Wireless Network Behavior under ICMP Ping Flood DoS Attack and Mitigation Techniques

Mitko Bogdanoski[1], Aleksandar Risteski[2]

[1]Military Academy, Skopje, Macedonia
[2]University “Ss. Cyril and Methodius”, Faculty for Electrical Engineering and Information Technology, Skopje, Macedonia

Abstract**:** Internet Control Message Protocol (ICMP) is an error reporting and diagnostic utility and it is considered as a part of Internet Protocol (IP) suite. Although this protocol is very important for ensuring correct data distribution, it can be exploited by malicious users for conducting different Denial of Service (DoS) attacks. Due to the broadcast nature of wireless communication, exploitation of this kind of attack is even easier. By sending bogus ICMP redirect packets, a malicious user can either disrupt or intercept communication from a wireless access point.

In this paper, we present our approach to simulate the ICMP Ping Flood Attack, and to analyze the effects of this attack on wireless networks using OPNET Modeler. We propose several countermeasures against this type of attack. Simulation results regarding the effects of link failure recovery mechanism against this type of attack are discussed.

Keywords**:** ICMP, Ping Flood, DoS, Failure Recovery

1. Introduction

ICMP is a part of the TCP/IP suite. This protocol handles error and control messages. More specific, routers and hosts use ICMP to send reports of problems about datagrams, back to the original source that sent the datagram [1][2]. ICMP messages are encapsulated and sent within IP datagrams.

When the message is generated and error occurred, the original IP header is encapsulated with the appropriate ICMP message and these two pieces are encapsulated within a new IP header in order to be returned as an error report to the ending device. As it can be seen from Figure 1, there are several types of the ICMP messages depending on what the ICMP message is reporting.

One of the best known examples of ICMP in practice is the ping utility. It uses ICMP to check remote hosts for responsiveness and examine overall round-trip time of the probe messages.

The regular ping operation relies on ECHO_REQUEST and ECHO_REPLY ICMP messages, but it may respond to ICMP messages other than ECHO_REPLY when appropriate.

It is more than obvious that ICMP messages are very useful, especially when an error occurs in the network. Unfortunately, malicious users have found a way to turn a good network tool into an attack. The most common types of ICMP attacks are:

ICMP Ping Flood Attack: This attack is based on sending huge number of ping packets, usually using “ping” command from unix-like host. In this way attacked system can not respond to legitimate traffic.

ICMP Smurf Attack: This type of attack floods the victim machine with spoofed ping packets. All these modified packets contain a spoofed IP address of the target victim. This cause broadcast of the misinformation to all hosts in the local network. All of these hosts now respond with a reply to the target system, which is then saturated with those replies. If there are many hosts in used networks, victim will be effectively spoofed by a large amount of traffic.

Ping of Death: An attacker sends to the victim an ICMP echo request packet that is larger than the maximum IP packet size of 65.536 bytes. Since the received ICMP echo request packet is larger than the normal IP packet size, it must be fragmented. A consequence of this is that the victim can not reassemble the packets, so the OS crashes or reboots.

ICMP Nuke Attack: In this type of attack nukes send to the victim an ICMP packet with destination unreachable type 3 messages. The result of this attack is that target system breaks communications with existing connections [4].

In this paper we implement simulation framework for WLAN using OPNET. We quantify the effect of ICMP Ping Flood Attack on WLAN parameters, thereat using different kind of security schemes and protocols we demonstrate their existing vulnerabilities.

Following this introduction, the paper is organized as follows. Section 2 discusses some research on ICMP Ping Flood Attack in 802.11 networks. In Section 3, we are giving brief overview about ICMP Ping Flood Attack. Next, our experimental results are summarized in Section 4. In Section 5 several methods to mitigate DoS effects are discussed, with special reference to the failure recovery mechanism. Finally, in Section 6 we conclude our results and provide some directions for future work.

2. Related work

Wireless networks are very susceptible to DoS attacks. ICMP Ping Flood attack is one of the simplest and most used DoS attacks. Many researchers have already discovered numerous strategies for mitigating this type of DoS attack. In this section, we summarize some of their findings and proposed defense mechanisms.

The authors in [3] embedded an ICMP processing module in the Network Processor (NP) - based firewall according to the characteristics of processing packets flow in IXP2XXX NP and the ICMP protocol layer. They carried out their simulation on development environment WORKBENCH. Their results show that the optimized method proposed in their paper can simplify the process flow and improve the

ICMP processing efficiency. This can be valuable reference for other abnormal packets processing methods in NP based firewalls and common ICMP prevention schemes.

In [5] is analyzed and proved that window based restriction scheme will remove the attack productivity region from the ICMP traffic and will promote only genuine traffic. This will help to neutralize the flooding attacks.

They identified the threshold to signify the attack traffic. If the window is opened beyond the threshold it will generate traffic beyond the tolerable rate. This traffic source which generates beyond identified threshold rate can be blocked for a while which will create more IP space for ICMP source.

Interesting approaches against several attacks caused by ICMP messages are presented in [6]. The number of mitigation techniques that help to eliminate or mitigate the impact of the ICMP attacks against TCP is described. These several techniques can be implemented together to increase the protection against these attacks.

Proposed techniques amongst many others are: TCP Sequence Number Checking, Port Randomization and Filtering ICMP Error Messages Based on the ICMP Payload.

Excellent practical example about the efficiency of the ICMP Ping Flood Attack is shown in [7]. ICMP Ping Flood Attack across a range of IP addresses during a certain period of time has been observed. Several conclusions are drawn based on their experimental obtained results. First, the attacker obstruct the probe responses of the access point to the clients who were using probe requests to search access points. As a result, responses from the access point in the wireless network were essentially jammed during heavy utilization. Control and management packets of the access point are also lost or delayed. This is the reason for contribution of the overall network congestion.

In [8] the authors are taking in consideration the fact that security mechanism for one layer cannot be used as protection mechanism for the other layers. Hence, they are discussing the importance of cross layer security mechanisms and routing protocols for multi-hop wireless networks by critical comparison. The reason of doing this is to protect multi-hop wireless networks from passive, active and denial of service attacks, including the flooding attack.

In [9] new so called Real-time cross-layer flood detection and attack trace-back mechanism (RCFDAT) is proposed. Using this mechanism the authors aim to construct a large-scale multilayer flood detection approach with low computational complexity, high accuracy, and low false-alarm rate. To test the accuracy of the proposed mechanism the theoretical fundamentals have been checked with the help of simulations. RCFDAT mechanism is observing the traffic flow variations. The reason for this is that this sharp increase in traffic flow is the first sign for flooding attack.

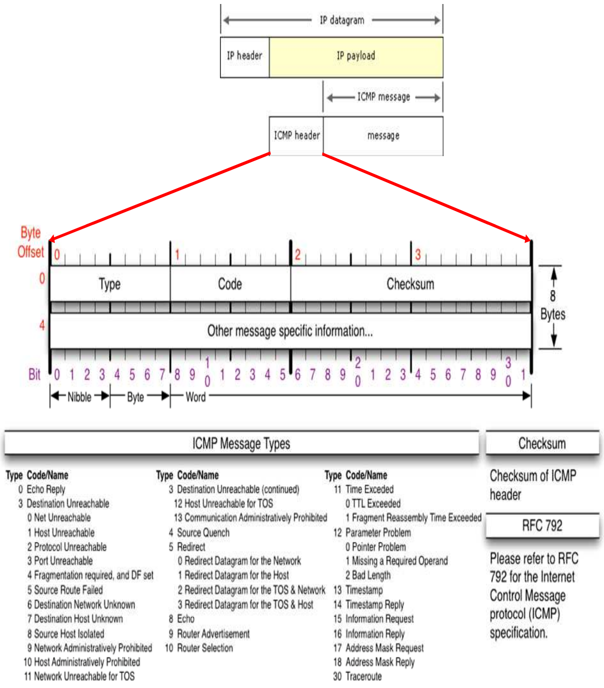
In [10] this type of DoS attack is presented in relatively easy way to understand. The author is giving two solutions against becoming a victim of this type of attack. First presented solution is filtering of the incoming echo request packets. The second solution involves using of netfilter and its "limit" module.

Taking in consideration flooding attack against Wireless Mesh Networks, the authors of [11] proposed a mutual cooperation mechanism between the backbone multi-hop APs and serving gateway. The reason for this is to detect and prevent the possibility of cloned AP. Using this mechanism the large scale exploration of WMN is eliminated.

3. ICMP Ping Flood Attack Background

As we already explained, the original ICMP messages are encapsulated and sent within IP datagrams. An ICMP packet is composed of ICMP header and ICMP payload (See Figure 1). The type and format of the ICMP packet are indicated in the type field in ICMP header [3].

One of the most used ICMP messages is ping command. This command is usually used to detect network or host communication failures and troubleshoot common TCP/IP connectivity problems. However, ping command can also be used to cause severe consequences on wireless network.



Type Code/Name
0 Echo Reply
3 Destination Unreachable
0 Net Unreachable
1 Host Unreachable
2 Protocol Unreachable
3 Port Unreachable
4 Fragmentation required, and DF set
5 Source Route Failed
6 Destination Network Unknown
7 Destination Host Unknown
8 Source Host Isolated
9 Network Administratively Prohibited
10 Host Administratively Prohibited
11 Network Unreachable for TOS

Type Code/Name
3 Destination Unreachable (continued)
12 Host Unreachable for TOS
13 Communication Administratively Prohibited
4 Source Quench
5 Redirect
0 Redirect Datagram for the Network
1 Redirect Datagram for the Host
2 Redirect Datagram for the TOS & Network
3 Redirect Datagram for the TOS & Host
8 Echo
9 Router Advertisement
10 Router Selection

Type Code/Name
11 Time Exceded
0 TTL Exceeded
1 Fragment Reassembly Time Exceeded
12 Parameter Problem
0 Pointer Problem
1 Missing a Required Operand
2 Bad Length
13 Timestamp
14 Timestamp Reply
15 Information Request
16 Information Reply
17 Address Mask Request
18 Address Mask Reply
30 Traceroute

Figure 1. ICMP Message Encapsulation

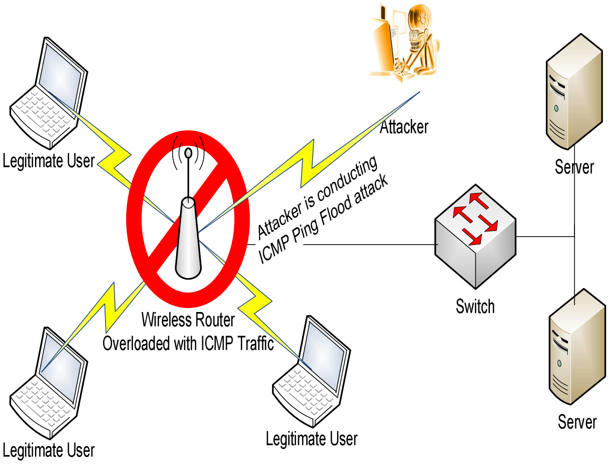
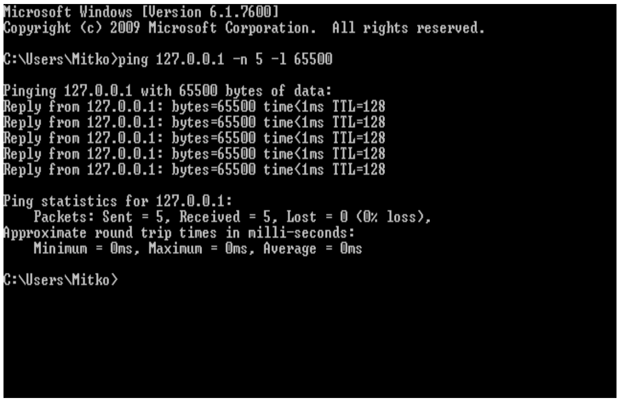

Legitimate User
Attacker
Server
Attacker is conducting ICMP Ping Flood attack
Switch
Wireless Router Overloaded with ICMP Traffic
Legitimate User
Legitimate User
Server

Figure 2. ICMP Ping Flood Attack



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Mitko>ping 127.0.0.1 -n 5 -l 65500

Pinging 127.0.0.1 with 65500 bytes of data:
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Mitko>
```

Figure 3. ICMP Ping Flood Attack through DOS

The attack caused using ping command is known as *ICMP Ping Flood Attack*, or simply Ping Flood Attack (Figures 2 and 3). ICMP Ping Flood attack is a simple DoS attack where the attacker continuously sends a large amount of ICMP Echo Request (Ping) packets to the victim machine and saturates the network with traffic.

The response to each of these requests limits the amount of available system resources for other processes. The continuing requests and replies can be a reason for slowing the network and causing the legitimate traffic to continue at a significantly reduced speed or, in extreme cases, to be disconnected. A Ping Flood attack can effectively disable the network connectivity.

4. Simulation results and analysis

Our work conducted regarding presentation of the effects of ICMP Ping Flood attack is based on OPNET Modeler. There are several reasons why we are using this simulation tool for our research. OPNET provides a Graphical User Interface (GUI) which allows realistic networks simulation, and has a performance data collection and display module. Moreover, it has been extensively used and there is wide confidence in the validity of the results it produces.

Our project contains a wireless network of three subnets, each representing a floor of a building. The third floor is the location of the network's two servers and a switch that connects the three floors to the outside world.

The access point (wireless router) is placed at second floor and eight workstations are evenly spread out among first and second floor. The access point is connected to servers through a switch.

In our paper we are going to consider four different scenarios.

The first scenario is when the wireless network, or in our case, the wireless access point (router) is not attacked (**no Attack**). The second scenario is when the same network is attacked by one malicious node with ping packet size of 256 bytes (**Attack 1**). In the third scenario (Figure 4) attack is conducted by three attackers with ping packet size of 256 bytes (**Attack 2**). The last scenario is situation when this network is attacked by one malicious node, but the size of the IP packets sent by this node is 22000 bytes (**Attack 3**).

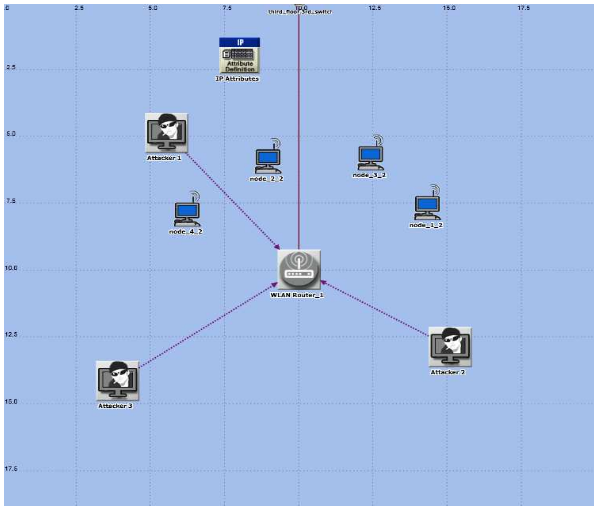


Figure 4. 2nd Floor of the building under atttack of three malicious nodes (attackers)

In our simulation we are setting the folowing ping parameters:

- IP Version - Specifies whether IPv4 or IPv6 packets should be used. The specified IP version must be supported on both the source and destination nodes. In all our scenarious this parameter is *set to IPv4.*
- Interval - time between successive "ping" packet transmissions. This time for all scenarios when attack is conducted is *set to 5s*.
- Packet size - "ping" packet size to be sent to the specified host. An extra eight bytes of ICMP header gets tagged on to this packet before it gets encapsulated in an IP datagram. The values of this parameter for different scenarious can be seen in Table 1.
- Count - Specifies the number of "ping" packets (ICMP ECHO Requests) to be sent. This parameter is *set to "unlimited"*.
- Timeout - Specifies the time after which the sent "ping" requests is considered lost, if no response has been received from the specified host. For all scenarios when network is under attack this time is *set to 5s*.
- Record Route - Specifies the option of printing the route a given "ping" packet takes to get to the specified host. It uses the "record route" option in the IP header. This parameter in all scenarios is *set to "enable"*.

Table 1. Characteristics of the three simulated attacks

	Attack 1	**Attack 2**	**Attack 3**
Number of malicious nodes	**1**	**3**	**1**
Packet size (bytes)	**256**	**256**	**22000**

Because malicious nodes are flooding the wirelees router with frequent ICMP Ping packets, the router is unable to respond to legitimate users, or in our case, response is slower.

The number of ICMP ECHO packets in the case when no ICMP Flooding attack is performed, is 0. Just for comparation, the total number of the ICMP ECHO packets when Attack 2 and Attack 3 are conducted is 5,511,030 and 5,430,732, respectively.

The time of simulation is set to 20 minutes. The profile start time is set to 100 s and for applications it is 5 s. During the initial 105 s no traffic is generated at all. This time can be considered as warm up time, which allows queues and other simulated parameters to get in a “normal running conditions for the system”.

The average value from the obtained simulation results will be presented. As results *global statistic* of the simulated scenario will be shown. These statistics are scoped to the simulation as a whole, in contrast to local statistics, which are scoped to a particular queue or processor. In other words, multiple processes, as well as pipeline stages, all at different locations in the model's system, can contribute to the same shared statistic. This is done by referring to the statistic by name and obtaining a *statistic handle*.

Figure 5 shows global statistic of WLAN Retransmission Attempts. With retransmission attempt, as a quantitative parameter, the rate of retransmission attempt can be determined.

This parameter also figures out the number of drops per second of the packets which has to be retransmitted. The lower retransmission attempt means more reliable link connection. In other words, this statistic show the number of retransmission attempts during the time the packet is successfully transmitted or when it is discarded as a result of reaching short or long retry limit..

The global statistic of WLAN retransmission attempts is presented when no attack is performed and in cases when 1 or 3 malicious nodes are attacking the simulated wireless network with large number of ICMP ECHO Requests, which means during attack, AP is permanently disturbed by the attacker/s.

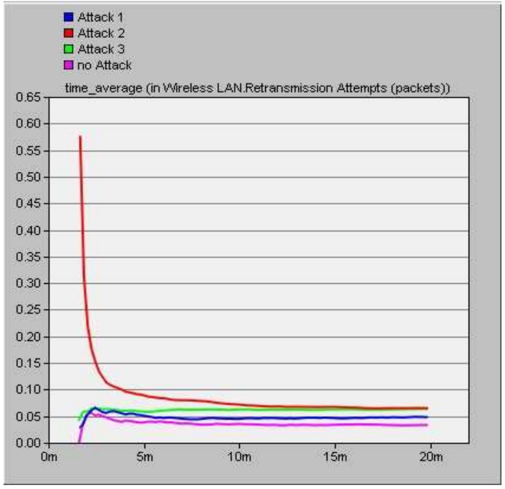


Figure 5. Packets retransmission attempts for different number of attackers and different ping packet size

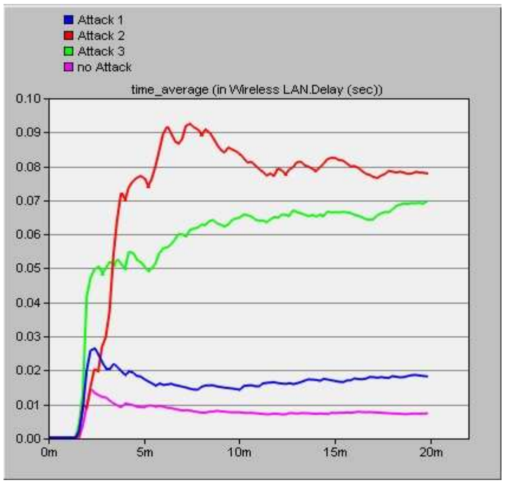


Figure 6. WLAN Delay for different number of attackers and different ping packet size

As it can be seen, increased attackers number is reason for increased number of packets retransmission attempts. It is the same situation when there is only one attacker, but the packet size is increased from 256 to 22000 bytes. It is due to the large size of sent ICMP messages from the attacker/s which causes AP buffer overflow. Once the router is attacked by malicious node problem occurs, the network retransmission attempts dramatically increase, which causes more collisions.

Comparing the results of Attack 2 and Attack 3, it can be seen that although at the beginning Attack 2 causes more retransmission attempts as the simulation run time increases, the effect of these two attacks in the network is becoming equal. It is evident that from the 1020th second of the simulation run time these two curves are almost equal.

Caused collisions are reason for slowing down simulated wireless network which can be seen in Figure 6. This figure shows global statistic of Wireless LAN Delay of all received packets in the network and forwarded to the higher layer as a function of simulation run time.

This parameter is a metric which determines delay between MAC layers. Several phases are included in this parameter: dividing the frames into packets, sending them to their destination and their assembling at their destination MACs. Medium access delay at the source MAC is also included within this statistic. From the obtained results for the delay it is more than obvious that collisions caused by retransmission attempts are reason for this high delay. Situation is almost similar as it was previously explained.

The network performance is reduced due to increased number of received packets form the AP. Again, Attack 2 at the beginning is more destructive and is causing higher WLAN delay compared to the Attack 3. With the simulation run time this delay is going down, and delay caused by Attack 3 is going up.

Very important characteristic when WLAN system is evaluating is Data Dropped metric. Generally, this characteristic shows how WLAN operates when number of users or number of packet is increased (scalability issue). Figure 7 shows relation between data dropped and simulation running time.

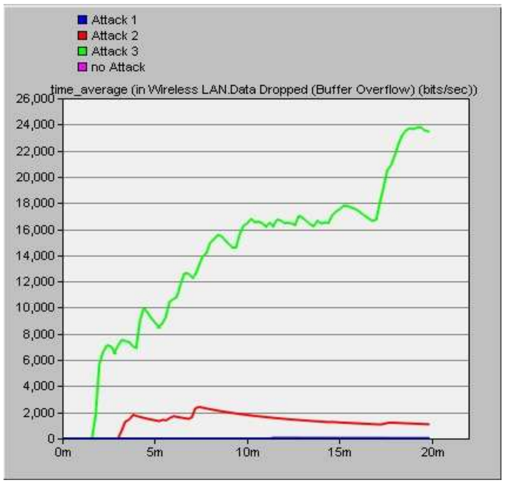


Figure 7. Data dropped for different number of attackers and different ping packet size

Wireless AP is the only one that receives all data traffic (control or data) from the legitimate users and malicious nodes and resends them to their receivers. This AP (in our situation wireless router) acts as a central gateway, so if the AP fails, the connection between users will be lost. The excessive number of packets that is going in or out of AP leads to buffer overflow or traffic jam around it. This excessive buffer overflow leads data packets to be dropped.

The previous is showing that the percentage of data dropped increasing by increased number of malicious nodes or increased number of ping packet size. It is interesting to notice that the number of data dropped is drastically higher during the Attack 3. This is reasonable because this number is directly connected with buffer overflow. It is obvious that the case of Attack 3 will have bigger influence on buffer overflow, which means higher number of data dropped (bit/sec).

Figure 8 is showing the average voice jitters which occur during voice transmission in the situation when no attack is performed and when the wireless network is under the described three attacks.

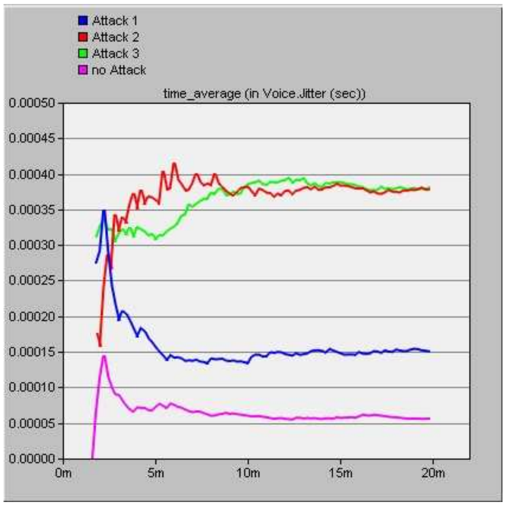


Figure 8. Voice Jitter for different number of attackers and different ping packet size

The jitter values during attacks are dramatically increased. Attack on voice transmission is showing the same characteristics as in previous described situations. At the beginning of simulation, Attack 2 has higher negative influence on the network behavior. During the simulation run time situation is changed, and from 590th second Attack 3 is causing higher voice jitter or higher voice packet delay variation.

Another QoS parameter which we analyzed during simulation is voice packet end-to-end (E2E) delay. E2E delay refers to the average time required the voice packet to be transmitted from the client node to the server. This time is critical, because higher E2E delay will mean higher voice distortion. In the situation when any of previously described attacks is performed, due to AP flooding the queue is a constantly large. Reason for high E2E delay can be more broken links and frequent re-routing during the transmission of the data packet.

The delay in the network must not exceed the threshold value of 80ms to maintain the minimum number of VoIP calls with acceptable quality, which is not situation when the network is under attack. Figure 9 is showing E2E delay statistics of the wireless network.

We have again the same situation – decreasing of the E2E delay with the simulation run time when attack is conducted by three attackers and slightly increasing of this metric when attack by one attacker with larger packet size is conducted.

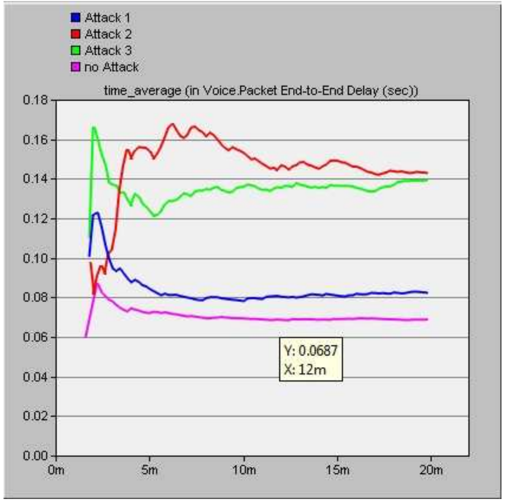
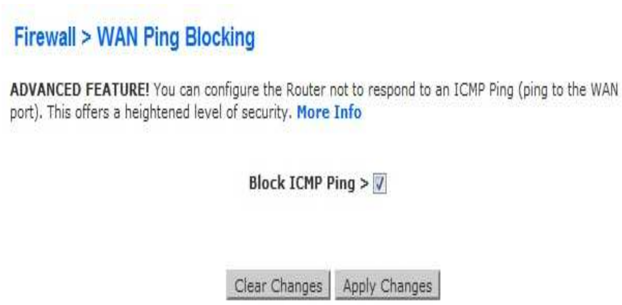


Figure 9. Voice Packet End to End Delay for different number of attackers and different ping packet size

5. Proposed mitigation techniques against ICMP Ping Flood Attack effects

There are several methods to mitigate the effects of this type of attack.

The simplest way of protection from this attack is complete blocking of the ICMP Ping packets, but on the other site this will be very radical solution and there will be problems with servers. If some problem come up it will be difficult to be diagnosed.



Firewall > WAN Ping Blocking

ADVANCED FEATURE! You can configure the Router not to respond to an ICMP Ping (ping to the WAN port). This offers a heightened level of security. **More Info**

Block ICMP Ping > ☑

For example, in Linux, all ICMP packets can be blocked as follows:

```
iptables –p icmp -j DROP
```

However, not all ICMP packets at the firewall should be indiscriminately blocked. Better solution is blocking certain types of packets; otherwise, network performance could suffer. Candidates for blocking are timestamp request and reply, information request and reply, address mask request and reply, and redirect [12].

Other solution is limiting the maximum number or the maximum size of ICMP packets using appropriate threshold. If registered ICMP traffic is greater than the traffic determined by threshold, it will be dropped.

```
ROUTER(CONFIG)# ACCESS-LIST 131 PERMIT ICMP ANY ANY ECHO
ROUTER(CONFIG)# ACCESS-LIST 131 PERMIT ICMP ANY ANY ECHO-REPLY
ROUTER(CONFIG)# INTERFACE ETH0/0
ROUTER(CONFIG-IF)# RATE-LIMIT OUTPUT ACCESS-GROUP 131
16000 8000 8000 CONFORM-ACTION CONTINUE EXCEED-ACTION DROP
```

In previous example, any ICMP ECHO or ECHO REPLY traffic will be allowed until it exceeds 16000 Bytes, at which point it will be dropped.

Also very effective method for reducing the effects of this attack is limiting the speed or frequency of sending ICMP packets from single user (source).

In the previous solutions it is important to determine acceptable value of this threshold. It is important this threshold not to be too low, because if certain ICMP packets are used to “keep-alive” or monitoring the status of a device, low threshold would be a reason the prevention from ICMP Ping flood attack to cause other major problems within the network.

Using OPNET Modeler simulation tool we conducted analysis of several methods to mitigate this type of DoS attack, for the case when the WLAN is attacked by one malicious node using Ping Flood attack with Ping size of 22000 bytes.

Filtering ICMP ECHO REPLY messages resulted in high improvement of the QoS characteristics.

We also considered behavior of different types of firewalls under ICMP Ping Flood attack. The following types of firewall were considered:

- CS PIX 525 8ae adv (CISCO),
- CKP Window Firewall 4e adv,
- CKP Unix Firewall 4e adv.

The Cisco Firewall gave far the best results. The results we got using Windows and Unix Firewalls was also improved but not as the improvement we got using specified Cisco firewall. The improvement we got using Windows and Unix Firewalls were almost the same.

The comparison between Reno and New Reno fast recovery mechanisms during conducted attack also gave a big difference on QoS Parameters. Namely, using of New Reno mechanism as a TCP parameter within wireless network when ICMP Ping Flood attack is conducted is giving much better effects than the case when we used Reno fast recovery mechanism.

5.1 Proposed Failure Recovery mechanism against ICMP Ping Flood Attack

Taking in consideration the same situation (ICMP Ping Flood Attack by one malicious node with ping packet size of 22000 bytes) we are using Link Failure/Recovery mechanism to show its effect on mitigation of this type of attack. The link is recovered during period of 500 to 900 seconds. For better preview, all graphs are showing not the average results as in previous simulation results, but the “*as is*” results generated from OPNET.

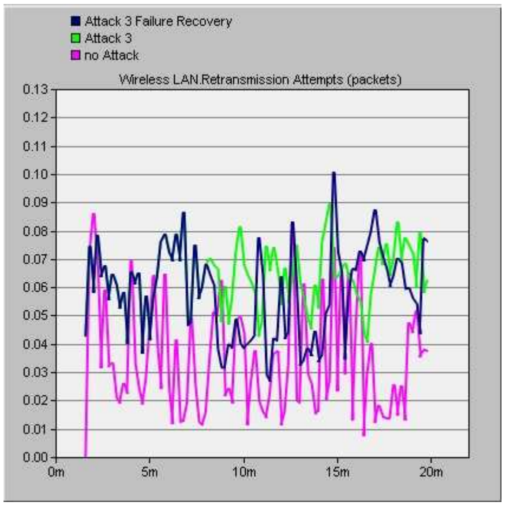


Figure 10. Packets retransmission attempts decreased using proposed Failure/Recovery mechanism

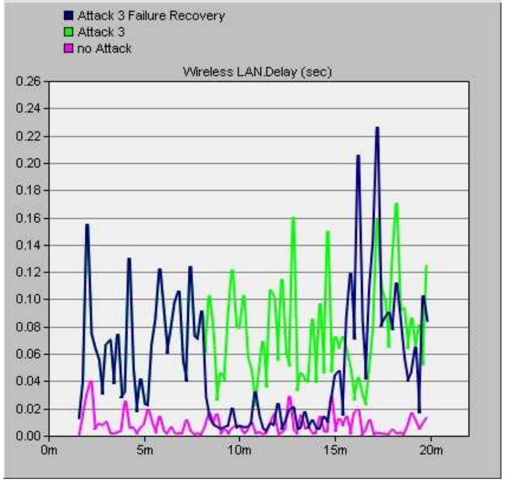


Figure 11. WLAN Delay decreased using proposed Failure/Recovery mechanism

The general goal of failure recovery mechanism is to extend the network lifetime by restarting or reprogramming failed or misbehaving links. In combination, these two measures raise the cost for a potential attacker. Even if an attacker manages to capture a node and abuses it for his own purposes, there is a chance that the aberrant behavior of this node will be detected and the link be recovered, thus nullifying the attack [13].

A good failure recovery mechanism can improve the efficiency and mitigate the DoS vulnerabilities [14].

Figure 10 shows attacked network behavior when failure/recovery mechanism is used. It can be seen that from the period of 500 to 900 seconds when failures are recovered the number of retransmissions attempts is going down.

This will cause the number of collisions to be reduced, so during the same period WLAN delay will be drastically reduced (Figure 11). In this period WLAN Delay will be slightly higher than it is in situation when there is no attack.

By analyzing voice traffic we got similar results which are shown in Figure 13. Namely, jitter caracteristics during this period of link failure recovery of 500 to 900 seconds are slightly higher than they were in case when there is not ICMP Ping Flood Attack

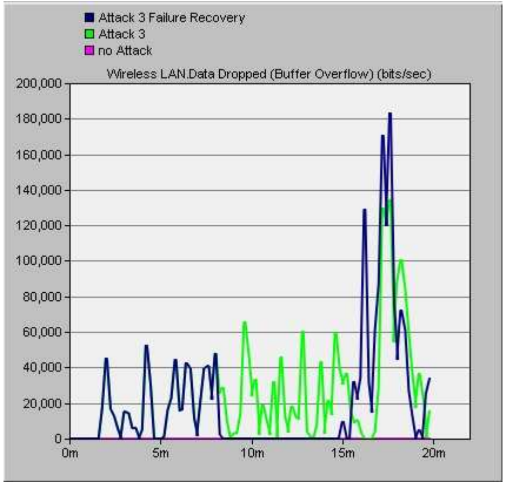


Figure 12. Data Dropped decreased using proposed Failure/Recovery mechanism

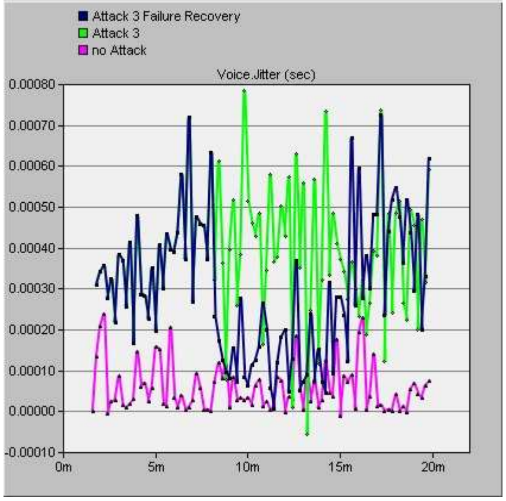


Figure 13. Voice Jitter decreased using proposed Failure/Recovery mechanism

The situation with voice packet end to end delay is the same. End to end characteristics for the period when failure recovery mechanism is used is decreased (Figure 14).

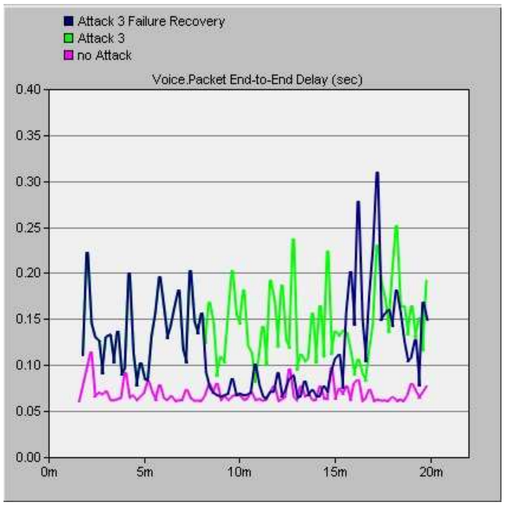


Figure 14. Voice Packet End to End Delay decreased using proposed Failure/Recovery mechanism

As we already explained, the delay in the network during the period of voice transmission must not exceed the threshold value of 80ms to maintain the minimum number of VoIP calls with acceptable quality, which is not situation when the network is under attack and Link Failure/Recovery mechanism is used.

6. Conclusion

In our paper, the effects of the ICMP Ping Flood Attack on the wireless network were explored. More specific, behavior of the wireless networks under attack of different number of attackers and different ping packets size is examined. With the in-depth simulation, we found that the wireless networks QoS parameters can be dramatically reduced under this type of flooding attack. Also, increased number of attackers and packet size has different effect at different WLAN QoS Parameters. Several defence mechanisms against this type of attack were analyzed. In the last section appropriate Link Failure/Recovery Mechanism is proposed and behavior of the attacked wireless network and improvement of QoS parameters under this proposal is shown. During our work we also simulated the same scenarios when appropriate firewall, fast recovery (New Reno) or filtering of specific ICMP ECHO messages is used. In all this situations we got improved results. In the future work, we intend to continue with exploration of possibility for setting optimal threshold for Failure/Recovery mechanism which will activate this mechanism when large number of packets or large sized ICMP packets is received.

References

[1] J. Postel, "Internet Control Message Protocol", STD 5, RFC 792, USC/Information Sciences Institute, September 1981.

[2] Team Cymru, “DDoS Basics”, March 2010.

[3] Y. Fu, X. Wang, “ICMP Processing Module Embedded in NP Based Firewall”, 2nd International Conference on Anti-counterfeiting, Security and Identification, ASID 2008, pp. 310-312, August 2008.

[4] M. Gregg, “Hack the stack: using snort and ethernal to master the 8 layers of an insecured networks”, p.138, November 2006, Syngress publishing.

[5] J.Udhayan, R.Anitha,”Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis”, 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, pp. 558-564, 6-7 March 2009.

[6] F. Gont, “rfc5927: ICMP Attacks against TCP”, Internet Engineering Task Force (IETF), July 2010.

[7] B. Stone-Gross, C. Wilson, K. C. Almeroth, E. M. Belding, H. Zheng, K. Papagiannaki, “Malware in IEEE 802.11 Wireless Networks”, 9th Passive and Active Measurement Conference (PAM), Lecture Notes in Computer Science, Springer Verlag, USA, pp. 222-231, April 2008.

[8] S. Khan, K-K Loo, Z. U. Din, “Cross layer design for routing and security in multi-hop wireless networks,” International Journal of Information Assurance and Security (JIAS), Vol. 4, No. 2, pp. 170-173, June, 2009.

[9] S. Khan, Kok-Keong Loo, “Real-time cross-layer design for large-scale flood detection and attack trace-back mechanism in IEEE 802.11 Wireless Mesh Networks,” Elsevier Network Security, Vol. 2009, Issue 5, pp. 9-16, May, 2009.

[10] Lukasz Tomicki, “Ping Flooding”, 2005.

[11] S. Khan, Noor Mast, Kok-Keong Loo, Ayesha Silahuddin, “Cloned access point detection and prevention mechanism in IEEE 802.11 wireless mesh networks,” International Journal of Information Assurance and Security (JIAS), Vol. 3, No. 4, pp. 257-262, December 2008.

[12] “SUSE Student Manual: Packet Filters, 3058 – SUSE Linux Security”, p. 6-9, 2010.

[13] H. Vogt, M. Ringwald, and M. Strasser, Intrusion detection and failure recovery in sensor nodes, Workshop Proceedings. Lecture Notes in Informatics, Vol. P-68, Gesellschaft für Informatik, Bonn, Germany, pp. 161-163, September 2005.

[14] C. He, “Analysis of security protocols for wireless networks”, A dissertation thesis, Stanford University, p.113, December 2005.