Finding DDoS Attack Sources:
Searchlight Localization Algorithm for Network Tomography

Omer Demir
Department of Information Technology
Turkish National Police, General Directorate of Security
Ankara, Turkiye
Email: omerdemirkos@gmail.com

Bilal Khan
Department of Mathematics & Computer Science
John Jay College, CUNY
NewYork, USA
Email: bkhan@jjay.cuny.edu

***Abstract*—Among the challenges facing the Internet, DoS/DDoS are a critical concern for Internet Service Providers. DDoS attacks can cause country-wide infrastructure problems, and can disrupt communications on a national level. Frequently, Botnets are used to carry out source-spoofed DDoS attacks. The problem of tracing such attacks has been the subject of significant inquiry.**

Here, we leverage the fact that a Botnet requires significant exposure to risk, and investments of time and resources. Thus, as a capital resource, it is likely that a Botnet will, over its lifespan, be used to execute *multiple* criminal DDoS attacks on different targets. Here, we report on new techniques that leverage information obtained over *sequences* of source spoofed Botnet-led DDoS attacks, demonstrating the efficacy of these techniques at pinpointing potential attacker locations.

DDoS attack flow descriptions can be collected in many ways, using a coordinated DDoS sensor agents (e.g. as described by the authors previously in [1]). Here, as a theoretical contribution, we provide formal statement of the attacker localization problem. We develop an new algorithm for localizing attack sources from sequences of DDoS attacks.

***Index Terms*—DDoS; source localization; source spoofing.**

I. Background

Denial of service (DoS) occurs when legitimate users are prevented from getting access to shared resources or services [2]. When a DoS attack is mounted concurrently from large numbers of distributed sources, it is called a Distributed Denial-of-service (DDoS) attack. Although DoS/DDoS attacks are just one of many challenges facing the Internet, they have been identified as a critical concern by Internet Service Providers (ISPs), see e.g. Arbor Networks survey [3].

The damage caused by DDoS attacks can vary in scale, ranging from specific to widespread. Attacks can cause country-wide infrastructure problems which can disrupt communications on a national level. A recent example of an attack at this scale was seen on June 25th 2008, when Radio New Zealand International reported that an attack on the National Telecommunications Authority–the monopoly Internet provider of Marshall Island–caused a complete shutdown of email traffic to the country for a week [4]. Attack dynamics frequently cross national boundaries. One such case included the web site of Rapid Satellite of Miami, a US company in Florida, which was attacked by European hackers who may have been hired by one of its competitors [5].

Core features of the Internet's design have implications for the feasibility of DoS/DDoS and the challenges in its mitigation: (i) Packet switching makes IP traceback difficult; (ii) core Internet components lack the capability to provide sufficient security and authentication since they must process high volumes of traffic, security-related computations are left to edge components. The core provides high volume capabilities, but it is too late to act against DDoS at the victim side! Finally, the Internet's distributed and heterogeneous administration makes deployment of DDoS defense mechanisms difficult.

Attackers typically require bandwidth amplification to carry out a DDoS attack. In a model of **unwitting accomplicies**, regular machines behaving according to poorly designed protocols are somehow orchestrated by attackers so that they cause DDoS. Examples of this phenomenon include SYN ACK and ICMP echo reply floods. Alternately, users may unwittingly surrender their machines by clicking on some link or installing malicious programs. In such cases, a malicious "Bot" is installed on the compromised computer, turning it into a **dedicated attacker** (see, e.g. Stacheldraht [6]).

Key observation. We start from the observation that a malicious attacker is unlikely to instrument a Botnet merely to execute a single attack. This is because the construction of a Botnet requires significant investment of time and resources, exposing criminal elements to significant risk. Once established, a Botnet represents a capital investment from which revenue can be derived, thus making it very likely to be used to execute *multiple* attacks over time.

Previous work. Several attack source identification and attack traceback techniques have been proposed like Backscatter [7], controlled flooding [8], router-centric traceback [9], iTrace [10], packet marking [11], and hash-based traceback [12]. In 2010, the authors described a distributed system capable of traceback of malicious flow trajectories in the wide area despite source IP spoofing. The system requires the placement of traffic volume sensing agents (hereafter referred to as "DDoS sensors") on a small subset of the inter-autonomous system (AS) links of the Internet. Once deployed, these agents are able to respond to DDoS attacks, as a self-organizing system capable of reconstructing topological and temporal information about the structure of malicious flows. The system effectively recovered DDoS flow structure even with very

978-1-4577-9538-2/11/$26.00 ©2011 IEEE

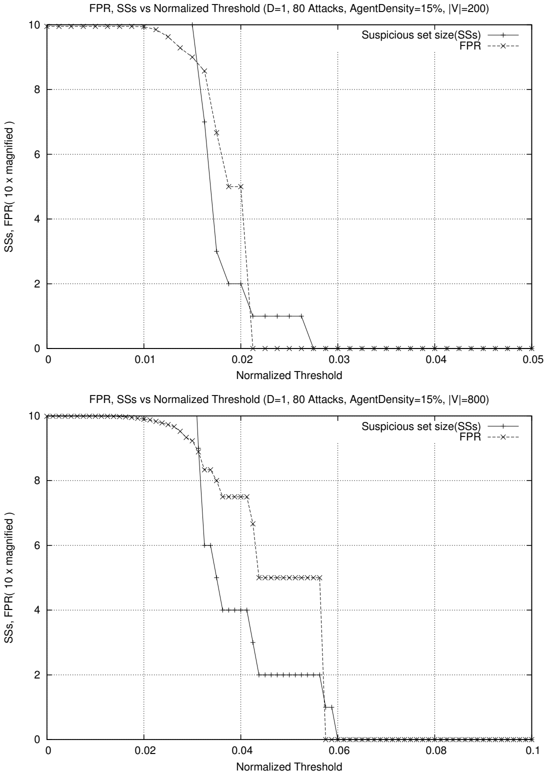

Fig. 5. SLANT on Waxman networks with one attacker (200,400 nodes)

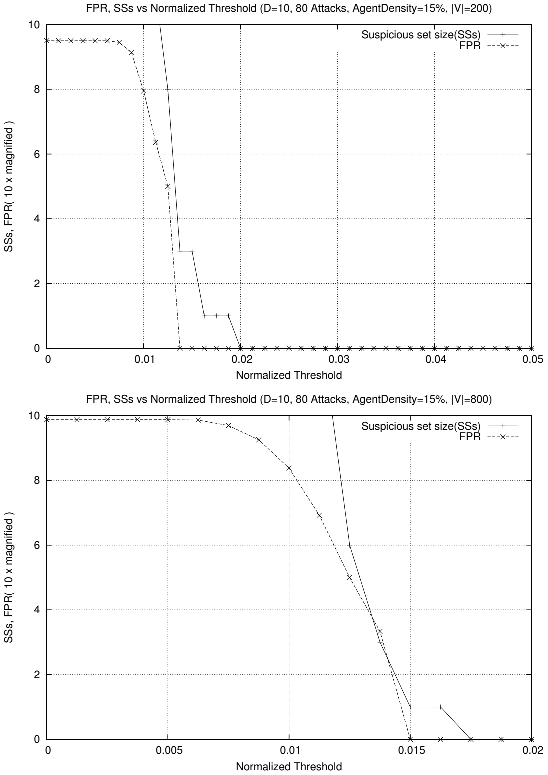

Fig. 6. SLANT on Waxman networks with 10 attackers (200,400 nodes)

VI. Conclusion and Future Work

We have shown that the SLANT algorithm is able to leverage information obtained over *sequences* of source spoofed Botnet-led DDoS attacks. The performance of the algorithm is promising, in terms of its scalability to large networks and numbers of attacking nodes. As such, the SLANT algorithm solves instances of the newly formulated attacker localization problem. SLANT's solutions enjoy low FPR and moderate suspicious set sizes under a suitable choice of threshold τ. This performance is manifested even at modest DDoS sensor agent deployment levels of 15%. As future work, the authors plan to consider the problem of automated selection of good threshold values τ, and a distributed implementation of SLANT.

References

[1] O. Demir and B. Khan, "Reconstruction of malicious internet flows," in *Proceedings of International Wireless Communications and Mobile Computing Conference*, 2010.

[2] V. D. Gligor, "A note on denial-of-service in operating systems," *IEEE Trans. Softw. Eng.*, vol. 10, no. 3, pp. 320–324, 1984.

[3] Arbor Networks, "Arbor networks worldwide infrastructure security report," http://www.arbornetworks.com/en/docman/worldwide-infrastructure-security-report-volume-iv-2008.

[4] T. R. Irirangi and O. Aotearoa, "Marshalls internet still affected after cyber attack," 2008. [Online]. Available: http://www.rnzi.com/pages/news.php?op=read|\&id=40547

[5] J. Kirk and IDG NewsService, "Two europeans charged in US over DDOS attacks," 2008. [Online]. Available: http://www.pcworld.com/businesscenter/article/151829/two_europeans_charged_in_us_over_ddos_attacks.html

[6] D. Dittrich, "The Stacheldraht distributed denial of service attack tool," 1999, accessed Dec. 1, 2010. [Online]. Available: http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

[7] B. Gemberling, C. Morrow, and B. Greene, "ISP security-real world techniques. presentation, nanog," Tech. Rep., 2001. [Online]. Available: http://www.nanog.org/meetings/nanog36/presentations/greene.ppt

[8] Burch and Hal, "Tracing anonymous packets to their approximate source," in *LISA '00: Proceedings of the 14th USENIX conference on System administration*. Berkeley, CA, USA: USENIX Association, 2000, pp. 319–328.

[9] D. Cotroneo, L. Peluso, S. Romano, and G. Ventre, "An active security protocol against dos attacks," *Computers and Communications, IEEE Symposium on*, p. 496, 2002.

[10] Bellovin, "ICMP traceback messages," RFC draft, September 2000. [Online]. Available: 'http://tools.ietf.org/draft/draft-bellovin-itrace/draft-bellovin-itrace-00.txt

[11] S. Stefan, W. David, K. Anna, and A. Tom, "Practical network support for IP traceback," *SIGCOMM Comput. Commun. Rev.*, vol. 30, no. 4, pp. 295–306, 2000.

[12] Snoeren and A. C., "Hash-based IP traceback," in *SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*. New York, NY, USA: ACM, 2001, pp. 3–14.

[13] J. Burns and R. Somaiya, "Hackers attack those seen as wikileaks enemies," http://www.nytimes.com/2010/12/09/world/09wiki.html, December 9, 2010.

[14] O. Demir and B. Khan, "Quantifying distributed system stability through simulation: A case study of an agent-based system for flow reconstruction of ddos attacks," in *Proceedings of 1st International Conference on Intelligent Systems, Modelling and Simulation*, 2010.

[15] B. M. Waxman, "Routing of multipoint connections," pp. 347–352, 1991. [Online]. Available: http://portal.acm.org/citation.cfm?id=128991

[16] H. Young, H. Bradley, A. Dan, A. Emile, L. Matthew, and S. Colleen, "The IPv4 routed /24 as links dataset11/15/2009," http://www.caida.org/data/active/ipv4_routed_topology_aslinks_dataset.xml, Accessed December 1, 2010.

[17] O. Demir, "A survey of network denial of service attacks and countermeasures," CUNY Computer Science Department, Tech. Rep., 2009.