ABSTRACT

Wireless mobile nodes have extremely limited resources and are easily vulnerable to Denial of Service (DoS) attacks. The traditional techniques that can detect or prevent DoS attacks in wired networks often require considerable resources such as processing power, memory, and storage space. Hence, it is not possible to deploy the traditional techniques on the wireless nodes. In this paper, we identify the requirements and challenges that are to be addressed in order to efficiently deal with DoS attacks on wireless nodes. Then we consider a general architecture for different types of wireless networks and propose a framework to counteract DoS attacks in the general architecture. We will also present the simulation results of our approach and directions for the future work.

1 INTRODUCTION

Today, network operators and service providers are working [1, 2] on the convergence of wired, wireless and cellular networks with the aim to provide additional services with seamless and uninterrupted access to the end users. It is believed that IP [3, 4] will be the predominant protocol that will be used for communication in next generation networks. Also, end users will be extensively making use of wireless mobile devices for communication. The wireless devices have limited resources and are vulnerable to several attacks. In particular, these wireless mobile devices are easily vulnerable to Denial of Service attacks.

Denial of Service (DoS) [5] is an attempt by the attacker to consume the resources of the victim machine and thereby prevent the victim machine from accessing or providing any services. In the case of DDoS [6, 7], the attacker compromises several hosts in the Internet and uses these machines to launch a coordinated attack on the victim machine. Recently, viruses and worms are actively being used [8] to generate DDoS attacks in the Internet.

Traditional security tools like firewalls and intrusion detection systems that can detect and prevent the DoS attack often require considerable resources such as processing power, memory, and storage space. In addition, there are several limitations for the recently proposed techniques such as filtering [9], IP Traceback [10, 11], logging [12], ACC routers [13], and automated model [14] to be applied to counteract DoS attacks in wireless networks. In this paper we consider a general architecture for different types of wireless network and propose a framework to counteract DoS attacks in the identified architecture.

The paper is organized as follows. Section 2 gives a detail discussion on the requirements and challenges for a robust DoS solution. In Section 3, we consider a general architecture for different types of wireless networks and propose a framework to deal with the DoS attacks in the identified architecture. Section 4 describes the simulation results and Section 5 presents a general discussion on the advantages, limitations, and directions for future work. Section 6 concludes.

2 REQUIREMENTS AND CHALLENGES

Let us discuss some of the requirements to efficiently counteract DoS attack on wireless nodes:

- Since wireless nodes have limited resources, the attacker can easily perform DoS attack on these devices by draining their resources. Hence the proposed techniques should quickly detect the DoS attack on the wireless mobile nodes and prevent the attack traffic.
- The attack traffic can be generated by multiple sources. In addition, the convergence of networks enables the attacker to generate attack traffic on the wireless mobile nodes from hosts that are connected to wired networks (which have considerable resources at their end). The attack traffic can consume all the bandwidth available at the victim node. Hence the proposed techniques should prevent the attack traffic at a point that is nearest to the source of attack.
- The attack traffic can be generated with spoofed source address. Hence it becomes extremely difficult to identify approximate source of attack and apply filters nearest to the source of attack. Also, this becomes difficult to identify attack signatures. Attack signature is a pattern of traffic that can be used to differentiate malicious traffic from legitimate traffic. Hence the proposed
technique should be capable of identifying the approximate spoofed source of attack.

- Attacker can generate the attack traffic from wireless mobile nodes by continuously changing his location. This also shows the importance for the need of efficient traceback techniques with fast response time.

Some of the challenges that are to be addressed in developing a robust solution are as follows:

Security tools like firewalls [15, 16] and intrusion detection systems [17, 18] are to be deployed on the nodes to detect the DoS attacks. In general, these tools are deployed at the network boundary or on all devices that are to be monitored for any suspicious behavior. The tools identify the attack signatures by matching with the stored attack patterns or based on anomaly detection. Currently, there are several hundreds of known attack signatures. Hence all the traffic should be matched with the attack patterns to detect any suspicious patterns. Hence, it requires considerable resources such as processing power, memory and storage space to deploy these tools. Wireless and mobile nodes have extremely limited resources. So, it is not possible to deploy traditional security techniques like firewalls intruder detection systems on the wireless mobile nodes. Hence the end users may not even be aware that their system is experiencing DoS attack.

The recently proposed IP traceback techniques require considerable number of attack packets to be received at the victim end to traceback the approximate source of attack. Also, since each marked packet represents only a sample of the path it has traversed, it requires considerable processing power to trace the path.

The ACC routers can identify the attack signatures even for zero day attacks (attacks that are previously not known) by identifying the similarities between the suspicious packets. However this technique requires considerable number of attack packets to be received in order to identify the similarities in the attack traffic. The main disadvantage with this technique is that the nodes are not capable of differentiating between benign and malicious traffic.

The logging techniques and automated model can efficiently trace back the attacking source. But the main disadvantage is that these techniques require the victim to deploy advanced security tools at its end.

Hence most of the recently proposed techniques first require the victim to differentiate between benign and malicious packets before any process can be initiated.

3 FRAMEWORK FOR DEFENDING AGAINST DoS ATTACKS

Let us first consider a general architecture for different types of wireless networks and then discuss the framework for defending against DoS attacks.

3.1 General Architecture for Wireless Networks

We consider an architecture that is similar to the automated model [14]. Figure 1 shows a general architecture for different types of wireless networks. In the case of Wireless LAN, wireless nodes can access the services through the access points. The access points can be part of the LAN and connected to routers to access the Internet. In some case, the access point itself has the functionality of routers and can access the Internet directly.

In the case of cellular network, the mobile nodes can access the services through the base station. The base stations access the Internet by connecting to base station controllers. The base stations are connected to the base station controller through a wired or wireless media. In some cases the base station and base station controller functionality is available at a single location. Similarly in some architectures of ad hoc and sensor network, the nodes can access the services through the cluster head or base station. The cluster head or the base station can be connected to other networks through wired or wireless medium. Hence it is clear that although there are some peculiarities for each type of wireless network, they have almost similar architecture.

Figure 1: General Wireless Network Architecture
The architectures can slightly vary in real time. For example multiple access points can be connected to a router. In case of cellular network, several base stations can be connected to a single base station controller. Also, there are several different architectures for ad hoc and sensor networks.

For simple presentation of our framework, let us further simplify the architecture in Figure 1 by representing the access points, base stations and clusters heads as base stations. Also, let us assume that all these base stations belong to a single provider. The simplified final architecture is shown in Figure 2. In Figure 2, the end users can access the services through their wireless mobile devices by connecting to the base stations (BS). The base stations are connected to other base stations through a wired medium (routers). Also, the service providers has a connection to other service providers through the router R2. Now let us discuss how DoS attacks can be prevented in the architecture shown in Figure 2.

3.2 Attack Scenario

In this paper, we do not consider jamming attacks and DoS attacks that are generated on the victim node by neighboring devices. Techniques such as frequency hopping, and fellowship [19] can be used to defend against DoS attacks from neighbouring networks.

We consider attacks where the attack traffic originates outside the autonomous systems (AS), passes through one or more base stations of the AS and targets the victim node which is outside the AS domain. In Figure 3, the dotted lines show the direction of attack traffic. The base station through which the attack traffic enters the AS domain is called ingress base station and the base station through which the attack traffic exits the AS is called egress base station. Our aim is to prevent the attack traffic at the ingress base station.

In Figure 3, $Atn$ represents total attack traffic generated by several attacking sources and $Gn$ represents good traffic to the victim node passing through a particular base station. Our aim is to identify and eliminate attack traffic to the victim node passing through a particular base station. ($At1$ at BS1, and $At2$ at BS2). We consider that the attack traffic has following properties. Attack traffic can be generated with spoofed source address. More than one attacking source may be involved in the generation of the attack traffic. The attacking sources can be mobile and can continuously change their location. The owners of the attacking sources may not be aware that their device is being used to generate attack.

3.3 Our Approach

Our architecture involves a Controller-Agent model. In each Autonomous System, we envisage that there exists a controller, which is a trusted entity within the domain and is involved in the management of denial of service attacks. In principle, the controller can be implemented on a router or base station or at a dedicated host. In Figure 3, the controller is assumed to be implemented on a dedicated host and connected to all the routers and base stations through router R1. The agents are implemented on all the base stations. The controller maintains the
topology of its network and has information about all the agents that are present in the domain. An agent has the information of its domain controller only. Both the controller and agents are designed to handle the attacks on multiple victims simultaneously. To simplify the presentation of our approach, we consider a simple scenario. Before discussing the operation of the model, let us first discuss some of the assumptions:

- All the communication is through IPv4 [3] or through IPv6 [4] protocol.
- The base stations can monitor the traffic that is destined to the mobile nodes and identify the intrusions. Some of the currently available base stations are capable of identifying and preventing the suspicious traffic. Alternatively, the technique discussed by Mahajan et. al [13] can be deployed on the base stations to identify the attack signatures.
- The controller is always available and the base stations or the internal routers are not compromised. If base station or internal routers are compromised, then the attacker can generate much severe threats. In general, the service provides employ security professional and deploy some security tools to monitor and prevent any suspicious activity on its devices.
- The communication between the controller and its agents is protected. Most of the currently available tools have this functionality.
- We define attacking source as the nodes that are connected to the base station of the AS. In case of attack traffic originating in upstream domain, then we consider attack host as the upstream service provider router or base station.

3.4 Operation

The agents (base stations) monitor the traffic that is destined to its wireless nodes. The agents identify and prevent any suspicious traffic from reaching the wireless nodes. If the bandwidth consumed by attack traffic reaches a particular threshold or if the attack persists for a longer time, then the agent sends a request to its controller to prevent the attack upstream. A session is established between the agent (victim’s base station) and the controller after proper authentication between them. The controller generates and issues a unique ID to each of its agents and commands them to mark the traffic that is destined to victim node. The controller updates the victim base station with the valid ID’s. The agents filter the traffic that is destined to the victim and marks the packets with the unique ID in the fragment ID field of IP packet [3]. All the packets that are fragments and all the packets that are marked by an attacker will be dropped in this stage. If the ingress agent receives a packet that is not marked in the fragment ID field, then it marks the packet with the unique ID. If the ingress agent receives a packet that is already marked in the fragment ID field, then it drops the packet since the packet could be a valid fragment or it could be marked by an attacker. Since agents are deployed on all the edge routers, all the traffic to the victim is marked with the ingress agent unique ID. Though the source address of the attack traffic is spoofed, for example in Figure 3, all the attack traffic At1 will have similar ID of BS1 in the fragment ID field. Since the controller has already updated the victim with valid ID’s, this enables the victim base station to identify different attack signatures for different attacking sources (At1 for BS1 and At2 for BS2). The victim base station updates the controller with different attack signatures based on the unique ID. The controller retrieves the 32-bit IP address of the agent from its database based on unique ID and commands that particular agent to prevent the attack traffic from reaching the victim. Since attack signatures are identified based on the unique ID, only the agents through which the attack traffic is passing (BS1 and BS2) will receive this command. Now all the agents that receive this command will start preventing the attack traffic from reaching the victim. The traffic that is matching with the attack signature will be dropped and logged at the agent. The traffic that is not matching with the attack signature is marked with the unique ID and destined to the victim. This enables the victim base station to easily track the changes in the attack traffic pattern. Also, this enables the victim base station to efficiently deal with the attacks even if the attacker generates the attack traffic by changing his location. In figure 3, since the packets are marked even if the traffic is not matching with the attack signature, the victim base station can easily detect and respond if the attacker changes his location from BS2 to BS3. The agents update the controller at regular intervals on how much attack traffic the agents are still receiving. Packet marking and prevention process will be done until the agent receives a reset signal from its controller. However the victim base station can request the controller to continue the packet marking process for an excess amount of time. This is very useful for intermittent type of attacks where attacking systems do not flood the victim continuously but send attack traffic at regular intervals.
We have conducted ns2 [20] simulations to test the performance of our model. The tests were performed on 2.2 GHz CPU running Red Hat Linux server with 512 MB RAM. The simulations were performed for by considering the scenario as shown in Figure 3.

The agents are implemented on each of the base station. The base stations monitor the mobile nodes traffic for any suspicious behaviour. The agent (base station) that is connected to the victim node sends a request to the controller to invoke the model when the suspicious traffic to the victim reaches a threshold of 100 packets. The controller issues a unique ID to all the agents and commands them to mark the traffic that is destined to the victim node. After packet marking is invoked, the agent that is connected to the victim node identifies attack signature for each agent and requests the controller to prevent the attack traffic at the identified agent. Figure 3 shows the results of our simulation.

Figure 3a shows the operation of our model. The solid line indicates the bad traffic received at victim base station. It starts with a sharp growth in the number of bad packets received due to the threshold limit and the time taken to invoke the model. The dashed lines represent attack packets dropped at the ingress base stations. The model is invoked when the attack traffic received at the victim base station reaches a threshold value of 100 attack packets. The rise in solid line indicates the total time taken for packet marking and dropping of the attack packets at different base stations.

At 20.0 seconds, the attack packets received at the victim base station starts increasing. This is because the malicious wireless nodes change their location and start generating the attack traffic from a different base station. The packet marking enables the victim base station to detect these changes, identify new attack signature and request the controller to prevent the attack traffic at the new base station. The total combination repeats recursively on receipt of a new bad signature. For every 10 seconds feedback messages from Routers are sent to the Controller indicating number of dropped packets in that interval.

Figure 3b shows the response time for different number of base stations by varying the number of attacking nodes connected to each base station. The response time is linearly dependent on the number of base stations.
5 DISCUSSION

The simulation results confirm that our model has several features to deal with DoS attacks in the general wireless architecture. There are several advantages with our model. The architecture of the some of the Network Management [21] tools and Network Intrusion Detection systems is similar to our model/framework. Hence our model can be easily integrated with the existing tools. Furthermore, there are some Intrusion Detection Systems that can identify the attack signature based on any filed in the IP packet header.

However there are several additional challenges that are to be addressed. Let us discuss some of the issues that are to be addressed in the future work.

We have only considered the case where attacking nodes are moving. We have to consider the case where the victim node is also mobile. In this case, when the victim node connects to a new base station, the old base station should transfer the attack signatures to the new base station. Alternatively, the new base station to which the victim node is connected should initiate the prevention process.

We have only considered prevention of DoS attack in an autonomous system. However the attack traffic can be originating from other autonomous system. There is need to extend this framework for multiple Autonomous Systems.

There are only 16-bit in the fragment-id field of IP packet. So the model can only be implemented where the total number of agents is less than 65535 agents. However in IP v6 the 24-bit flow label field [22] can be used for this purpose.

6 CONCLUSION

We have presented a detailed analysis of the requirements and challenges in order to efficiently deal with DoS attacks in emerging wireless networks. Then we have considered a general architecture for different types of networks and proposed a framework to deal with the DoS attacks in the identified architecture. We have tested the performance analysis of our model by performing simulations in NS2. The results confirm that our model has very fast response time, can deal with attack traffic that is generated with spoofed source address, can prevent the attack traffic nearest to the source of attack, has low overhead. We have also presented a detailed discussion on the limitations of our model and the directions for further work.

BIBLIOGRAPHICAL REFERENCES


