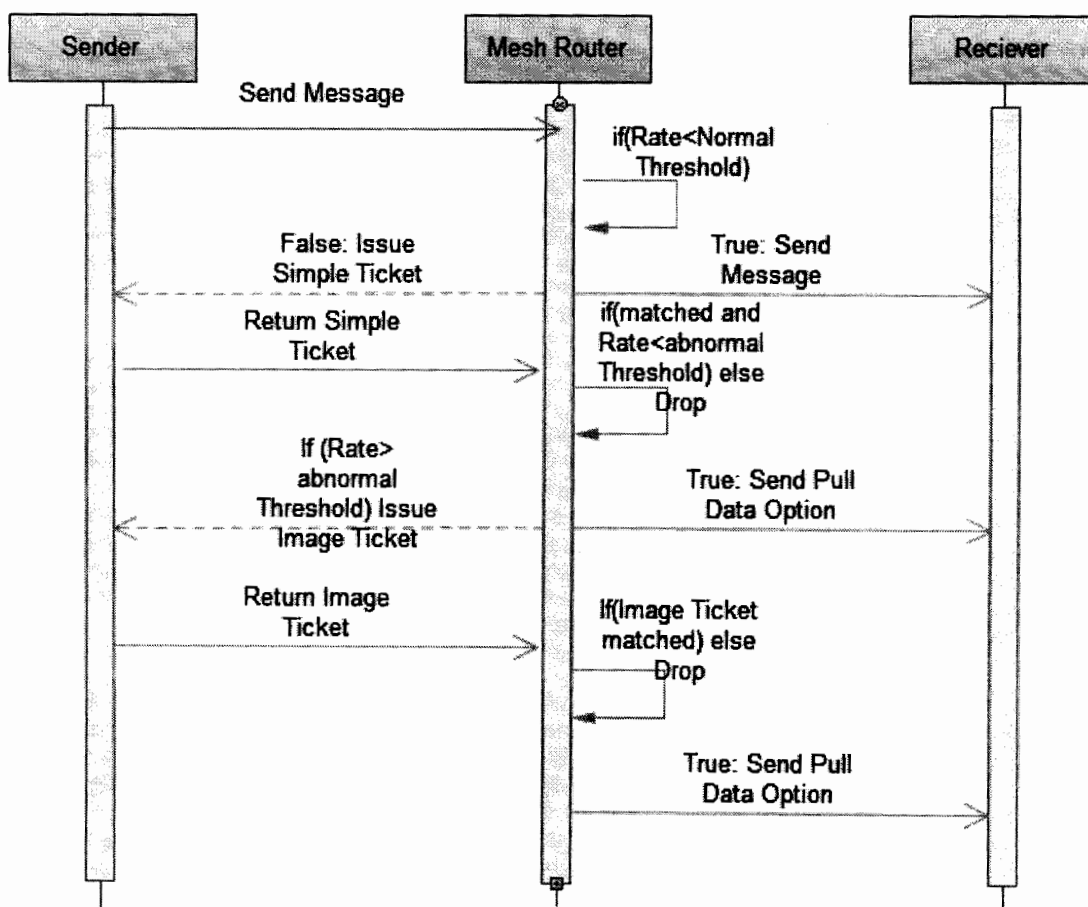


Figure 4.2: Authentication Process

Communication between a particular sender and receiver is analyzed carefully and as soon as it crosses the normal threshold value the wireless mesh router comes into action.

Authentication(Sender, Router, Reciever)

```
begin  
  
var Rate, Normal Threshold, Abnormal Threshold  
  
Sender:Send Packet→Router // Sender sends Packet to router  
  
if Rate < Normal Threshold and Presence matched then  
    Router:Send Packet→Reciever //Router Forward Packet to receiver  
  
    return true  
  
else  
    Router:Simple Ticket→Sender // Issue Simple ticket to sender  
  
end  
  
Sender:Simple Ticket-->Router // Sender Return the Simple ticket  
  
if Presence matched and Simple Ticket matched then  
    if Rate<Abnormal Threshold then  
        Router:Send Pull Data Option→Reciever //Send Pull data option to receiver  
  
        else  
            Router:Image Ticket→ Sender // Issue image ticket to sender  
  
        else  
            Drop Packet  
            return false  
  
        end  
  
        Sender:Image Ticket→Router // Sender Return the Image ticket  
  
        if Presence matched and Image Ticket matched then  
            Router:Send Pull Data Option→Reciever //Send Pull data option to reciever  
  
            else  
                Drop Packet  
                return false  
  
            end  
  
        end  
  
end
```

Algorithm 4.2: Authentication Process

It verifies whether the sender is a real user or she is using a spoofed ID. For this purpose the wireless mesh router sends a simple ticket to the sender.

Simple ticket is four bytes packet and the sender is required to submit the same ticket back to wireless mesh router within a specified period of time. If the wireless mesh router receives the same ticket back it shows that the sender is using real ID, she is not a spoofed user. If the received ticket does not match with the one issued or the wireless mesh router does not receive the ticket back until timeout it decides that the sender is using a spoofed ID, it blocks the communication of that particular sender for a temporary period of time and notify the node whose ID is spoofed. Receiver is also notified about this decision. If the received ticket is valid, communication remains in progress until the abnormal threshold arrives. As soon as sender's data touches the abnormal threshold the wireless mesh router verifies whether the sender is a legitimate user or a zombie (compromised machine) node. If it is a zombie node then it can submit the previously issued ticket back to wireless mesh router easily. So issuing a simple ticket can detect a spoofed user but can not detect the zombie machine. So when the traffic rate touches the abnormal threshold the wireless mesh router launches another mechanism to detect the zombie machine. In that mechanism wireless mesh router sends an image ticket (image with printed text) to the sender. Since till now there exists no such software which can read text from an image 100% correctly so a zombie machine can not return the printed image text in textual form.

So if the sender is a zombie machine it can not submit the image text back and on timeout or on getting wrong image text the sender is blocked and receiver is notified. If neither the spoofed nor zombie attack is detected then the mesh router consults the presence

server to check the presence information of the receiver. If the incoming request does not match with the presence information, it is again discarded.

4.3 Pull Data Options

If a large amount of traffic is generated for a single node and the node will be unable to handle the packets or in case of targeted attack the router will send the option to use pull data. In pull data the router will not forward the packet to the receiver until the receiver request for the data.

PullData(Receiver, Router)

begin

Router → Receiver : PullData //Router sends the pull data option to receiver

Receiver → Router: Request Packet //Receiver sends request for packet

Router → Receiver: Packet // Router sends the packet to receiver

end

Algorithm 4.3: Pull data option

The above algorithm shows the process of the pull data option. In the first step when the traffic for a particular node exceed from the defined threshold value then router send the pull data option to the receiver so that the receiver will get the data according to its capacity. Also router stops the transferring of the packets until the receiver do not send request for data. When the receiver is ready to receive the packets then it will send the pull data request to the router and wait for the response of the router. The router delivers the packet according the applied pull data technique.

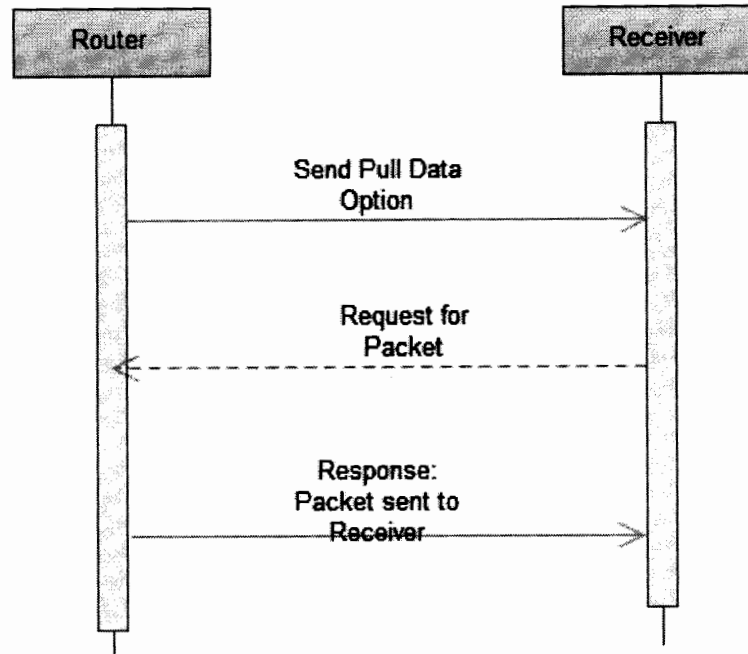


Figure 4.3: Pull data option Sequence Diagram

The response sent by the router is depends upon the mechanism which is used for the pull data. We have applied different pull data mechanism according the preferences of the receiver.

4.3.1 Periodic Pull Data Traffic

In periodic pull data traffic a rule is defined to pull the data from the server. The rule is based upon the time. In the periodic rule the receiver define the amount of data want to receive according to per unit time. In this approach receiver will not send request for message each time. When the pull data option is applied the router will automatically deliver the traffic to receiver according to the specified rule. Periodic rule is actually based upon the preference of the receiver and it varies time to time. For example the receiver defined the rule that when the process start the router will send 2 packets per

second and after the 5 seconds it will double the speed of packet sending. Now when the receiver select the pull data option the router will start sending 2 packets per second as defined in the periodic rule. After the 5 seconds the router will start sending 4 packets per second. This technique is very useful and efficient because the receiver sends the rule one time and then the router will perform operation accordingly so it is efficient in term of time and bandwidth. Also it will minimize the chances of attack or congestion on the receiver node because the packets are delivered according to the receiver preferences.

4.3.2 Pull Data Traffic (Pull Message)

In this technique no periodic rule is defined. It purely works on the ad-hoc or on demand basis. In this approach the receiver will send the pull data packet message to the router and in response the router send exactly one message to the receiver. In this approach each time when the receiver want to receiver a message it will send pull message to the router. The advantage of this technique is that it will not prevent the receiver node from attack and congestion. And the receiver will demand messages according to its capacity. The drawback of this technique is that there is more delay involved. Each time when receiver requires a message it will have to send request to the router which will cause the delay as well as it use the network resources.

4.3.3 Pull Data Traffic (Multiple Pull)

In this approach the router will send multiple messages on one pull request. The receiver will defined the number of messages it required against one pull. So when the receiver will send the pull request to the router then router will send the specified number of

messages to the receiver. For example if the receiver specified that it requires 5 messages against one pull request. Then the router will send 5 messages when it receives a pull request from the receiver. This technique is better than pull message technique because for each message there is no need to send a separate pull request, that's why it is efficient in term of delay and bandwidth resources. The delay of sending pull request for each message will be minimized by sending multiple messages against one pull. Also the bandwidth and other resources used in pull request can also be saved in pull data traffic, multiple pull technique.

4.3.4 Pull Data Traffic (Pull at Middle)

In this approach the receiver will not use the pull option from the beginning. It defined a specified rule or limit to start using the pull data option. From the start the router will forward all the traffic to the receiver. The receiver will make a rule that if the traffic exceed from this limit then it will start using the pull data option. Now when the specified threshold value is exceed the router stop sending the messages to the receiver and inform it to use the pull data option. After it the receiver will shifted to pull data and router will respond according to the pull technique used. This technique will reduce the chances of the denial of service attack because when the traffic exceed from the capacity of the receiver the router stops the message sending and waits for the receiver to demand the message. The receiver will process the all the traffic received then send request to pull more messages. If during the communication the amount of traffic becomes normal and it is under control then the receiver can again shift to the normal flow of the traffic and stop using the pull data option.

4.4. Solution Scenarios

We proposed a new solution to handle the targeted attacks in wireless mesh networks.

Our solution will work in three different scenarios which are described below:

4.4.1 Scenario 1: Wireless Mesh Router Detects a Targeted Attack

In this scenario first of all two threshold values are configured on the wireless mesh router. First threshold value is named as normal threshold and the second threshold value is titled as abnormal threshold. After that presence information of the receiving node is published on presence service and mesh router can be authorized on presence information of the nodes. Communication between a particular sender and receiver is analyzed carefully and as soon as it crosses the normal threshold value the wireless mesh router comes into action. It verifies whether the sender is a real user or she is using a spoofed ID. For this purpose the wireless mesh router sends a simple ticket to the sender. Simple ticket is four bytes packet and the sender is required to submit the same ticket back to wireless mesh router within a specified period of time. If the wireless mesh router receives the same ticket back it shows that the sender is using real ID, she is not a spoofed user. If the received ticket does not match with the one issued or the wireless mesh router does not receive the ticket back until timeout it decides that the sender is using a spoofed ID, it blocks the communication of that particular sender for a temporary period of time and notify the node whose ID is spoofed. Receiver is also notified about this decision. If the received ticket is valid, communication remains in progress until the abnormal threshold arrives. As soon as sender's data touches the abnormal threshold the wireless mesh router verifies whether the sender is a legitimate user or a zombie

(compromised machine) node. If it is a zombie node then it can submit the previously issued ticket back to wireless mesh router easily. So issuing a simple ticket can detect a spoofed user but can not detect the zombie machine. So when the traffic rate touches the abnormal threshold the wireless mesh router launches another mechanism to detect the zombie machine. In that mechanism wireless mesh router sends an image ticket (image with printed text) to the sender. Since till now there exists no such software which can read text from an image 100% correctly so a zombie machine can not return the printed image text in textual form.

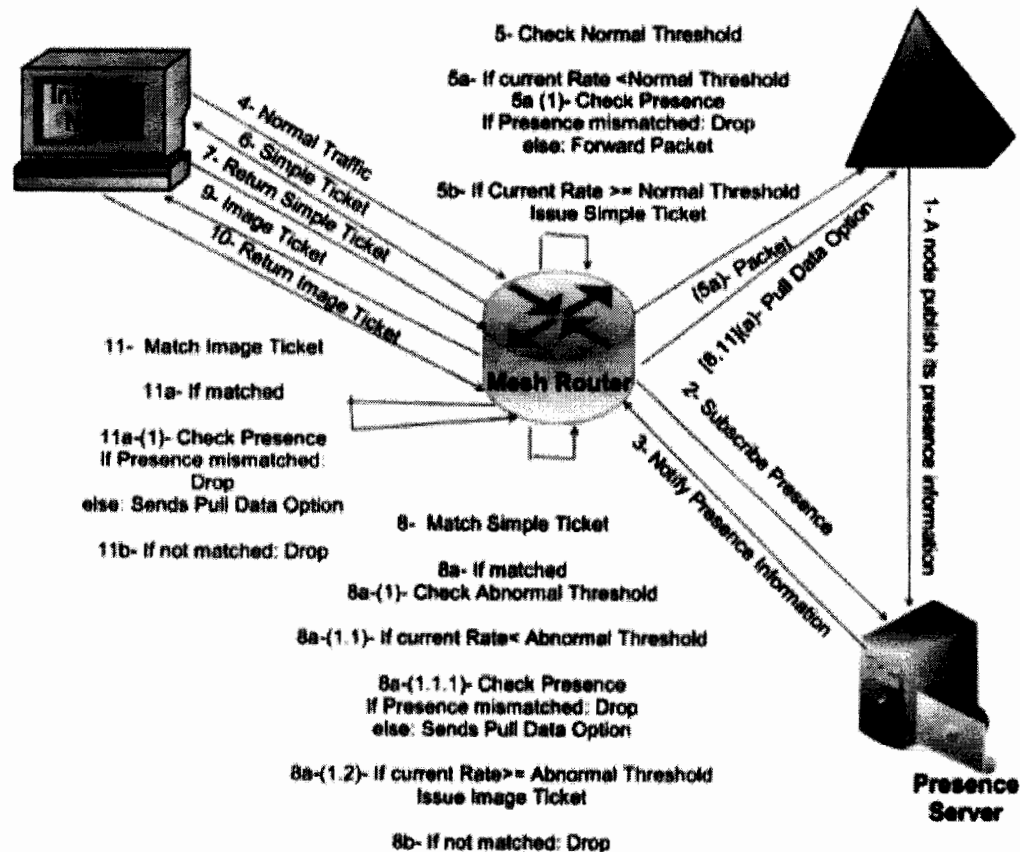


Figure 4.4: Description of Scenario 1

So if the sender is a zombie machine it can not submit the image text back and on timeout or on getting wrong image text the sender is blocked and receiver is notified. If neither the spoofed nor zombie attack is detected then the mesh router consults the presence server to check the presence information of the receiver. If the incoming request does not match with the presence information, it is again discarded. Figure 6 describes the scenario in detail.

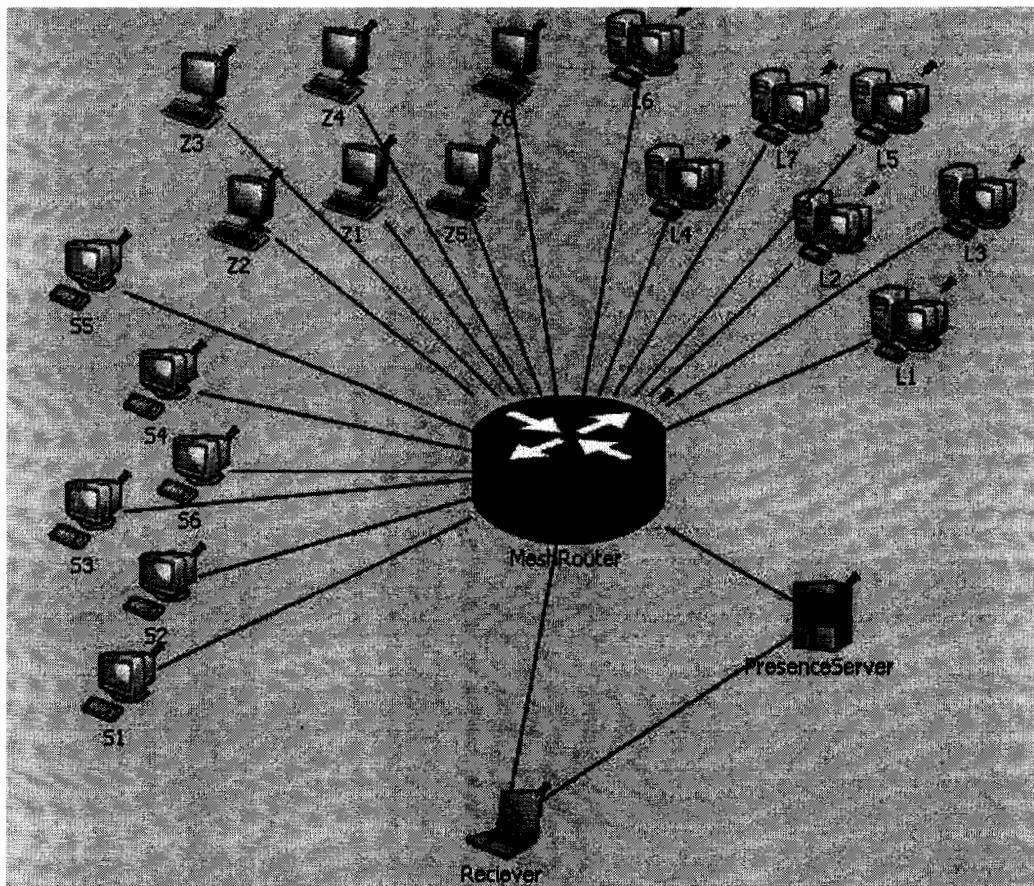


Figure 4.5: Implementation of Scenario I

We have taken a network of 20 nodes to implement the targeted attacks scenario. From L1 to L7 are the seven legitimate nodes, from S1 to S6 are six Spoofed users and from Z1 to Z6 are the six zombie machines which generate the dummy traffic for the receiver. The

receiver published its presence information on the presence server while the mesh router watches the receiver presence information from the presence server.

4.4.2 Scenario II: Receiver Detects a Targeted Attack

If a single sender tries to flood a particular receiver the threshold values can work to stop her. But if this attack is launched through distributed nodes then it is very hard for wireless mesh router to detect it. It may be launched by nodes those are connected with different wireless mesh routers, so in this situation it becomes more difficult to detect it. Therefore to address this situation the receiver upon him attack is launched sends a complaint to directly connected wireless mesh router. That wireless mesh router informs the other wireless mesh router that verifies the senders who are sending requests to that particular receiver. So the wireless mesh routers start ticket base authentication mechanism (See Scenario 1). On the same time directly connected wireless mesh router of the receiver asks the receiver whether she wants to use pull data traffic control mechanism or not. If the receiver selects the pull data traffic control mechanism the wireless mesh router stops sending data to that receiver until the receiver demands it. So in this way targeted attacks are blocked. It is very hard to detect the distributed targeted attacks because the traffic is generated from different path and different routers are involved in the transmission. In case of distributed attacks the receiver will detect the attack and notify the mesh router and it converts it to some pull data techniques. To launch distributed targeted attacks we have defined the topology which contains three mesh routers. The legitimate, spoofed and zombie nodes are directly connected to the

mesh router and mesh router 1. These two mesh router are connected with the mesh router 2 which is directly connected with the receiver.

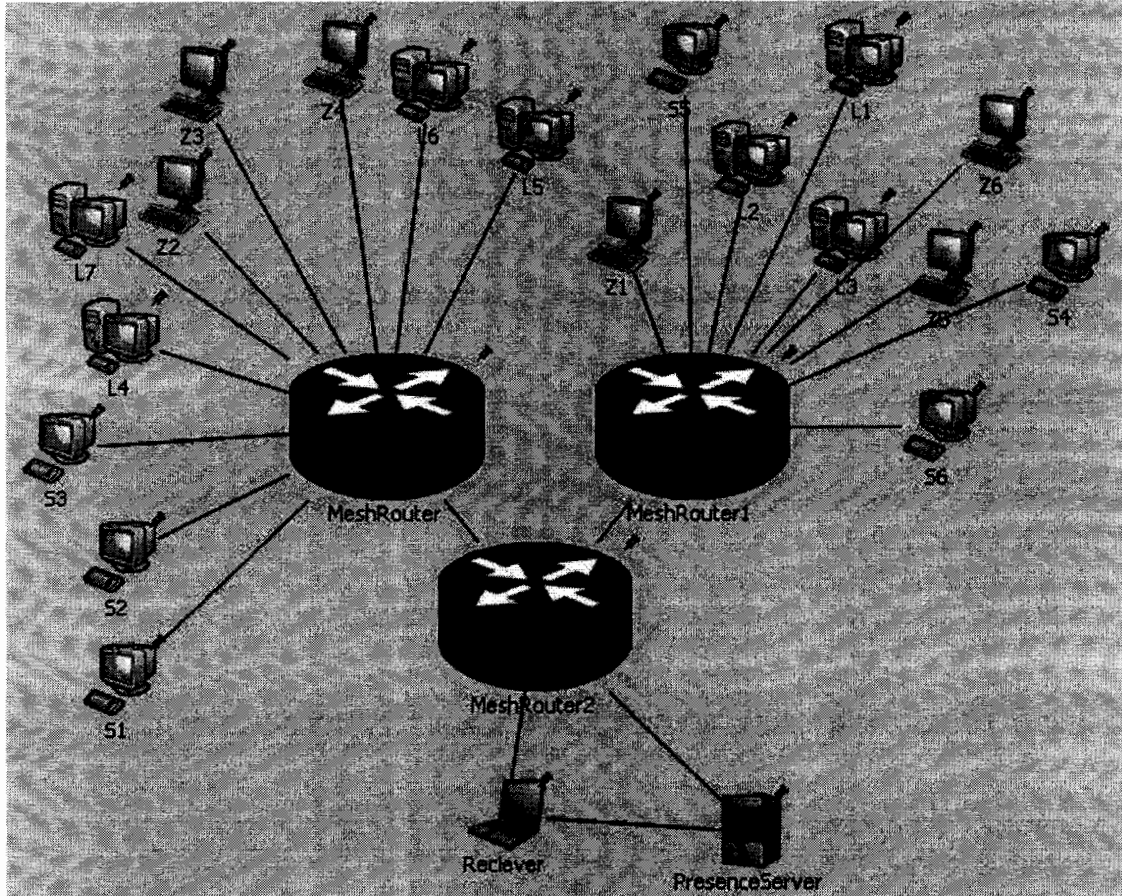


Figure 4.6: Implementation of Scenario 2

4.4.3 Scenario III: Middle Node of Multi-hop Wireless Mesh Network Detects a Targeted Attack

Wireless mesh network may also work in multi-hop mode. It is not necessary that all the nodes should directly connect to wireless mesh router, few nodes can be connected to wireless mesh router through other nodes. So if a node which is two hop away from the wireless mesh router tries to launch a targeted attack on one hop away node (while the

one hop away node is not the receiver, it is only the middle node which is connecting the sender or attacker to the wireless mesh router) then we need a mechanism to detect and prevent this attack.

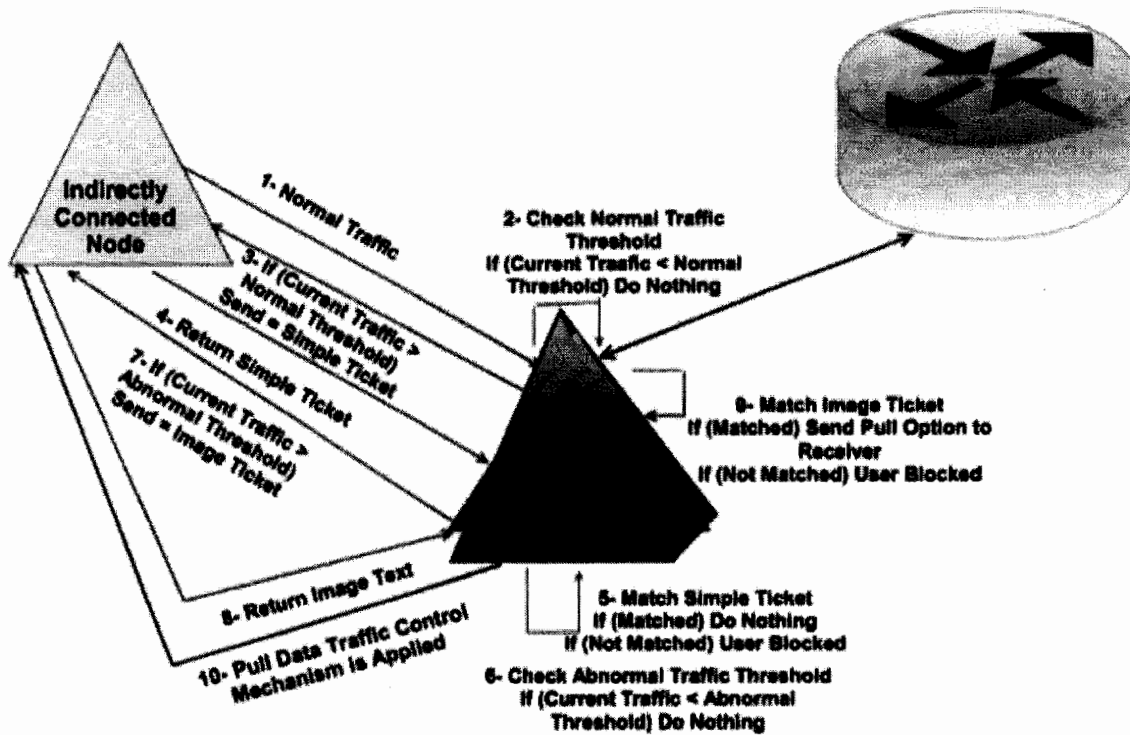


Figure 4.7: Description of Scenario III

For this purpose when a middle node feels that the connected node is sending too many requests it first verifies the identity of the sender by issuing simple ticket as discussed in scenario 1. If the traffic crosses the abnormal threshold the middle node sends the image ticket to the connected node in order to check that the connected node is not a zombie machine. At a stage when a middle node feels that now it is not possible to accept more data from the connected node it notifies to the connected node that I am starting a pull data traffic control mechanism. After that the middle node accepts data from the

connected node only when it has some resources to process it. Figure 4.7 describes the scenario in detail.

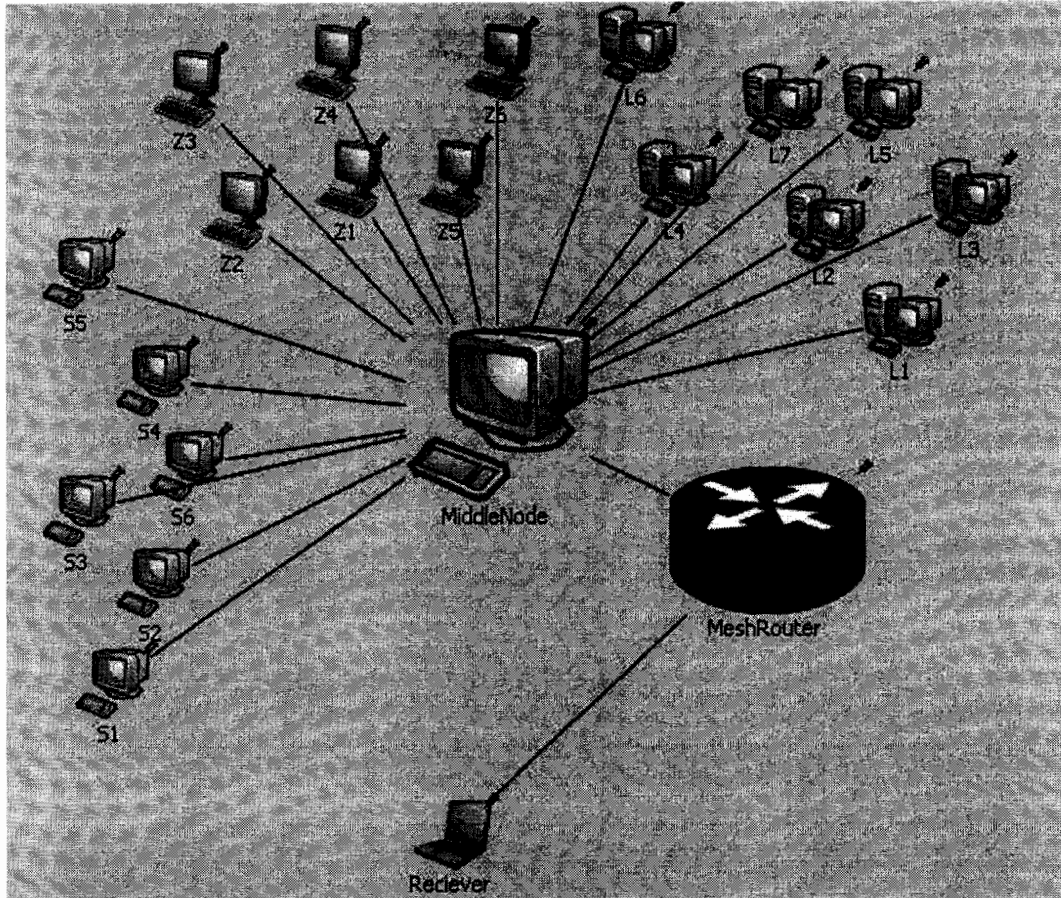


Figure 4.8: Implementation of Scenario III

4.5 Chapter Summary

In this chapter we have discussed the solution scenarios and methodology to implement these solutions. First of all we have discussed the presence process. The receiver publishes its presence information and the mesh router subscribes the presences. After that we have discussed the different pull data options which can be used to receive messages from mesh router. After that we have discussed the authentication process by using simple

ticket and image ticket based authentication. At the end we have combined these processes and explains the solution scenarios.

Chapter 5

5. Implementation and Results

In this chapter we will discuss the implementation scenarios and elaborate the obtained results in detail. The implementation scenarios are divided into four parts. In the first part we will discuss the authentication process with spoofed and zombie detection process, and compare the results of all the scenarios. In the second part we will discuss the different types of pull data option techniques used to pull the data from mesh router. In the third part we will apply the different presence conditions and check the behavior of the system in the applied conditions. In the fourth part we will discuss the delay occurs due the authentication and presence checks.

5.1 Authentication Process with Spoofed and Zombie Detect

We have developed three different implementation scenarios to perform the authentication. In the first scenario we have taken 20 nodes. From which 19 are sending nodes and one is receiving node. In this scenario we did not perform any authentication and simply forward the message the target node without any checking. In second scenario we perform the simple authentication by only checking for the spoofed attacks. In this scenario 6 out of 19 source nodes are spoofing there IPs to launch an attack while other 13 are the legitimate clients. We perform the spoofing check by sending a simple token to from the mesh router to the sender, so if it is spoofed user then it will be unable to return the simple ticket and we will discard the traffic from that node. And in the third scenario we checked for the spoofed as well as zombie attacks.

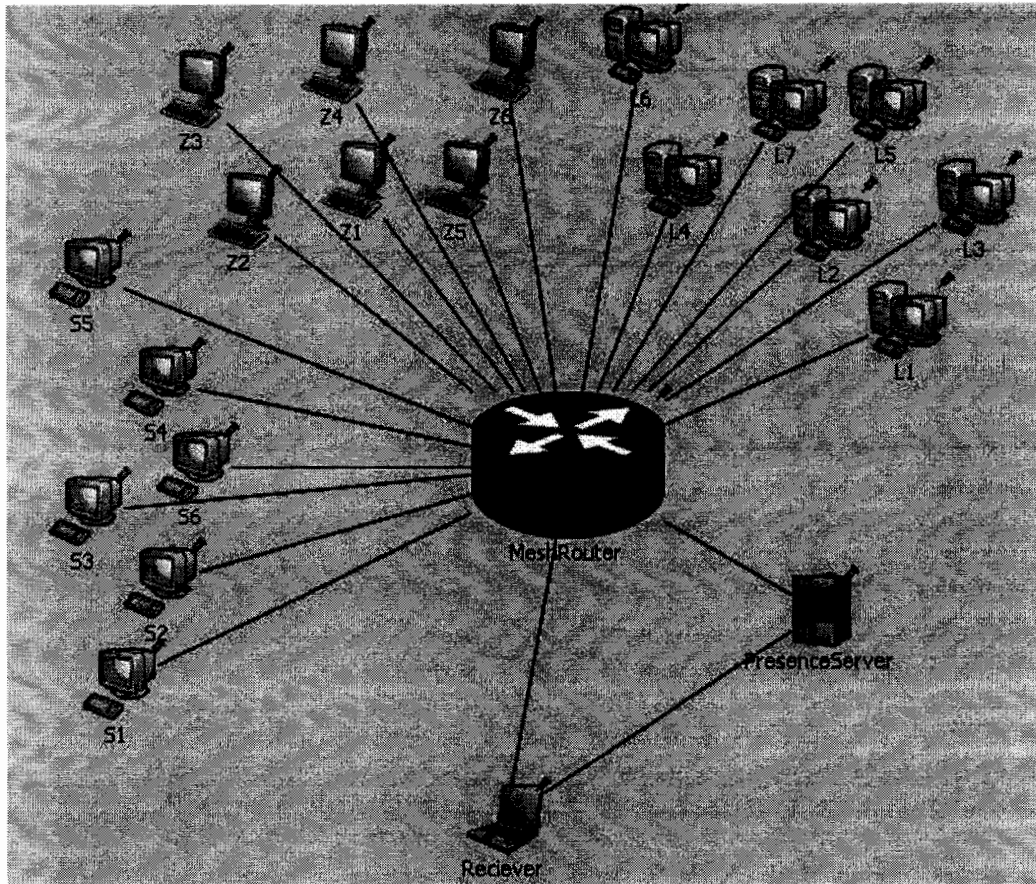


Figure 5.1: Implementation of Spoofed and Zombie Detects

As the zombie is specialized programs and it can return the simple token as it is that's why to block the zombie attacks we perform the image ticket based authentication. As there is no such program which accurately read the complex images that's why that's why the zombie machine will unable to return the image ticket and in this way we can prevent from the attacks. The figure 5.1 shows the implementation screen of the spoofed and zombie detects scenario. We have taken a network of 20 nodes to implement the targeted attacks scenario. From L1 to L7 are the seven legitimate nodes, from S1 to S6 are six Spoofed users and from Z1 to Z6 are the six zombie machines which generate the dummy traffic for the receiver. The receiver published its presence information on the

presence serve while the mesh router watches the receiver presence information from the presence server. We have performed these experiments multiple times and the results are shown in the figure 5.2.

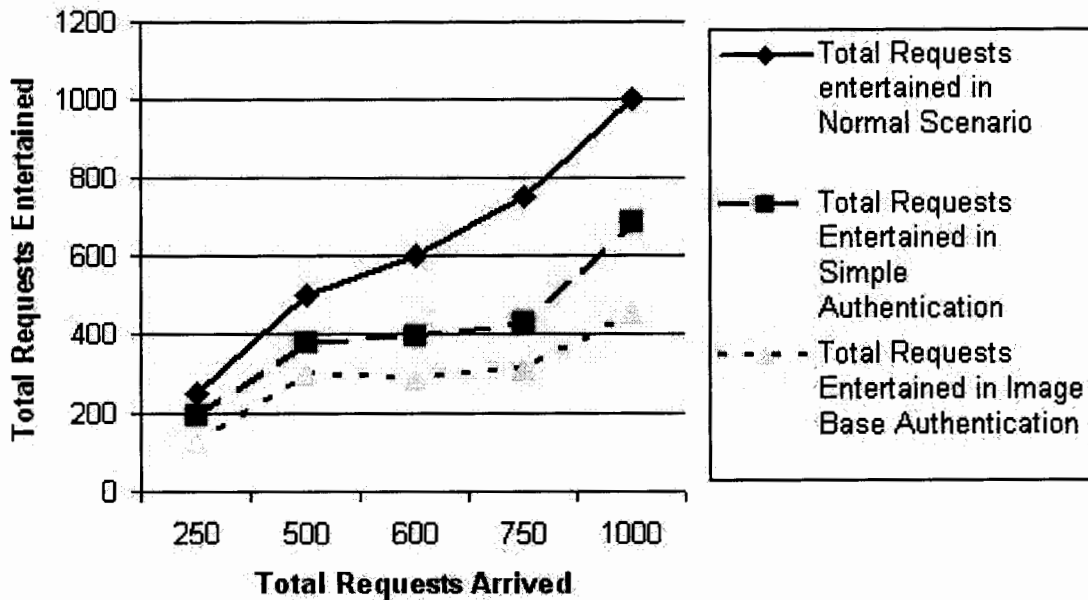


Figure 5.2: Authentication Process

In the above figure we have taken total number of requests sent by all the source nodes along x-axis and total number of requests entertained along y-axis. The blue points and points shows the total number of request entertained for a simple scenario in which no authentication is applied. In this scenario all the request arrived at the mesh router are entertained. In first experiment 250 requests arrived and all of them are entertained by the mesh router and send them to the destination node. Similarly in the second experiment the 500 requests are arrived and all of them are entertained and same results for the other experiments as well.

The pink points shows the second scenario in which simple authentication is applied. The simple authentication will not entertain the requests from the spoofed nodes. In the first

experiment 196 requests are entertained out of 250, the remaining 56 requests are from the 6 spoofed nodes that's why they blocked and not sent to the receiver. In second experiment the total number of request arrived at mesh router are 500 out of which 378 are entertained and remain 122 spoofed requests are discarded. Similar results for the other experiments as well.

The yellow points show the scenario of image based authentication. In this scenario the spoofed as well as zombie request are not entertained on the mesh router. In the first experiment the total number of request entertained are 126 out of the 250 and the remaining 124 which are from spoofed and zombie nodes are discarded. In second experiment 202 requests are discarded out of the 500 arrived requests. Similarly for the other experiments the total number of request entertained are decreasing because the filtering of spoofed and zombie requests.

5.2 Pull Data Traffic Control (Periodic)

If the normal traffic follow exceeds the abnormal threshold value then the router send the pull data option to the receiver. In the pull data technique the receiver will get the data according to its capacity. The first technique we used for the pull data by using the periodic rule. In this scenario the receiver will define the periodic rule to receive the messages from the mesh router. For example the destination node set the 2 messages per second as periodic rule. Now in every second the router will send the 2 packets to the receiver. We perform this experiment several times and calculate the results which are shown in the figure 4.2. If there is no message in the queue then the router will not send any message to the receiver.

In the figure 5.3 we have taken the number of requests along with y-axis and the number of experiment along x-axis. In the vertical bars the blue bar shows the total number of requests arrived at the mesh router and the purple bar shows the number of requests forwarded to the receiver. The periodic rule is set that the mesh router will send two messages per second. The simulation runs for the 100 seconds and we perform multiple experiment by increasing the number of request.

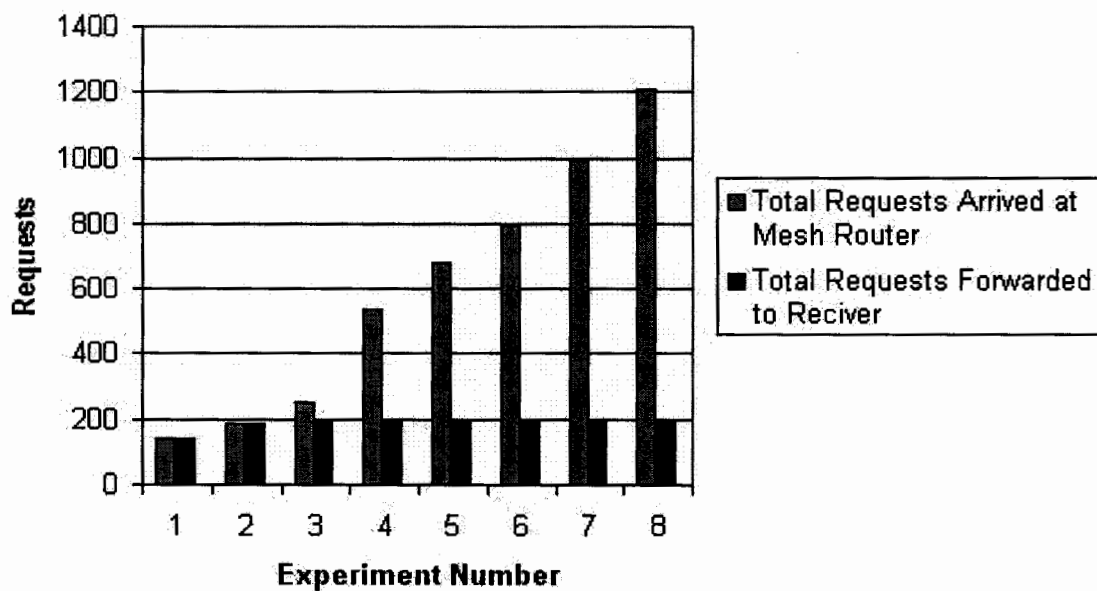


Figure 5.3: Pull Data Option Periodic

In the first experiment 145 messages are sent in 100 second by the source nodes to the mesh router. Mesh router will forward the 2 message per second to the receiver. As there is not much traffic from the sender node that's why the mesh router will not send any message if there is no message in the queue. In the next experiment the sender nodes send the 187 requests in 100 second and all of them are forwarded to the destination node with the rate of two requests per second. Now in the third experiment the number of request increases and the mesh router can forward maximum 200 requests in 100 seconds. From

the 250 requests arrived at the mesh router only 200 will forward to the receiver on First Come First Serve (FCFS) bases and all the remaining messages will be discarded. In the next experiments we increase the traffic rate that's why more requests are received at the mesh router. In all the experiments exactly 200 requests are forwarded to the receiver and remaining all discarded. These result shows that the increased legitimate traffic will not cause as a targeted attack if we use the pull data option periodic rule because the receiver sell defined the periodic rule according to its capacity.

5.3 Pull Data Option Control (Periodic Rule Change)

It works same as the pull data option periodic but in this scenario the receiver can change the periodic rule during the transmission. For example at the start of the simulation the receiver set the periodic rule to receiver two requests per second but during the transmission the node want to receive three requests per second then it simply send the periodic rule change message to the router and router will start forwarding the requests according to the new periodic rule. By using this technique receiver will efficiently utilize its resources by changing its state time to time accordingly.

In the below figure the number of requests is shown along y-axis and experiment number is shown along x-axis. The periodic rule is dynamically changes during the simulation. At the start of the simulation the receiver set the periodic rule as two requests per second. After the 25 seconds the receiver sends the request to change the periodic rule to the mesh router. The new periodic rule is the receiver can receive three requests per second. After the 50 seconds the receiver again changes the periodic rule to two requests per second. The simulation runs for the 100 seconds. Now by using these periodic rules a receiver can receive maximum 250 requests in 100 seconds.

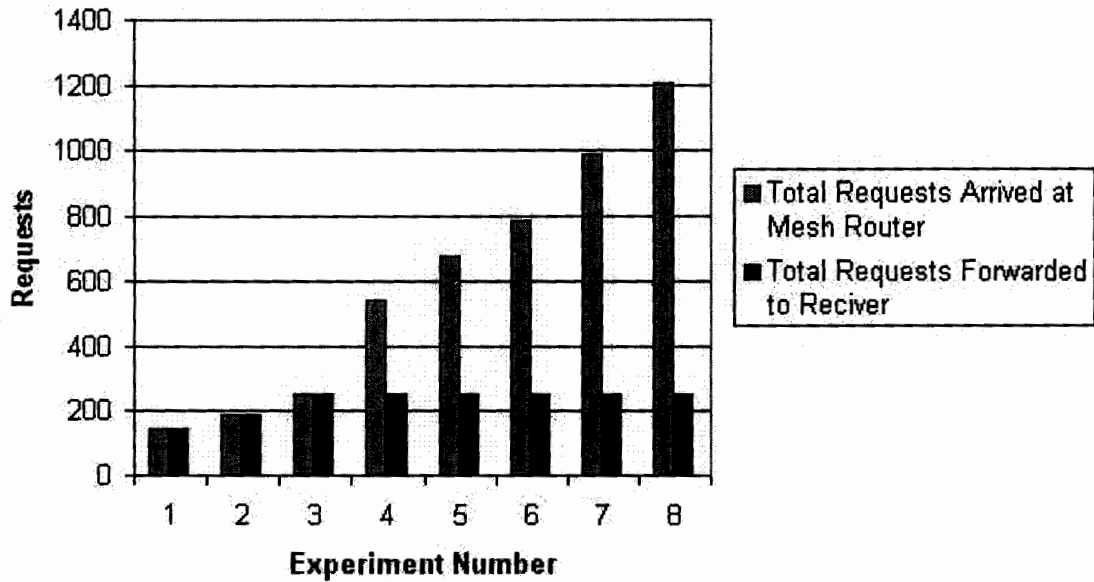


Figure 5.4: Pull Data Option Periodic rule Change

In the figure 5.4 the first experiment shows that the 145 requests are sent and all are delivered to the receiver by using the dynamic periodic rule. In second and third experiment also all the requests are entertained and forwarded to the receiver. In all other experiments 250 requests are received by the receiver by using the dynamic periodic rule on FCFS bases. All the requests other than first 250 are not entertained and discarded.

This pull technique is more feasible than the pull data option with static periodic rule because it utilize the network resources more efficiently. If the receiver feels congestion or it will unable to manage the requests according to the periodic rule than it can easily be managed by changing the periodic rule.

5.4 Pull Data Option Control (Pull Message)

In this pull data option control technique no periodic rule is used. The request is forwarded when the receiver send pull data request to the mesh router. When the receiver

wants to receive message it sends pull data request to the mesh router as a result of which mesh router send exactly one message to the receiver. This technique can be used on congested links. It will restrict the bulky traffic and only receive limited desired number of requests. It will waste the network bandwidth and resources bus sending pull request for each message to receive.

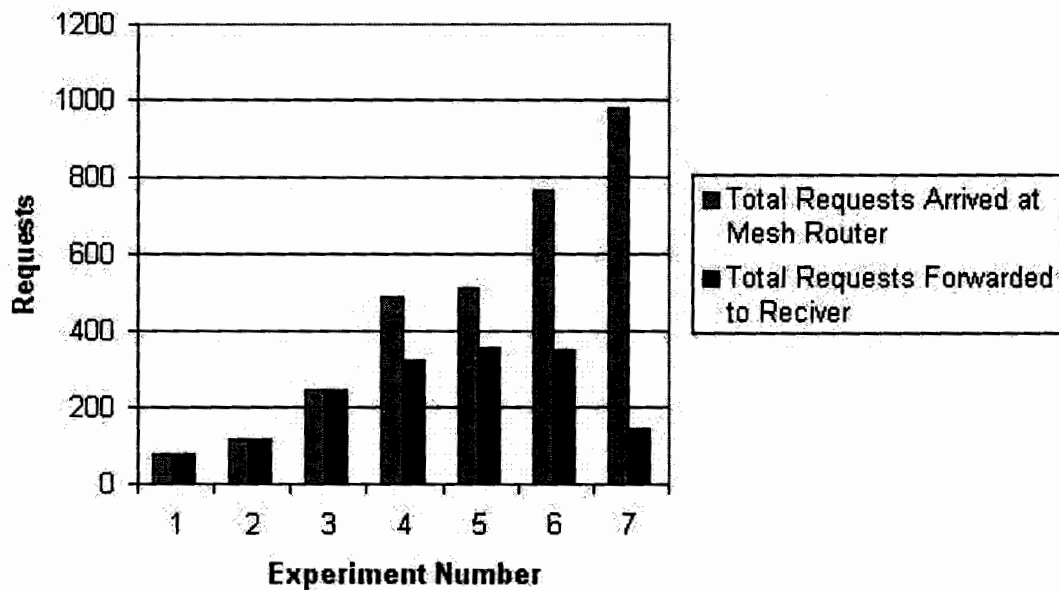


Figure 5.5: Pull Data Option Control (Pull Message)

We have performed multiple experiments by using this technique and results are shown in the figure 5.5. In the above figure the number of requests is shown along y-axis and the experiment number is shown along x-axis. The blue bar shows the total number of requests arrived at mesh router and the purple bars shows the number of requests forwarded to receiver. In the first experiment 80 messages are sent by the sending nodes and receiver send 80 pull message requests to the mesh router as a result of which mesh router will forward all messages to the receiver, one against each pull message request. If there is no message in the queue and receiver sends the pull message request than mesh

router will wait for message. When any sender sends the message the mesh router will send it to the receiver against the saved pull message request. In the forth experiment total 490 messages are received by the mesh router but only 324 messages are forwarded to the receiver because the receiver sends 324 pull message requests to the mesh router. The messages are forwarded in FCFS order and all the extra messages will be discarded.

5.5 Pull Data Option Control (Multiple Pull)

It works same as pull data option control pull message with minor variation. In this technique the mesh routers sends multiple message against one pull data request. The receiver will specify the number messages it wants to pull for one pull data request. This technique is better than the pull data option pull message because the receiver can receive multiple message against one pull request, it will automatically save the network resources. For example if receiver creates a rule that it wants to receive 5 messages against one pull request. The receiver will notify mesh router about the rule. When the receiver sends the pull data request the mesh router sends the specified number of messages to the receiver. We have performed multiple experiments using this technique and captured the results which are shown in the figure 5.6.

In the below figure the number of requests is shown along y-axis and the experiment number is shown along x-axis. The blue bar shows the total number of requests arrived at mesh router and the purple bars shows the number of requests forwarded to receiver. In the first experiment 82 messages are sent by the sending nodes and receiver send 17 pull message requests to the mesh router as a result of which mesh router will forward 82 messages to the receiver, five against each pull message request. If there is no message in

the queue and receiver sends the pull message request than mesh router will wait for message. At the end of the simulation the receiver send the pull request but the mesh router contains only two messages to send. So the mesh router will send 2 messages and wait for the next message to arrive.

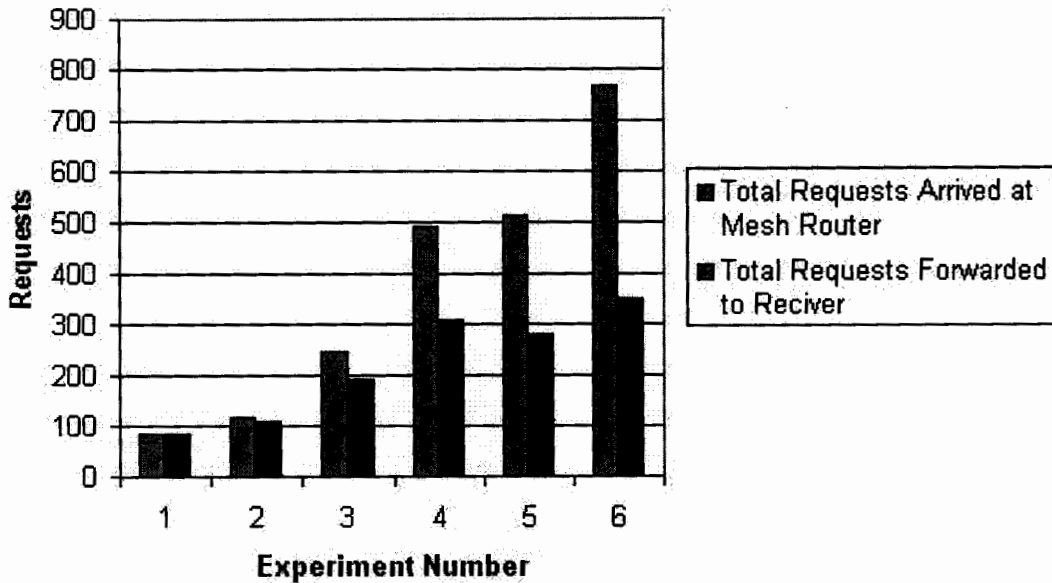


Figure 5.6: Pull Data Option Control (Multiple Pull)

When any sender sends the message the mesh router will send it to the receiver against the saved pull message request. In the fourth experiment total 490 messages are received by the mesh router but only 310 messages are forwarded to the receiver because the receiver sends 62 pull message requests to the mesh router. The messages are forwarded in FCFS order and all the extra messages will be discarded.

5.6 Pull Data Option Control (Pull at Middle)

In this technique the user will not use pull data option from the start of the simulation. The pull data option is adopted according to a certain rule. If the specified rule fulfilled

then the receiver will shift to the pull data option. For example if the request rate is more than 10 per second the receiver will use the pull data option. In the start the receiver will receive the messages in flow when the message rate increase from the 10 messages per second then the receiver will start pull data option control pull message technique. The mesh router will send exactly one message against one pull request.

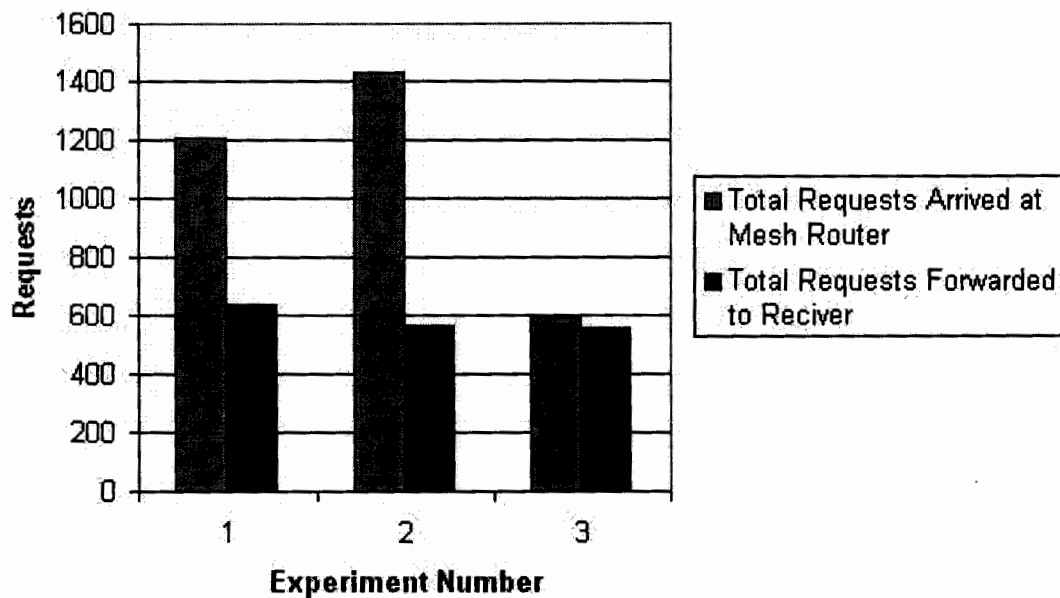


Figure 5.7: Pull Data Option Control (Pull at Middle)

When the rate of the message arrival comes down from 10 messages per second then the receiver again start getting messages in flow without pull request. We have performed multiple experiments to capture the results. The results of the experiments are shown in the figure 5.7. In the above figure the number of requests is shown along y-axis and the experiment number is shown along x-axis. The blue bar shows the total number of requests arrived at mesh router and the purple bars shows the number of requests forwarded to receiver. In the first experiment the sending rate is 7 messages per second for first 10 seconds, 8 messages per second for next 17 seconds, 14 messages per second

for next 25 seconds, 9 messages per second for next 19 seconds, 19 messages per second for next 24 seconds and 6 messages per second for last 5 seconds. By using these rates the mesh router received total 1204 messages in 100 seconds. When the simulation starts the arrival rate is less than 10 that's why the receiver will get 70 messages in first 10 seconds and 136 messages in next 17 seconds. After 27 second the rate increase to 14 messages per second which exceeded from the specified rule that's why the receiver will start pulling data by sending pull data option request. The receiver pulled 113 messages in the next 25 seconds by using pull data option. After that the rate again becomes less than 10 so the receiver will again start getting messages in flow without pull request. The receiver will get 162 messages in next 19 seconds. Then again rate increases from 10 so receiver will pull 123 messages in next 24 seconds and get 30 messages in the last 6 seconds. In this way total 634 messages will be delivered to the receiver in the 100 seconds. The messages are forwarded in FCFS order and the remaining messages will be discarded.

5.7 Presence Check (Scenario 1)

In the first experiment three presence rules are configured. In this scenario there are three sender nodes X, Y and Z, and receiver wants to get the traffic form these senders according to the following rules.

1. Don't accept any message from user Z
2. Accept only 2 messages per second from user Y
3. Give priority to messages of user X

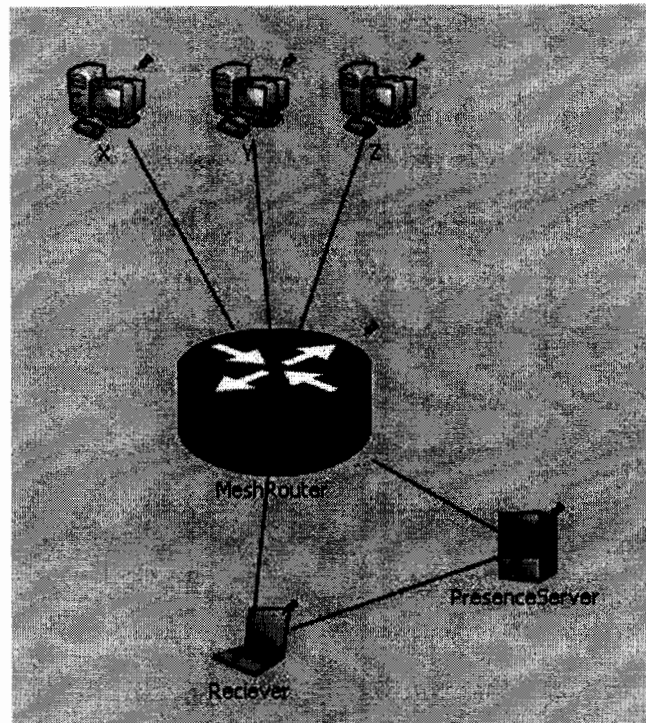


Figure 5.8: Implementation of Presence Scenarios

In 100 seconds simulation user Z sends total 250 requests. User Y sends 4 requests per second. User X sends 2 requests per seconds in first 30 seconds, 3 requests per second in next 45 seconds and 4 requests per second in last 25 seconds. Pull rule was periodic and it was to receive 3 requests per second. In this way the total messages sent in 100 second simulation is 945 and total message received by the receiver are 300.

In first 30 seconds of the simulation the receiver does not receive any message from node Z because of the presence condition. Node X sent 60 messages in first thirty seconds and all are forwarded to the receiver while remaining 30 will be forwarded from Node Y.

For the next 45 seconds all the message from the Node X will be forwarded to the receiver because of the higher priority. Node Y also sent the message during this time but it remains in the queue until all the messages from Node X forwarded to the receiver.

first 20 seconds, 3 requests per second in next 50 seconds and 4 requests per second in last 30 seconds. Pull rule was periodic and it was to receive 5 requests per second.

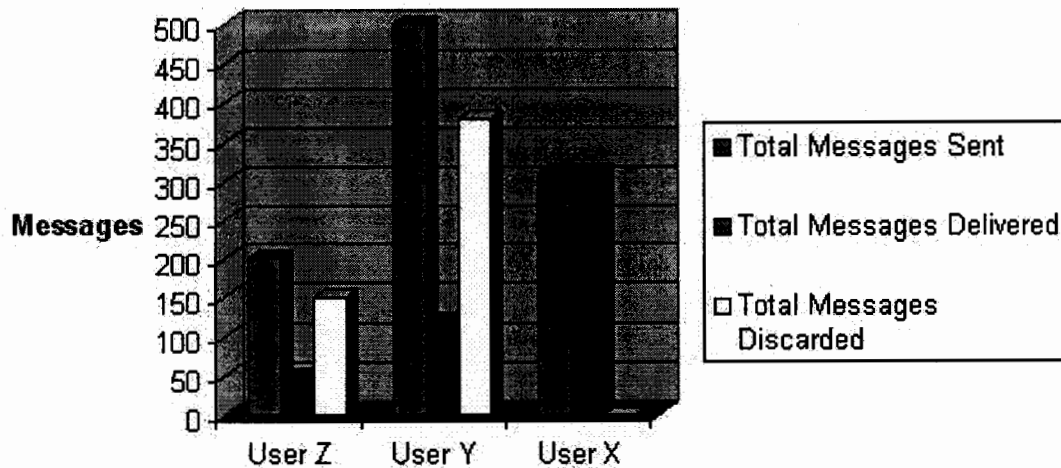


Figure 5.10: Presence Check (Scenario 2)

The simulation runs for the 100 seconds and during this time the node Z will send 200 messages, node Y sends 500 messages while node X sends 310 messages. The destination will receive 500 messages in total. For first 20 seconds the receiver will receive 100 messages. The node X sends 40 messages during 20 seconds and all of these messages are forwarded to the destination node. The user Y sends 100 messages from which 60 are forwarded while time is less than 5:00 PM that's why no message from node Z have forwarded. For the next 50 seconds 150 messages from node X, 80 messages from node Y while 20 messages from node Z are forwarded to the destination node. Now as the time exceeded from the 5:00 PM that's why destination node can accept traffic from node Z. As the node Z have priority over the node Y that's why for last 30 seconds 30 messages from node Z are forwarded and no message from node Y forwarded to the

destination node. While 120 messages from node X are forwarded in last 30 seconds due its high priority.

5.9 Presence Check (Scenario 3)

In this scenario three presence rules are configured. In this scenario there are three sender nodes X, Y and Z, and receiver wants to get the traffic form these senders according to the following rules.

1. Don't accept any message from user Z from 4:30 to 5:00 pm
2. Accept 2 messages per second from user Y for first 50 seconds and 3 messages per second for next 50 seconds.
3. For first 30 seconds user X has the priority, next 40 seconds user Y has the priority, last 30 seconds user Z has the priority.

The simulation starts running at 4:59. In 100 seconds simulation user Z sends 2 requests per seconds for first 50 seconds and 7 requests per second for last 50 seconds. User Y sends 5 requests per second. User X sends 2 requests per seconds in first 20 seconds, 3 requests per second in next 50 seconds and 4 requests per second in last 30 seconds. Pull rule was periodic and it was to receive 5 requests per second. During the 100 seconds the node Z sends 450 messages, node Y sends 500 messages while node X will send 310 messages. In this way the total messages sent by three senders will be 1260 and total messages the receiver can receive in 100 seconds are 500.

For first 30 seconds the receiver can receive maximum 150 messages. As the time is less than 5:00 PM that's why no message from node Z will forwarded. Node X has priority in first 30 seconds and node X sends 70 messages in these 30 seconds that's why all of these

70 messages are forwarded to the destination. Remaining 80 messages are forwarded from node Y.

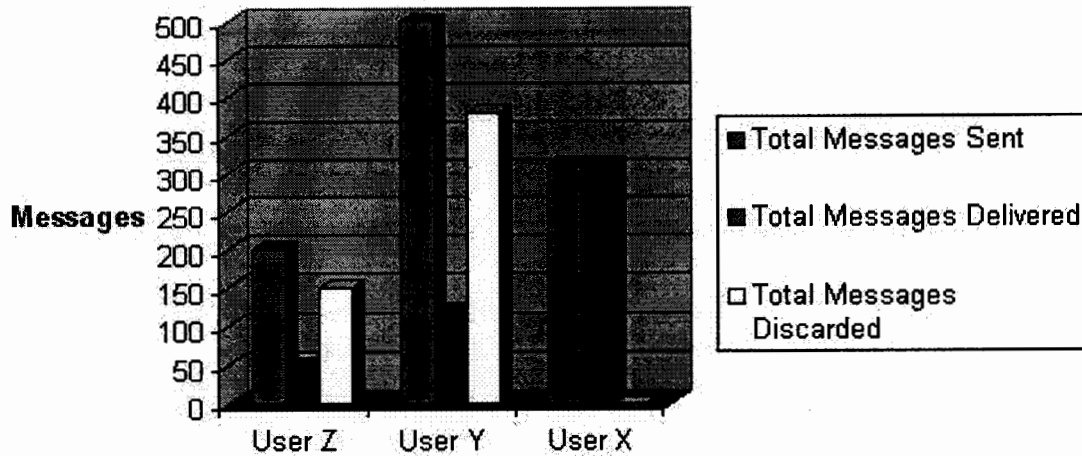


Figure 5.11: Presence Check (Scenario 3)

For next 40 seconds node Y has priority and the node Y sends total 250 messages and receiver can only receive only 200 messages maximum. That's why the 200 messages of node Y are forwarded to the destination and no message from node X and Z are forwarded during this time period. For last 30 seconds node Z has priority and the node Z sends total 210 messages and receiver can only receive only 150 messages maximum. That's why the 150 messages of node Z are forwarded to the destination and no message from node X and Y are forwarded during this time period. The figure 5.9 shows that 70 messages from node X, 280 message from Y and 150 messages from node Z are forwarded to destination node during the 100 seconds simulation and all other messages are discarded.

5.10 Delay in Simple Ticket based Authentication

First of all we check the delay in the simple scenario when there is no authentication is applied. We calculate the time consumed for a message to reach up at the mesh router without any authentication method applied. Then we calculate the delay from sender to the mesh router and simple ticket based authentication for multiple messages. On the bases of these calculations we calculate the average delay per packet in both scenarios.

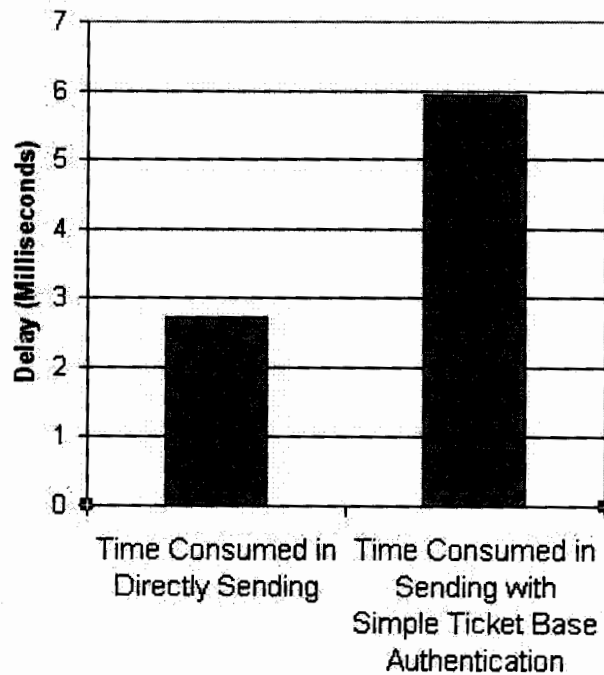


Figure 5.12: Delay in Simple Ticket Based Authentication

In the above figure the time consumed to send packet from sender to mesh router is along Y-axis. The unit of time is in milliseconds. The first blue vertical bar shows the time consumed directly sending packet from sender to mesh router without any authentication method applied, so it takes 2.72 milliseconds on average for one packet. The second vertical blue bar shows the average time consumed to send the packet when simple ticket based authentication is applied. It takes 5.94 milliseconds for one packet on average.

5.11 Delay in Image Ticket based Authentication

After calculating the time for simple sending and simple ticket base authentication we applied the image ticket based authentication and calculate the time consumed in sending message, simple ticket based authentication and image ticket based authentication.

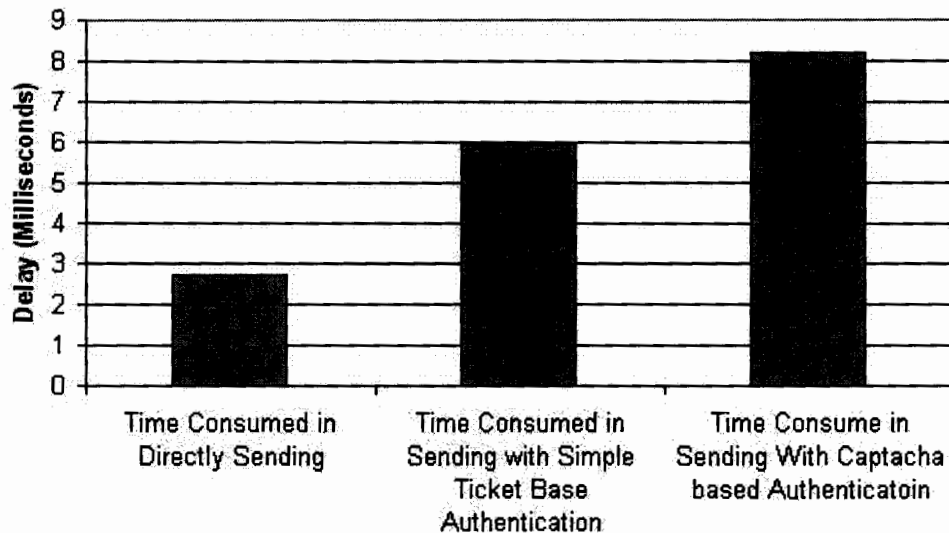


Figure 5.13: Delay in Image Ticket based Authentication

In the above figure the time consumed to send packet from sender to mesh router is along Y-axis. The unit of time is in milliseconds. The third vertical bar shows the time consumed on the image ticket based authentication process. The average time to send one packet from sender to mesh with image ticket based authentication applied is 8.17 milliseconds. The first blue vertical bar shows the time consumed directly sending packet from sender to mesh router without any authentication method applied, so it takes 2.72 milliseconds on average for one packet. The second vertical blue bar shows the average time consumed to send the packet when simple ticket based authentication is applied. It takes 5.94 milliseconds for one packet on average.

5.12 Delay in the Presence Check

After the image ticket based authentication we applied the different presence checks and calculate the time consumed for the presence conditions. On the basis of these calculation we calculate the average time taken by the complete process for one packet which includes simple ticket based authentication, image ticket based authentication and presence conditions checks.

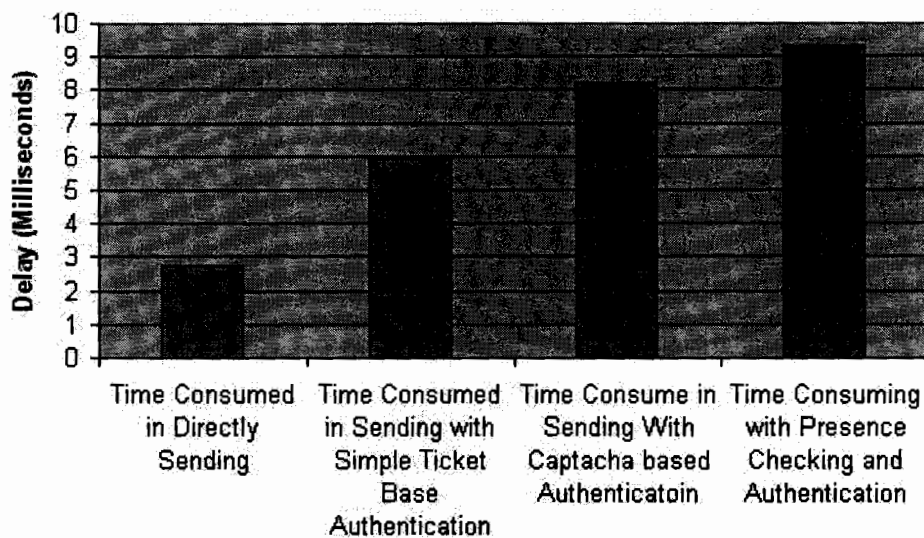


Figure 5.14: Delay in Presence Check

In the above figure the time consumed to send packet from sender to mesh router is along Y-axis. The unit of time is in milliseconds. The fourth vertical bar show the time consumed for the presence check after the authentication process. And the complete process takes 9.31 milliseconds per packet. The third vertical bar shows the time consumed on the image ticket based authentication process. The average time to send one packet from sender to mesh with image ticket based authentication applied is 8.17 milliseconds. The first blue vertical bar shows the time consumed directly sending packet from sender to mesh router without any authentication method applied, so it takes 2.72

milliseconds on average for one packet. The second vertical blue bar shows the average time consumed to send the packet when simple ticket based authentication is applied. It takes 5.94 milliseconds for one packet on average.

5.13 Overall Delay Comparison

We have performed multiple experiments to obtain the time consumed in each of the scenarios listed in the section 5.1.

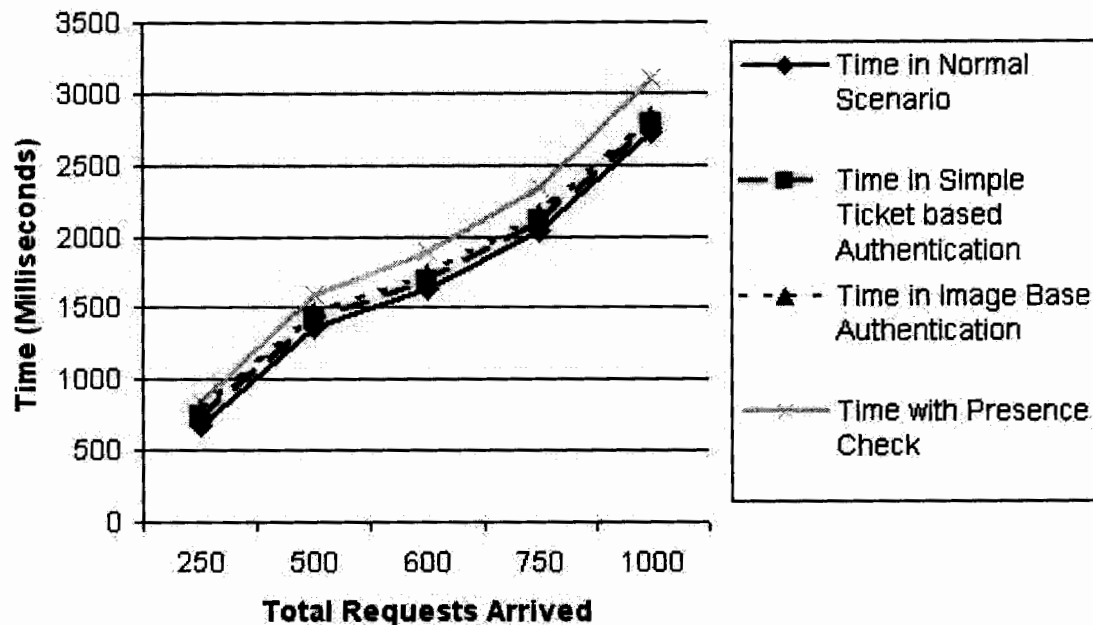


Figure 5.15: Overall Delay Comparison

We have separately calculated the time taken by the specific number in normal scenario, simple ticket based authentication and image ticket based authentication and applying presence conditions. The comparison of the time taken by different scenarios is shown in the above figure. In the above figure the blue line shows the normal scenario when no authentication and presence conditions are applied. For 250 messages it takes 680

milliseconds for processing. The pink line showing the time for simple ticket based authentication process. It takes 744.4 milliseconds to process 250 requests. The image based ticket authentication takes 786.39 milliseconds to process 250 requests, the green line in the figure is showing this scenario. The sky blue line is the time taken when the authentication as well as presence conditions are applied. For 250 requests it takes 840.09 milliseconds for processing.

5.14 Chapter Summary

In this chapter we have discuss the implementation of the solutions scenarios. In the experiment we show the number of spoofed and zombie packets blocked due to the proposed authentication process. The experiments show that the proposed solution successfully detects the attacking behavior of the spoofed and zombie nodes and discard the traffic from those nodes for a specified time. In the second part we have discuss the different pull strategies applied on the sender and mesh router. It will help the sender to avoid the congestion of legitimate traffic. The receiver will receive the traffic according to its capacity and requirement. In the next part we applied the different presence conditions of the sender. By using these presence checks the receiver can receive messages from its specified nodes and rates. At the end of the chapter we have discussed the delay occurs due to the authentication and presence checks. The results show that we the targeted attacks are prevented with very minor delay.

Chapter 6

6. Conclusion and Future Work

In this chapter we will conclude the thesis and discuss the future work.

6.1 Conclusion

Infrastructure based wireless mesh network connects different types of networks with each other by using mesh routers. So on one side of a mesh router an Internet node can be connected and on the other side a sensor node may exist. So for an Internet node there are high processing speed, high bandwidth, and no battery or energy issues but for sensor node energy is a very serious issue and bandwidth is also low. Processing power of a sensor node is also very low as compared to an Internet connected high speed workstation. This situation allows the Internet connected node to launch a targeted attack on a node of sensor network.

Targeted attack can easily be launched by sending enormous number of requests to a particular receiver. For Internet connected node, generating thousands of requests per unit time is not a big issue but for a sensor node receiving and processing those requests is a big problem and it can result in expiring the battery of a sensor node. It can also cause denial of service attack on that particular sensor node.

We proposed an authentication process to detect and prevent from targeted attacks. We introduce the simple ticket based authentication to detect the spoofed attacks and image based authentication for the zombie attacks. We also use the presence service to

communicate the receive state and priorities with the mesh router. We also proposed the pull data options if the legitimate traffic exceed from the node capacity.

Our solution successfully detects the spoofed and zombie attacks and discards all the requests from these nodes. By using these scenarios we detects the targeted attacks as well as the network resources are also saved. By the use of presence service and pull data options techniques the receiver will able to receive the traffic according to its requirement on the basis of presence conditions and pull data options used.

6.2 Future Work

Our solution detects and prevents the targeted attacks in the wireless mesh networks. In WMN a selfish mesh router can create the problem by introducing some type of congestion or make it unable for the communication. The attack can be launched on the mesh router by using the sniffer. The sniffer is specialized program which analyze the traffic by launching a passive attack. So there must be some solution to recognize those selfish nodes to avoid the attacks.

References

- [1] Ian F. Akyildiz, Xudong Wang, Weilin Wang " Wireless mesh networks: a survey Broad band and Wireless Networking", (BWN) Lab, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, 1 January 2005
- [2] Raheleh B. Dilmaghani, Ramesh R. Rao, "Hybrid Wireless Mesh Network with Application to Emergency Scenarios ", Journal of Software, 3:2, PP: 52-60 February 2008
- [3] YAN Wei, REN Maosheng, Tong Zhao, LI Xiaoming "A Bandwidth Management Scheme Support for Real-time Applications in Wireless Mesh Networks", ACM symposium on Applied computing Computer networks, Fortaleza, Ceara, Brazil, PP: 2063-2068, 2008
- [4] Ian F. Akyidiz, Xudong, Weilin Wang, "Wireless Mesh Network: a Survey", The International Journal of Computer and Telecommunications Networking, 47:4, PP: 445-487, March 2004
- [5] Vital Mynampati, Dilip Kandula, Raghuram Garimilla, Kalyan Srinivas, "Performance and Security of Wireless Mesh Networks", Blekinge Institute of Technology, June 2009
- [6] Vinod Kone, Sudipto Das, Ben Y. Zhao, Haitao Zheng "QUORUM: quality of service in wireless mesh networks" Mobile Networks and Applications, 12:5, PP.358-369, December 2007
- [7] Fabian Hugelshofer, Paul Smith, David Hutchison, Nicholas J. P.Race, "OpenLIDS: A Light weight Intrusion Detection System for Wireless Mesh Networks", International Conference on Mobile Computing and Networking, Beijing, China, 2009

- [8] YeYan, JiannongCao and ZhuLi, "Stochastic Security Performance of Active Cache Based Defense against DoS Attacks in Wireless Mesh Network", Second International Conference on Advances in Mesh Networks, Athens/Glyfada, Greece, 2009
- [9] XiaWang, JohnnyS.Wong , Fred Stanley and SamikBasu, " Cross-layer Based Anomaly Detection in Wireless Mesh Networks", Ninth Annual International Symposium on Applications and the Internet , Washington, DC, USA, 2009
- [10] Shafiullah Khan, Kok-Keong Loo, Tahir Naeem, Mohammad Abrar Khan, " Denial of Service Attacks and Challenges in Broadband Wireless Networks ", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008
- [11] Mehdi Bezahaf, Luigilanne, "Practical DHT-Based Location Service for Wireless Mesh Networks", International Conference on Emerging Networking Experiments and Technologies, PP: 47-48, Rome, Italy, 2009
- [12] Fabio Martignon, Stefano Paris, Antonio Capone, "A Framework for Detecting Selfish Misbehavior in Wireless Mesh Community Networks", Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks, Pages: 65-72, 2009
- [13] Zeeshan Shafi Khan, Muhammad Sher, Khalid Rashid, Aneel Rahim, "A Three-Layer Secure Architecture for IP Multimedia Subsystem-Based Instant Messaging", Information Security Journal: A Global Perspective, 18: 3, PP:139-148, 2009
- [14] Zeeshan Shafi Khan, Khalid Rashid, Fahad Bin Muhaya, Qutbuddin, Aneel Rahim, "Realization of call back authentication for web to cellular phone SMS communication", Computer and Mathematics with Application, Elsevier, doi:10.1016/j.camwa.2009.12.038. 2009

- [15] Sharjeel Gilani, Zeeshan Shafi Khan, Muhammad Zubair, "Receiver Based Traffic Control Mechanism To Protect Low Capacity Network In Infrastructure Based Wireless Mesh Network" First International Workshop on Wireless and Network Security (WNS 2010), Japan.
- [16] Dongmei Jiang, Tet Hin Yeap, Logrippo, L., Liscano, R. , "Personalization for SIP multimedia communications with presence", International Conference on Services Systems and Services Management, 2005.
- [17] Miladinovic, I, "Presence and event notification in UMTS IP multimedia subsystem", Fifth IEE International Conference on 3G Mobile Communication Technologies, 2004
- [18] Wegscheider, F., "Minimizing unnecessary notification traffic in the IMS presence system", 1st International Symposium on Wireless Pervasive Computing, 2006
- [19] Vishal K. Singh and Henning Schulzrinne, "A Survey of Security Issues and Solutions in Presence", www1.cs.columbia.edu/~vs2140/presence/presencesecurity.pdf
- [20] Victoria Beltran, Josep Paradells, "Middleware-Based Solution to Offer Mobile Presence Services", Mobilware'08, 2008
- [21] Lan Wang, Daqing Gu, "A Study on Session Setup for Group Communications in Push-to-talk over Cellular Using Rich Presence", ieeexplore.ieee.org/iel5/4391971/4391972/04392055.pdf?arnumber=4392055
- [22] Michael Rabinovich, Hua Wang "DHTTP: An Efficient and Cache-Friendly Transfer Protocol for the Web", 2001
- [23] Roberto Cusani, Tiziano Inzerilli, Giacomo Di Stasio "Performance analysis and simulation in wireless mesh networks Via Eudossiana 18, 00184 Rome, Italy

[24] Thomas Staub, Reto Gantenbein, Torsten Braun "VirtualMesh: An Emulation Framework for Wireless Mesh Networks in OMNeT++", ICST, ISBN 978-963-9799-45-5 2009

