A new model development for efficiency analysis of OS-based smurf attacks

Mina Malekzadeh[#1], Moghis Aashrostaghi[#2]
[#1]Electrical and Computer Faculty of Hakim Sabzevari University, Sabzevar, Iran
[1]m.malekzadeh@hsu.ac.ir
[#2] Mirdamad Institute of Higher Education, Gorgan, Iran
[2] moghis.ashrostaghi@gmail.com

***Abstract*—Lack of accurate and quantitative information related to smurf attack field makes it impossible to measure severity of the attack, quantify success of proposed defenses, and compare their performance. Therefore, development of models capable of quantifying the impact of the attack in simulation and also testbed experiments can lead to development of defenses tools to accurately block the attack. To the best of our knowledge, this work is the first attempt to develop a model to quantify the consequences of the smurf attacks on performance of the wireless networks. Hence, the primary contribution of this work is development of a comprehensive smurf-based attack model. We further investigate the factors that mainly contribute to the amplification of the smurf attack traffics and determine the relation among the original attack traffic, intermediate unprotected network, and the final amplified smurf attack traffic. The model involves a variety of experiments which run against real wireless network testbed in addition to a simulation environment using NS2. The testbed results are compared against the simulation results to verify the validity of the model.**

Keywords-smurf attack, wireless testbed, attack simulation, NS2, cyber attacks, OS

I. INTRODUCTION

The Internet services have become essential part in today's communication infrastructure. Hence, providing security for the systems that apply these services against the cyber attacks becomes a crucial challenging task. It is important to prevent, or otherwise minimize, the damage caused by the attacks exposing the security of the systems on the public Internet. Due to several resource constraints, wireless networks are prone to variety types of attacks. One of the common types of attacks against Internet services utilized by wireless networks is Denial of Service (DoS) attack. Different types of DoS attacks can be classified based on how they affect a victim computer or how they are generated. Thus, based on different criteria, DoS attacks can be classified in different ways [6]. Whether the DoS attacks are conducted directly or indirectly by an intermediate system, is one way to classify these attacks which is shown in Fig1.

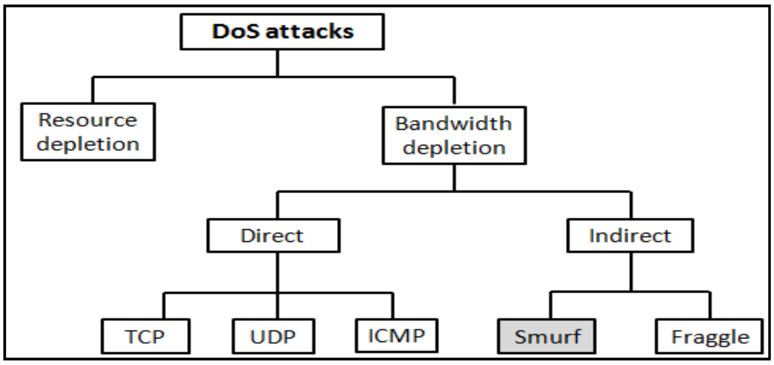


Fig1: Classification of DoS attacks

Based on the above diagram, there are two categories as direct attacks and indirect (reflective) attacks. In the first category, packets are sent directly to the victim. On contrary, in the second category, packets are sent to an intermediate network before hitting the victim [7]. The smurf attack is an example of reflective attack.

The smurf attacks involve both the Internet Protocol (IP) and Internet Control Message Protocol (ICMP). In order to launch this attack, the attackers need to accomplish two steps for the packet crafting. The first step is spoofing which the IP networks are vulnerable to and smurf attack is not possible without it. The attacker creates a forgery echo request packet that appears to originate from the victim system. Then the attackers set destination address as broadcast IP address. After these preparations, the attacker sends the forgery packet to the broadcast address of the target network called an amplifier. The receivers of the forgery packets will send replies with echo responses to the source address which has been set to the target. Repeating the attack will flood the network link of the target [1]. The number of replies depends on the number of machines connected to the amplifier network. Hence, for *n* ICMP echo request messages sent to a broadcast domain, *n x m* ICMP echo reply messages are sent out of the broadcast domain towards the victim computer where *m* is the number of hosts in the broadcast domain [6].

The impact of the smurf attacks can vary from minor instability to serious availability issues to the target systems. Hence, before developing the defenses mechanisms, it is necessary to model the attack and deeply examine different features affecting the attack's severity. Without such models, it is impossible to: (1) quantify severity of various attacks, (2) measure success of the proposed defenses, and (3) compare their performance to determine whether different kinds of countermeasures are implemented correctly.

In this paper we set up a testbed in real world in addition to a simulation framework to model different types of smurf attacks in infrastructure wireless networks. We further investigate the factors that contribute to the amplification of the smurf attack traffics. Based on these factors, a variety types of experiments are designed and implemented under the exact same conditions in both testbed and simulation environment. Finally, the testbed measurements and simulation results are compared to each other to determine validity of the model and findings.

The rest of the paper is organized as follows. Section 2 reviews the related security research conducted by others in the field of smurf attacks. In Section 3 we propose an attack model to conduct the smurf attacks on a real testbed and also a simulation environment. We present and analyze the experimental results in Section 4. The work is concluded in Section 5.

II. Related works

In [1] the author implemented the smurf attack in a testbed against Windows XP and Ubuntu 9 systems. Through some screenshots, transmission of forgery packets related to smurf attack was shown. However, the work did not quantify the impact of the attack in terms of any network performance metric to show the amount of damages caused by the attack.

The authors in [2] described the nature of the smurf attacks and introduced principal component analysis for detecting intrusion. However, the implementation of the model is considered as a future work.

A description of two types of Distributed DoS (DDoS) attacks including Malicious Packet Dropping Based and Flooding Based DDoS attack was provided in [3]. They used GloMoSim as the simulation platform for wireless networks. Number of collisions, energy consumption, and packet delivery ratio were calculated to show the impact of the attack. Based on the results, it was found that flooding based DDoS attacks have great impact on wireless networks. However, smurf attack is not taken into account by them.

Smurf attacks were considered as one of the most common types of DoS attacks by [4]. The work proposed an information-theoretic frame work that models the flooding attacks. Based on this model they generalized the flooding attacks and proposed an attack detection using Honeypots. However, the model did not quantify the severity of the smurf attacks.

In [5] smurf attack under IPv6 was investigated with and without IPSec configuration. They sent multicast ICMPv6 echo response packets with their source address targeting at other IPv6 node. Using Ethereal to capture the subsequent observation on victim and attacker, they found that all nodes received the echo response packets did not respond to the sender even though the source address was not spoofed.

In [6] the author mentioned that conducting a DDoS attack using smurf attacks can be very dangerous for computer systems if not prevented in early stages. They explained that it is possible for a smurf attack to exhaust a very high speed link (such as OC-3, OC-12 or even OC-48 links) by amplifying attack bandwidth. However, there is no implementation of the smurf attack to prove this possibility.

Description of smurf attack as one of the most difficult types of DoS attacks was provided in [7]. They proposed a traceback approach to locate the source of smurf attacks. They developed a specific simulator in order to evaluate the number of packets needed to traceback the attacker. However, the smurf attack was not implemented.

In [8] the authors identified the smurf attack as a nasty type of DDoS attack. The embedded system Single Board computer (SBC) used to ensure security through incorporation of smurf attack detection. However, the impact of the smurf attacks was not measured.

The [9] provided a survey on taxonomy of DDoS attacks, including smurf. A list of the attacks along with the date and name of companies that the attacks conducted against them was provided to emphasize feasibility and severity of the attacks. In [10] they theoretically described the existing methods to perform smurf Attack. However, there is not practical implementation of the attack.

Based on the related works, there have been no prior attempts regarding development of a model to quantify the impact and severity of the smurf attacks on performance of the wireless networks which is the main contribution of this work.

III. Characterize the attack model

Form the viewpoint of the attackers it is highly important to: (1) not be localized and detected by the IDS systems and (2) impose as much damage as they possibly can in one single attack run. Therefore, many considerations are taken into account by them before running the attacks. In this section we characterize the requirements to develop our attack model capable of implementing smurf attacks with variety of attributes. The purpose is to investigate the nature of the attack and the factors that affect its severity.

A. Topology environment

We design two similar wireless network environments as targets that the smurf attacks run against them. One environment is designed using NS2 simulator to simulate smurf attacks and the second environment is a real testbed wireless network to run smurf attacks in real world. The two environments are designed with the exact same specifications to provide adequate fair conditions over comparison of the simulation results and testbed measurements. This comparison enables us to verify the validity of the model and investigate the general effectiveness of smurf attacks. The topology of the victim wireless networks targeted to run smurf attacks in both simulation and testbed is illustrated in Fig2.

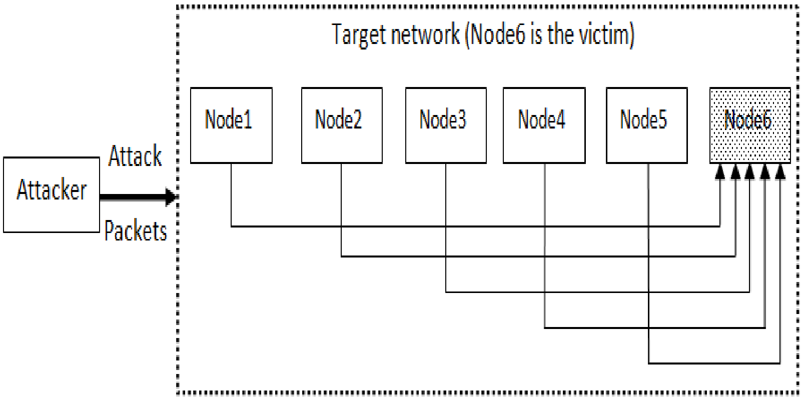


Fig2: Topology of target wireless network as the victim of smurf attack

Based on the above topology, the target wireless network consists of seven potential targets including one wireless access point and six computers. These seven nodes are normally communicating with each other in the wireless network until the attacker launches the smurf attacks against them.

B. Factors affecting smurf attack

In order for our attack model to be capable of implementing variety types of smurf attacks, we need to involve main factor affecting the severity of smurf attack. Therefore, we quantify via simulations and testbed modeling the survivability of wireless networks under smurf attacks as a function of size and rate of the attack packets and moreover the type of victim as follows.

1) Characterize attack packets size (APS): IP networks are based on packets of different sizes either small or big each with their own transmission advantages and disadvantages:

- Smaller packets advantage: cause less delay and if the packet lost, it causes less problem to fix.
- Smaller packets disadvantage: require more bandwidth due to higher packets overhead.
- Bigger packets advantage: transmit more data at once which reduces the bandwidth requirements.
- Bigger packets disadvantage: cause longer delay and more problems to fix if lost.

Therefore, the size of packets can directly affect the network performance. The same goes for the Attack Packets Size (APS) which can vary the impact of the smurf attacks. Hence, the attackers need to create forgery packets with a proper size to achieve their desired malicious intentions. Our attack model considers three distinct APS ranging from small to large as 50B, 100B, and 500B for the size of the smurf attack packets.

2) Characterize the attack rate: When packets reach the destination, they are loaded into memory and wait for their turn to be proceeded. As a result, the more packets are loaded, the more memory is required. Hence, the load rate of attack packets can directly affect the severity of the attacks. In order to investigate the relationship between the smurf attack rate and its severity, our model considers three distinct attack rates ranging from low to high as follows.

- ***Low-rate smurf attack***: in this mode, the attacker provides 0.05s as interval between the attack packets. The purposes of considering such a low rate for the attack packets are to: (1) keep the attack silent and causes the IDS tools cannot detect them and (2) cause the attack traffics to be indistinguishable from the normal traffics.

- ***Moderate-rate smurf attack:*** in this mode, 0.02s intervals are assigned between the attack packets to examine the possible effects and consequences due to growing the density of the attack packets on the target wireless network. The purpose is to determine whether the Windows Firewall (WF), embedded firewalls bulit in antivirus, and also IDS services available on the routers are vulnerable to moderate-size smurf attacks.
- ***High-rate smurf attack***: in this mode, 0.01 second intervals are selected between the attack packets. At such a volume, only the most high end enterprises and DoS service providers stand a chance at successfully mitigating the attack.

3) Type of victim: Generally in real world, networks consist of heterogeneous types of machines that communicate with each other. On the other hand, having different motives in mind, the attackers choose a specific type of target according to their own malicious intentions to fulfill their goals. Considering this fact, we choose different types of targets in our testbed based on the type of the operation system and type of node. Therefore, all the experiments run with the exact same conditions but separately against the following targets.

- ***Windows-based target***: different types of smurf attacks run against Windows 7 32-bit machine to quantify the impact of the attacks and determine survivability level of Windows 7 under the smurf attacks.
- ***Linux Ubuntu-based target***: the same smurf attacks with the exact conditions like Windows7 experiments, run against Linux-based machines having Ubuntu 11 as the OS. The purpose is to compare the possible attack resilience of Linux machines versus Windows machines under the smurf attacks.
- ***Access point-based target***: in an infrastructure mode of wireless networks, all the data transmitted from the source are received by the access point device first before heading the data to the intending destination. This is the access point that decides how and when to send the data. This proves the critical role of the access points in infrastructure wireless networks. Since all traffics have to go through the access point, targeting this device can affect the entire network and thereby clients connecting to that network. For this reason, in addition to targeting a client machine, in our testbed we run the smurf attacks against the wireless access point. This can clear the point for the attackers to whether target a specific client or an access point as the target of the smurf attack to provide the highest devastating effects.

Note that the smurf attacks on specific operation system is only done in our testbed and not in our simulation environment since simulators do not take into account the differences between the type of OS installed on the machines.

C. Characterize legal packets size (LPS)

In order to assess the damage that smurf attacks can cause to wireless networks, we need to quantify the performance of the networks under normal conditions to be compared to those under the smurf attacks. This will point out the performance degradation caused by the attack. Therefore, Legal Packet Size (LPS) is considered 500 bytes which are transmitted during the entire experiments time between the legal users in the target wireless network with 0.02 seconds intervals between them.

D. Material and methods

In order to conduct the smurf attacks against the target wireless networks, some specific tools are required to apply in right way to achieve the desired level of success from the view point of the attackers. This section describes these materials and also the methods to utilize them.

1) Attack tools preparation: To simulate our experiments, we use NS2 network simulator. Moreover, the Xgraph is used to create graphic representations of our simulation results.

In order to implement the same attacks on real world targets, we need some specific hardware and tools to fulfill our goals. These requirements are listed in Table I and Table II.

TABLE I: Hardware used in the testbed

Hardware tool	Description
Wireless access point	Linksys, Asus
Wireless NIC	Netgear, Atheros chipsets
CPU	Intel; i7, dual core
RAM	2GB, 4GB

TABLE II: Software used in the testbed

Software tool	Description
Kali Linux, Metasploit framework, and Nmap	Penetration tool that we use for packet crafting which is prerequisite for launching the smurf attacks.
Wireshark	Network analyzer to examine the network state before, during, and after the smurf attacks.
Firewall	We enable Windows7 Firewall for all Windows machines.
Antivirus	Windows machines are protected with Symantec Endpoint Protection with built-in firewall.
Operating system	Windows7 32-bits/Linux Ubuntu 11

2) *Experiments duration:* The total time for all the experiments is considered 60 seconds which is further divided into three 20 seconds. The first 20 seconds (0-19s) represents the normal operation of the target network without any attack. The second 20 seconds (20-39s) is the attack time. For 20 seconds the attacker's machine runs smurf attacks against the target. The last 20 seconds (40-59s) represents the behavior of the target network while recovering from the attacks.

3) *Performance metrics:* Through implementation of our experiments we quantify the effects and severity of smurf attacks in terms of throughput, end-to-end delay, and packet lost rate as our performance metrics.

Concluding from all the parameters based on characterizing our attack model, nine experiments are developed to implement different types of smurf attacks. These experiments are summarized in Table III.

TABLE III: Nine experiments designed to run different types of smurf attacks

Attack type	Evaluation environment	Target
Light-rate smurf attack	NS2	UDP Agent in 802.11 MAC layer
Moderate-rate smurf attack	NS2	UDP Agent in 802.11 MAC layer
High-rate smurf attack	NS2	UDP Agent in 802.11 MAC layer
Light-rate smurf attack	Testbed	Windows 7
Moderate-rate smurf attack	Testbed	Windows 7
High-rate smurf attack	Testbed	Windows 7
Light-rate smurf attack	Testbed	Linux-Ubuntu
Moderate-rate smurf attack	Testbed	Linux-Ubuntu
High-rate smurf attack	Testbed	Linux-Ubuntu

IV. Testbed and Simulation results

In this section we present the simulation results and testbed measurements obtained from implementation of the nine experiments as follows.

A. Evaluation of low-rate smurf attack in NS2

In this experiment, the six clients are normally communicating with each other through the access point for 20 seconds. After that, the attacker launches the smurf attack against the target. The attack lasts for 20 seconds after which the network attempts to recover from the attack to its normal transmission. The simulation results of this experiment in terms of throughput, delay, and packets lost are presented in Fig3.

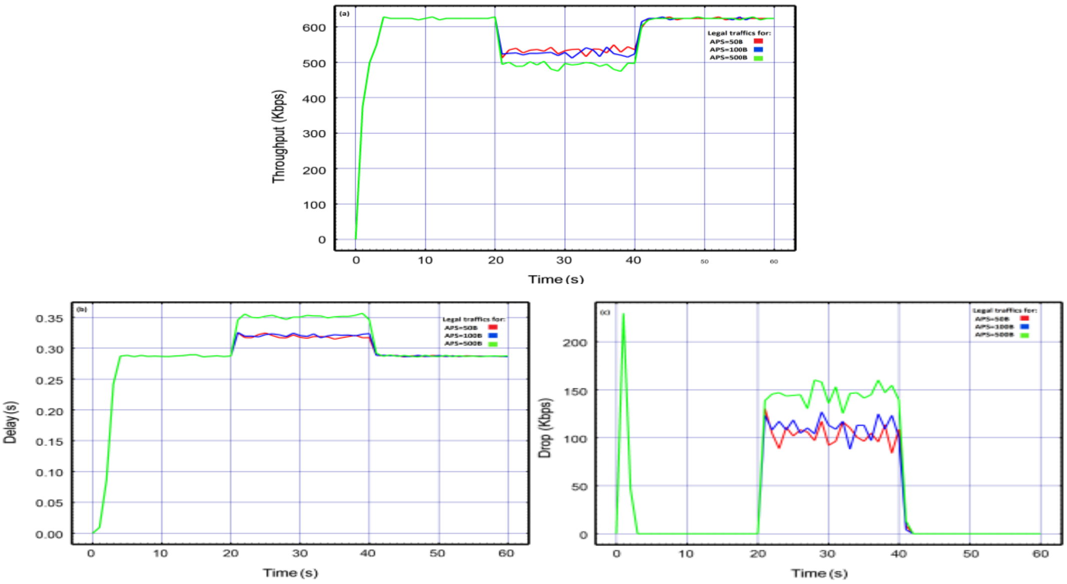


Fig3: Simulation results: (a) throughput, (b) delay, (c) packet lost

The above results represent the direct relationship between the APS and performance degradation of the victim under a low rate smurf attack. The results show that in such a low rate, still the attack is capable of degrading the throughput down to a notable amount. During the attack, the very high increase in the amount of lost packets, about 50% lost, confirms the effectiveness of the attack with even very small efforts from the side of the attacker. Additionally, the results prove the same impact for the 50B and 100B attack packets. The impact of the attack increases as the size of attack packets increase to 500B.

B. *Evaluation of moderate-rate smurf attack in NS2*

The purpose of this experiment is to determine how growing the smurf attack rate to a moderate level can influence the severity of the attack. The simulation results in terms of throughput, delay, and packets lost rate are presented in Fig4.

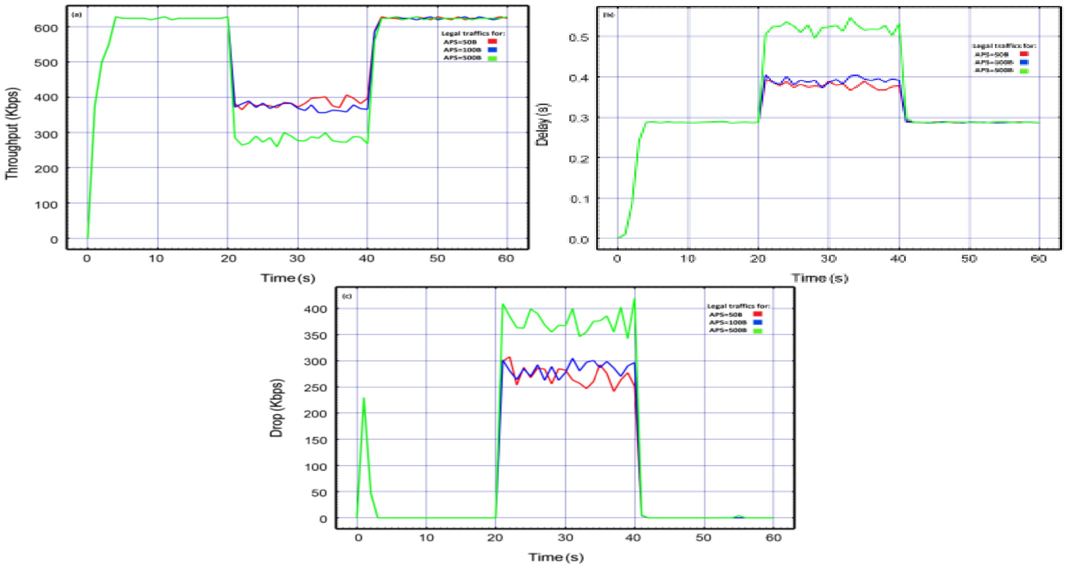


Fig4: Simulation results: (a) throughput, (b) delay, (c) packet lost

As the above results show, a moderate rate smurf attack can significantly disrupt the target's normal operation. During the attack, the throughput degrades from 600Kbps to about 270Kbps in the lowest state which is about one over third of the normal throughput before the attack. In this case, delay correspondingly increases to about twice amount of before the attack. The high peak in the lost packets graph before the attack is related to exchanging high number of control packets by the routing protocols (in our case DSDV) to establish the main route between the users. After that, the number of lost packets is zero until the attack starts. Immediately after starting the attack, losing the packets in target wireless network starts as well. Significant growth from zero to about 400Kbps lost rate implies the devastating impact of the attack even in moderate rate.

C. Evaluation of high-rate smurf attack in NS2

This experiment attempts to increase the smurf attack rate to a higher level compared to the two previous experiments to quantify the possible effects. The simulation results of this experiment in terms of throughput, delay, and packets lost rate are presented in Fig5.

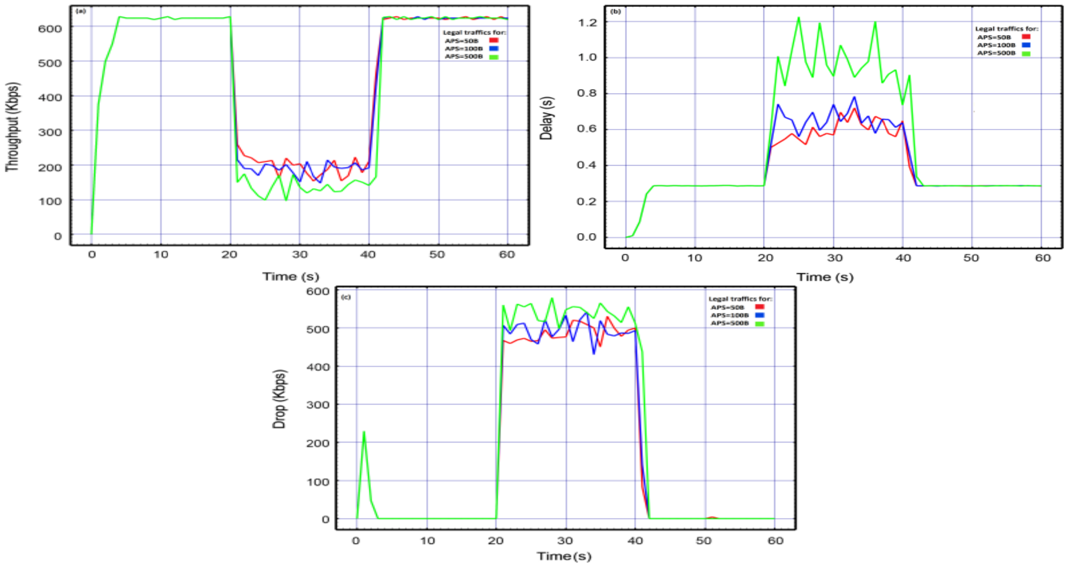


Fig5: Simulation results: (a) throughput, (b) delay, (c) packet lost

The above results signify the high destructive impact of the attack to bring the target to such a low performance that it is almost inaccessible to the other users. From the graphs we can see that for all three APSs, the corresponding impacts are nearly identical. This is unlike our previous experiments at which the larger packets had more impact on degrading the network performance than the smaller packets which is related to higher rate of the attack packets.

D. Evaluation of low-rate smurf attack in testbed against Windows7 target

The last three experiments simulate the smurf attacks in NS2 simulator. Now we are going to use our testbed to launch the exact same attacks against real targets to measure impact of the smurf attacks in real world wireless networks. This experiment runs low rate smurf attacks against real wireless network in our testbed. The target is Windows7 32-bit machine with an installed and updated antivirus while the Windows Firewall (WF) is enabled. The throughput results are provided in Fig6. Additionally, Table IV summarizes the packets lost during the attacks.

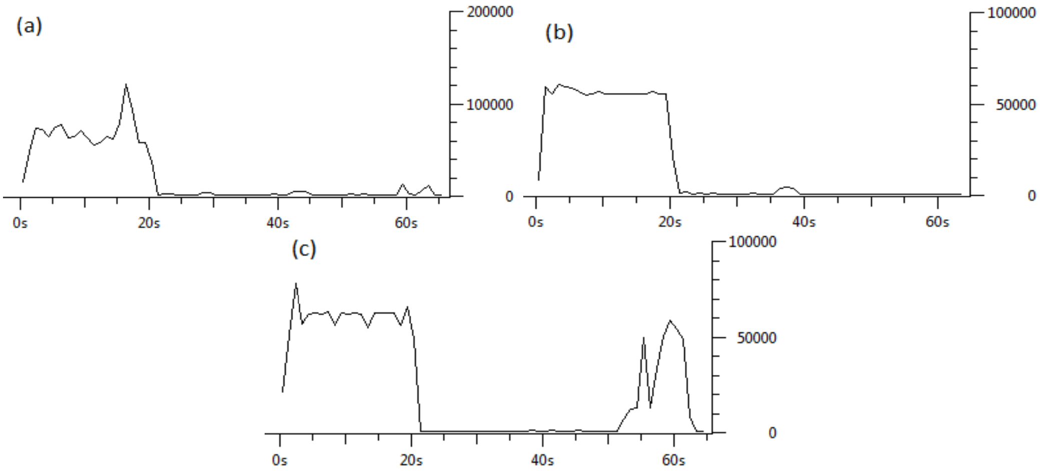


Fig6: Testbed throughput on Windows target for APS equal to: (a) 50B, (b) 100B, (c) 500B

TABLE IV: Packet lost rate during the attack in testbed

Attack packet size	Transmitted	Received	Lost
50	870	9	98
100	823	19	97
500	758	0	100

The above results provide evidence for 100% success rate for the attacker. Regardless of the size of attack packets, the smurf attacks completely shut down the target. The significance of the attack is so high that we did not observe any data transmission not only during the attacks, also for a while after the attacks. The high effect of the attack causes the target suffers even after the attack during recovery. It takes a long time for the target to recover and turn back to the state that it was before the attack. The huge number of lost packets confirms these results in term of remarkable impact of the attack.

E. Evaluation of moderate-rate smurf attack in testbed against Windows7 target

We run the previous experiment against the real target after increasing the attack rate to a moderate level to investigate the possible effects. The target like before is Windows7 machine protected by antivirus and WF. The throughput results are provided in Fig7. Additionally, Table V summarizes the packets lost during the attacks.

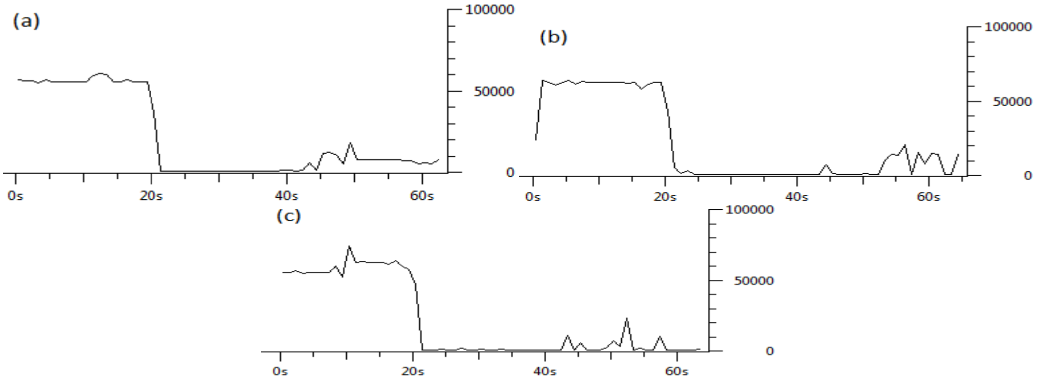
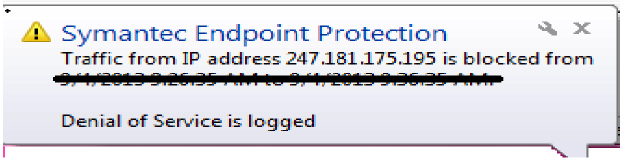


Fig7: Testbed throughput on Windows target for APS equal to: (a) 50B, (b) 100B, (c) 500B

TABLE V: Packet lost rate during the attack in testbed

Attack packet size	Transmitted	Received	Lost
50	814	15	98
100	807	7	99
500	840	8	99

The above results also confirm our previous results in that the attacks entirely render the Windows7 target machine shutdown. Despite protecting by antivirus and WF, the attack even with small 50B packets can completely overwhelm the target and make it unavailable. During the attack we observed the antivirus installed on the target machine can detect the attack and block it. However, despite blocking some of the attack packets, still the attacks easily shut the target down. A screenshot related to blocking of the smurf attacks packets is presented in Fig8.



Symantec Endpoint Protection

Traffic from IP address 247.181.175.195 is blocked from [redacted]

Denial of Service is logged

Fig8: Detection and blocking of the attack packets

F. Evaluation of high-rate smurf attack in testbed against Windows7 target

Although the previous attacks with even low and moderate rate could completely disable the Windows7 target machine, in this experiment we still increase the attack rate to investigate the network behavior particularly after recovery. The purpose is to determine that whether higher rate smurf attack can compel longer time spending on recovery process of the Windows target machines. The throughput results on the protected Windows7 machine are provided in Fig9. Additionally, Table VI summarizes the packets lost during the attacks.

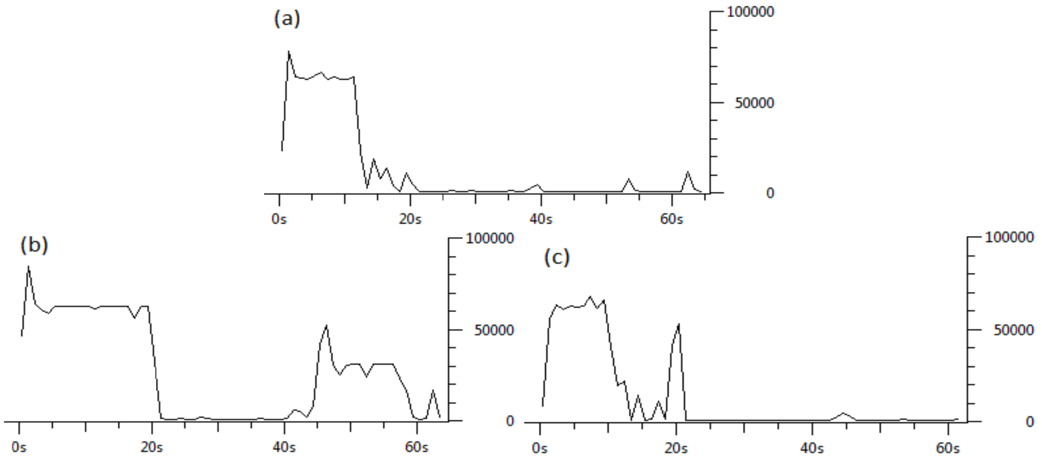


Fig9: Testbed throughput on Windows target for APS equal to: (a) 50B, (b) 100B, (c) 500B

TABLE VI: Packet lost rate during the attack in testbed

Attack packet size	Transmitted	Received	Lost
50	828	10	98
100	813	7	99
500	769	4	99

The results of this experiment reveal that Windows machines are very simple targets for the smurf attacks. Despite being protected by WF and high performance antivirus, still even a lightweight smurf attack (low attack rate with very small attack packets) can bring the machine to a complete halt. The 99% packet lost rate during the attack clearly points out the severe impact of the smurf attacks on the performance of the targets.

We further, changed our target from a Windows7 machine to wireless access point and repeated these experiments. We observed that this time the entire network was shutdown and all the computers were disconnected from the network and became unavailable. The reason is that the attacks successfully render the access point shut down which is a central point of connections for all other clients in the infrastructure wireless networks. When the access point goes down, it causes all the users connected to it to be disconnected from the network which highly extends the impact of the smurf attack.

G. Evaluation of low-rate smurf attack in testbed against Linux target

After having 100% success to shut down the Windows7 machines under different types of smurf attacks, a question is rising up that whether the same attacks on Linux-based targets are as devastating as they are on Windows machines. To answer this question we implement this experiment which runs low-rate smurf attacks against Ubuntu machine as the target. The throughput results are provided in Fig10 along with the packets lost in Table VII.

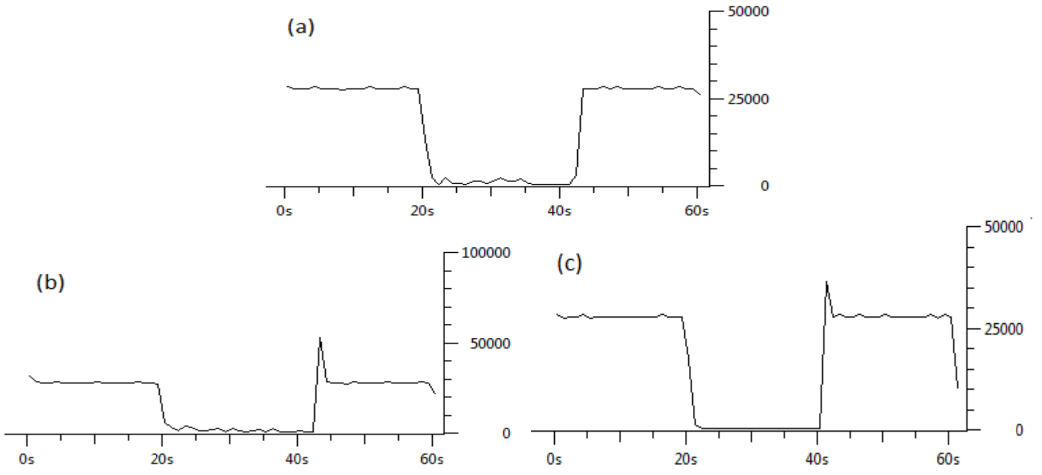


Fig10: Testbed throughput on Linux target for APS equal to: (a) 50B, (b) 100B, (c) 500B

Table VII: Packet lost rate during the attack in testbed

Attack packet size	Transmitted	Received	Lost
50	998	16	98
100	828	16	98
500	616	3	99

The above results point to the same effect of smurf attacks on Linux target as the Windows target on one hand and a different behavior on the other hand. Like when targeting the Windows machine, as soon as the attack starts (at 20th second) the normal operations stop as well. However, as the results clearly indicate, the recovery process is faster and immediate after the attack. We observed that unlike the Windows machine which was suffering from a poor performance for a while after termination of the attack, the Linux target behaves differently. As soon as the attacks stop, the target immediately recovers from the attack and right away becomes available for the other users in the wireless network.

H. Evaluation of moderate-rate smurf attack in testbed against Linux target

This experiment increases the smurf attack rate to a moderate level in order to determine the corresponding effects on performance of Linux-based target. The throughput results of the attack against the Ubuntu machine are presented in Fig11 along with the packets lost in Table VIII.

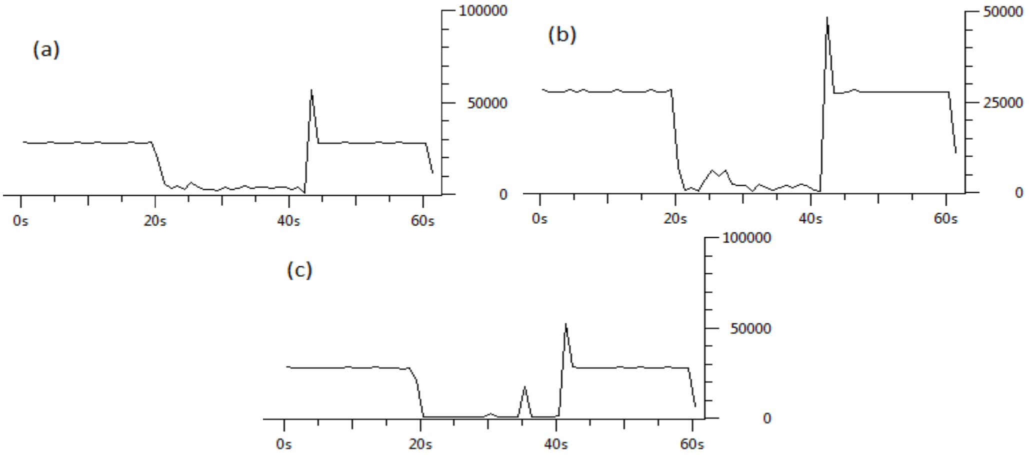


Fig11: Testbed throughput on Linux target for APS equal to: (a) 50B, (b) 100B, (c) 500B

TABLE VIII: Packet lost rate during the attack in testbed

Attack packet size	Transmitted	Received	Lost
50	1000	3	99
100	829	11	98
500	630	3	99

This experiment attains the similar results as the previous experiment. The results imply dramatic performance reduction of the Linux target system. Soon after launching the attacks, they prevent legitimate network traffics and disrupt the connections between the target and the rest of the network. The attacks completely prevent the target from communicating on the network. However, after the attacks stop, the Linux target is capable of resuming the normal operation immediately.

I. Evaluation of high-rate smurf attack in testbed against Linux target

As the last experiment we increase the rate of the smurf attack to see if it has any impact on the performance reduction of the target Linux machine. The throughput results are provided in Fig12 along with the packets lost in Table IX.

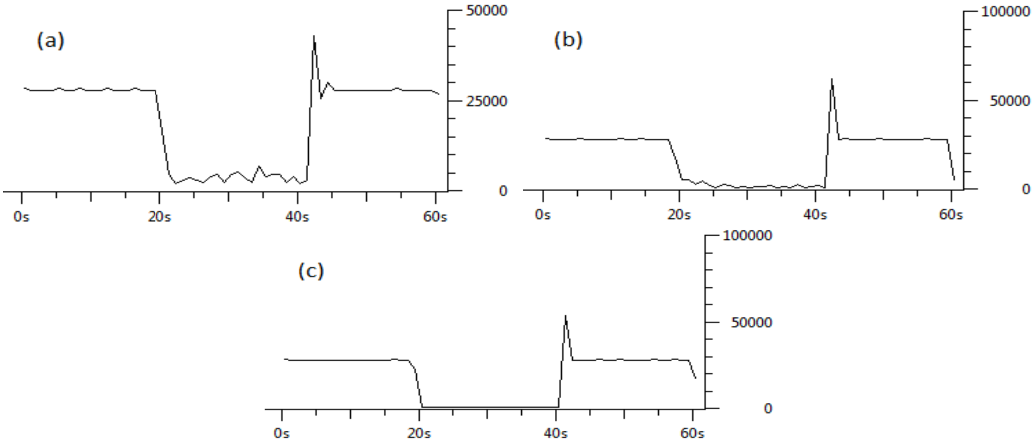


Fig12: Testbed throughput on Linux target for APS equal to: (a) 50B, (b) 100B, (c) 500B

TABLE IX: Packet lost rate during the attack in testbed

Attack packet size	Transmitted	Received	Lost
50	800	27	96
100	866	24	97
500	568	0	100

Based on the results like before, the attacks quickly and effectively cause tremendous disturbance and disable the Linux target machine for the whole attacks duration. The 100% lost rate during the attack for 500B attack packets prove the dramatic severity of the smurf attacks with the specified characteristics.

V. Conclusion

In this work we developed an attack model which is capable to implement variety types of smurf attacks against wireless networks. The results quantify the huge amount of damages caused by the attacks. Based on the results, the attackers can generate very small packets and inject them with very small rate to the targets and in return achieve a huge complete success in term of completely shutting down the target with the least efforts. This in one hand keeps the attack silent so that the attack packets are not distinguishable from the normal packets and on the other hand prevents the attackers from being detected or localized. Comparing the simulation results and testbed measurements signifies the difference between them. While the testbed results imply that regardless of the specified size or rate of attacks packets or type of OS, the smurf attacks are capable of shutting down the target, the simulation results show significant performance reduction but not 100% success to shutdown the target. Our findings and results also point that targets with Windows7 and Linux installed on them are both highly vulnerable to the smurf attacks but Windows7-based machines prove to be highly affected by the attack which will continue for a while after the attack too. In contrast, despite to be completely shut down during the attack, Linux-based machines are capable of recovering from the attack soon after termination of the smurf attacks.

References

[1] H.C. Chaudhari and L.U. Kadam. Wireless Sensor Networks: Security, Attacks and Challenges, International journal of networking, Vol.1, No.1, pp.4-16, 2011.

[2] K. Labib and V.R. Vemuri. Detecting Denial-of-Service and Network Probe Attacks Using Principal Component Analysis, In Proceedings of SAR'04, pp.1-8, 2004.

[3] Y. Chaba, Y. Singh, and P. Aneja. Performance Analysis of Disable IP Broadcast Technique for Prevention of Flooding-Based DDoS Attack in MANET, Journal of Networks, Vol.4, No.3, pp.178-183, 2009.

[4] K.M. Prasad, A.R.M. Reddy, and M.G. Karthik. Flooding attacks to internet threat monitors (itm): modeling and counter measures using botnet and honeypots, International Journal of Computer Science & Information Technology (IJCSIT), Vol.3, No.6, pp.159-172, 2011.

[5] X. Yang, T. Ma, and Y. Shi. Typical DoS/DDoS threats under IPv6, IEEE Proceedings of the International Multi-Conference on Computing in the Global Information Technology (ICCGI'07), pp.1-6, 2007.

[6] S. Kumar. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet, IEEE Second International Conference on Internet Monitoring and Protection (ICIMP'07), pp.1-5, 2007.

[7] H. Guerid, A. Serhrouchni, M. Achemla, and K. Mittig. A Novel Traceback Approach for Direct and Reflected ICMP Attacks, IEEE International Conference Network and Information Systems Security (SAR-SSI), pp.1-5, 2011.

[8] N. Ahmed, Z.I.A. Khalib, R.B. Ahmad, S. Sudin, S. Asi, and Y. Laalaoui. Low-End Embedded Linux Platform for Network Security Application – Smurf Based Attack Detection, International Journal of Computer Science and Network Security (IJCSNS), Vol.8, No.11, pp.1-7, 2008.

[9] C.M. Pate and V.H. Borisagar. Survey On Taxonomy Of DDoS Attacks With Impact And Mitigation Techniques, International Journal of Engineering Research & Technology (IJERT), Vol.1, No.9, pp.1-8, 2012.

[10] K. Choudhary, Meenakshi, and Shilpa. Smurf Attacks: Attacks using ICMP, International Journal of Computer Science and Technology (IJCST), Vol.2, No.1, pp.75-77, 2011.