IST-152 Workshop on Intelligent Autonomous Agents for Cyber Defense and Resilience

Distributed Attenuation Agents for Mitigation of DDoS Attack

PRIMARY AUTHOR: Hugh Harney, Co-Authors: Kevin Andrea, Robert Simon

Axiom Inc.
6716 Alexander Bell Dr, Suite 220
Columbia, MD, 21046
Tel: 443-540-6153
hh@axiom-inc.com

Dept. of Computer Science
George Mason University
Fairfax, Virginia 22030
kandrea@masonlive.gmu.edu
simon@gmu.edu

Multicast protocols are particularly vulnerable to Distributed Denial of Service (DDoS) attacks today. Distributed Attenuation Agents for Mitigation of DDoS Attack applies group cryptographic key management properties to a Group ID used for packet delivery. The result creates a distributed network of routers that enforce a simple coordinated multicast routing policy that attenuates DDoS attacks. In effect, each routing element (traditional routers and mobile platforms) becomes a gateway agent. We demonstrate the distributed enforcement of this simple routing policy results in the attenuation of DDoS attacks.

DDoS attacks serve to diminish the ability of the network to perform its intended function over time. For an adversary to succeed with a DDoS attack, they need to rely on the network state and device configurations to remain static throughout their period of observation. Moving Target Defense (MTD) techniques upset this paradigm by inducing unpredictable changes on the attack surface of a network, mitigating the efficacy of an attack by limiting exposure of vulnerabilities and increasing the cost of an attack. For DDoS efficacy, multiple devices in a botnet need to receive coordination prior to engaging in their attack; MTD further limits this as an option as the attack vulnerabilities will be of limited duration prior to a configuration change.

DDoS Resistant Multicast (DRM) is a technique wherein the concepts of MTD can be used to secure multicast traffic on a network from DDoS attacks. The primary DRM principle has universal applicability on heterogeneous implementations and in mitigating the efficacy of DDoS attacks against a network. This principle is that of address agility: the rotation of the valid address for the network resource. This agility relies on a code embedded within the multicast address that each receiving router checks for validity.

This construct hardens the communications channels of a device or network resource by rotating its valid address frequently. Any attacker attempting to send hostile traffic across the network using an invalid or expired address would have their messages filtered and dropped, closing off any vulnerable channels from attacks. While this construct can be used generally, this is particularly useful within the spectrum of multicast, whereby any router upon receiving an attacking message would not only reject its payload, but would also refuse to forward the message, thereby protecting the rest of the network.

The address agility scheme rotates the multicast Group ID carried in the addresses, using an embedded code that is generated by a shared group key. The group key can be superseded by a new key from a trusted authority at any point, changing the address; this is designed to mitigate replay attacks. This scheme provides a means for networked systems to filter out improper or out of sync messages, providing an asymmetric advantage to the defender over the adversary.

The address agility scheme relies on a group cryptographic key shared by all participating group members. The secure distribution and management of grouped cryptographic keys is a solved topic with IETF standards describing the process. The Group Secure Association Key Management Protocol (GSAKMP) provides a distributed key dissemination architecture and advanced group key management processes for managing a secure group.

There are several group cryptographic key management techniques that enable interesting properties when those group keys are used to extend the Group ID. The most obvious is synchronization of the embedded code section of the Group ID. Group cryptographic keys have multiple methods to ensure group synchronization that include distributed coordinated group key policy, distributed delegated group controllers, cryptographic rollover, coordinated key lifespans, and finally, binary key trees to perform group membership management.

When these group cryptographic properties are applied to the Group ID space, the traditional domain for Software Defined Networks (SDN) is expanded to include distributed routers and mobile endpoints. The multicast distribution network achieves the properties of autonomous malware filtering gateways, where each router and mobile node only route multicast packets that possess a valid Group ID. This property results in an attenuation of malware packets that are “out of sync” with the underlying group key. Moreover, because the group key is distributed in a secure manner, an adversary has little chance of randomly determining a future valid Group ID.

Evaluation of DRM was performed on the George Mason University Hydra cluster. This cluster employed 13 physical servers, with six configured as DRM routers and seven as clients, forming the topology depicted in Figure 1. The Packet Delivery Rate (PDR) was measured for variations in both window duration and epoch size. Each of the seven clients generated 100 packets with a packet generation rate of one per 503ms. For each test, clients from among this set of seven would disconnect and reconnect periodically at random intervals to ensure the randomness of the client-router synchronization.

Figure 2 below shows the average results of different packet delivery distances for the variations in both epoch size and window duration. ANOVA analysis performed on these results showed that the window duration was statistically insignificant, implying that epoch size was the significant factor that affected the delivery ratios and the window sizes were large enough to accommodate the 5-hop network, even with an epoch size set

to three.

Following this evaluation, we introduced an adversary to the network, which began replaying a message at a rate of one packet per 20ms, which is greater than a full order of

Fig. 1. DRM Evaluation Topology

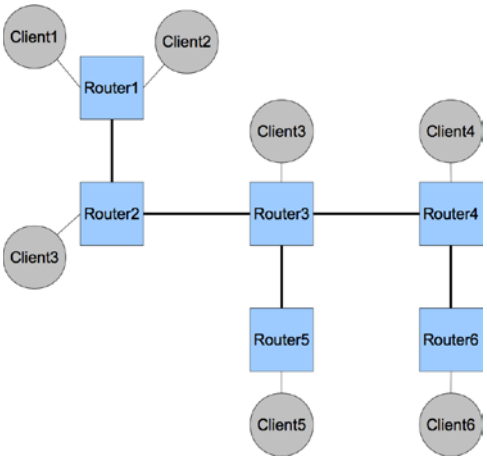

Fig. 2. DRM Evaluation Results[1]

Epoch size	Window (ms)	1-hop delivery ratio	2-hop delivery ratio	3-hop delivery ratio	4-hop delivery ratio	5-hop delivery ratio
3	200	91.03*	88.76*	69.23*	66.03*	61.622*
3	250	92.3636*	90.73*	83.70*	82.65*	82.45*
3	400	91.48*	78.5*	85.88*	79.15*	59.14*
3	500	90.19	75.91*	73.85*	77.09*	70.76*
3	1000	100	77.65*	80.40*	80.95*	83.40*
5	200	100	99.99	99.81	98.52	96.11
5	300	99.97	99.98	99.98	99.96	95.45
7	200	100	100	100	100	100

[1]The table entries marked with an * exhibited large degrees of variance.

magnitude faster than the normal system traffic. This attack was performed at the most stable system configuration with an epoch size of 7 and a window of 200ms. The experiment resulted in the DRM network stopping all propagation of adversary packets after the 1400ms attacking window had expired, protecting the network from further damage by the adversary network while packet delivery ratio was 100%.

The current research base is focused on smaller IoT networks; however, research is not moving toward larger internet size simulations. The initial results show a high degree of resilience to DDoS attacks from current threats. This work demonstrates how MTD concepts can be applied to the larger Internet in a way that forces the complexity of a DDoS attack above the current level of attacker sophistication.