# Moving Target Defense Agent (MOTAG)

Dr. L. Sridhara RaoAuthor[1], M. SanjayAuthor[2], Y. RuthikshaAuthor[3], V. Krishna Vamshi Author[4]
[1,2,3,4] *Member, Dept of Information Technology JB Institute of Engineering and Technology*

***Abstract:*** **Denial of Service (DoS) attacks are immense threat to internet sites and among the hardest security problems in today's internet. With little or no advance warning, a DDoS attack can easily exhaust the computing and communication resources of its victim within a short period of time. In this project we are going to create a Defense Mechanism and secure service access for authenticated clients against DDoS attacks. The goal of the project is to place some order in to the existing system attack and defense mechanisms so that a better understanding of DDoS attacks can be achieved and more efficient defense mechanisms and techniques can be devised. In this mechanism we will shuffle clients to proxy locations continuously to avoid DDoS attack.**

***Index Terms*— Distributed Denial of Service(DDOS), Denial of Service(DOS),Random forest greedy approach, Application server, Authentication server, Proxy server.**

## 1.INTRODUCTION

Arbor Networks has reported a significant increase in the prevalence of large-scale distributed denial-of-service (DDoS) attacks in recent years. In 2010, the largest reported bandwidth achieved by a flood-based DDoS attack reached 100 GB p/s. Meanwhile, the cost of performing a DDoS attack has turned out to be surprisingly low. A Trend Micro's white paper has revealed that the price for 1-week DDoS service could be as low as $150 on Russian underground market. A number of mechanisms have been proposed in the past to prevent or mitigate DDoS attacks. Filtering-based approaches use ubiquitously deployed filters to block unwanted traffic sent to the protected nodes. Capability-based defense mechanisms endeavor to constrain the resource usage by the senders within the threshold permitted by the receivers. Secure overlay solutions interpose an overlay network to indirect packets between clients and the protected nodes, aiming to absorb and filter out attack traffic. However, these static defense systems either rely on global deployment of additional functionalities on Internet routers or require large, robust virtualized network to withstand the ever-exacerbating attacks. Besides, some of them are still vulnerable to sophisticated attacks, such as sweeping and adaptive flooding attacks. In this paper, we propose MOTAG, a dynamic DDoS defense mechanism that adopts moving target defense strategy to protect centralized online services. In particular, MOTAG offers DDoS resilience for authorized and authenticated clients of security sensitive services such as online banking and finance. MOTAG employs a layer of secret moving proxies to mediate all communications between clients and the protected application servers. The network-level filters surrounding the application servers only allow traffic from the valid proxy nodes to reach the protected servers. Proxy nodes in MOTAG have two important characteristics. First, all proxy nodes are "secret" in that their IP addresses are concealed from the general public and are exclusively known by legitimate clients after successful authentication. Each legitimate client is provided with the IP address of one working proxy at any given time to avoid unnecessary information leakage. We apply existing proof-of-work (PoW) schemes to protect the client authentication channel. Second, proxy nodes are "moving". As soon as an active proxy node is attacked, it is replaced by another node at a different location, and the associated clients are migrated to alternative proxies. We show that these characteristics not only enable us to mitigate brute-force DDoS attacks, but also empower us to discover and isolate malicious insiders that divulge the location of secret proxies to external attackers. We do so via shuffling (repositioning) clients' assignment to new proxy nodes when their original proxies are under attack. We develop algorithms to accurately estimate the number of insiders and adjust client-to-proxy assignment accordingly to rescue most innocent clients after each shuffle. Our solution does not rely on global adoption on Internet routers or collaboration across different ISPs to function. Neither do we depend on resource-abundant overlay

network to out-muscle high bandwidth attacks and to provide fault tolerance. Instead, we take advantage of our proxies' secrecy and mobility properties to fend off powerful attackers. This entails lower deployment costs while offering substantial defensive agility, resulting in an effective DDoS protection.

Distributed Denial of Service (DDoS) attacks still pose a significant threat to critical infrastructure and Internet services alike. In this paper, we propose MOTAG, a moving target defense mechanism that secures service access for authenticated clients against flooding DDoS attacks. MOTAG employs a group of dynamic packet indirection proxies to relay data traffic between legitimate clients and the protected servers. Our design can effectively inhibit external attackers' attempts to directly bombard the network infrastructure. As a result, attackers will have to collude with malicious insiders in locating secret proxies and then initiating attacks. However, MOTAG can isolate insider attacks from innocent clients by continuously "moving" secret proxies to new network locations while shuffling client-to-proxy assignments. We develop a greedy shuffling algorithm to minimize the number of proxy re-allocations (shuffles) while maximizing attack isolation. Simulations are used to investigate MOTAG's effectiveness on protecting services of different scales against intensified DDoS attacks.

## 2. ARCHITECTURE

Architecture diagram explains the design of the project. It acts as a Blue Print for the project. It gives a brief idea of the project overview. Here the Architecture diagram represents how authentication server assigns a proxy server, how proxy server is going to avoid DDOS attacks and forwarding task to application server.

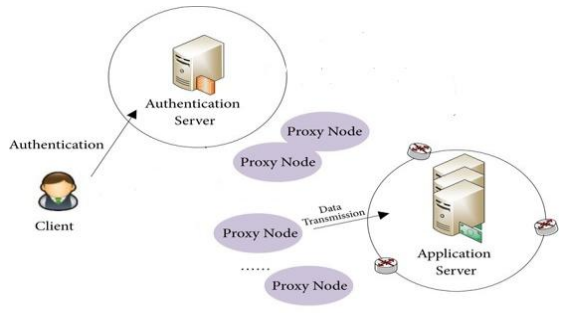


*Fig1:ArchitectureofMOTAG system*

Whenever client interacts with a Application serve r Authentication serevr come into action and assign task to a Proxy server by using random forest greedy approach method. Then this proxy servers checks weather the task is raising DDOS/DOS attacks . If attack is raised then proxy server did not pass the task to application server so we can stop DDOS/DOS attacks. If task did not raise any DDOS/DOS attack then then task is passed to application server and this application server is going to execute the task.

## 3. ALGORITHMS

*RandomForest:*

As the name implies, a random forest is made up of a huge number of individual decision trees that work together as an ensemble. Each tree in the random forest produces a class prediction, and the class with the most votes becomes the prediction of our model.

Random Forest Model Visualization Predicting the Future.Any of the individual constituent models will outperform a large number of reasonably uncorrelated models (trees) working as a committee.

## 4. MODULES

A) Authentication server.

Whenever a client interacts with the system authentication server come into action assign a proxy servers with random forest greedy algorithm to check weather that action raises DDOS/DOS attack or not.

B) Application server**.**

An application server is a program on a computer that handles all application operations given by user. Proxy server sends user actions to application server by restricting DDOS/DOS attacks. Then this application server executes the actions given by user.

C) Proxy servers

Where proxy servers are nothing but intermediate between user/client and application server. The main aim of these proxy servers are to differentiate the users actions and restrict the action if it is a DDOS/DOS attack. If not it will assign the action to application server.

D) Client

Where this client module is the place where user interacting with the MOTAG system. Where this client module mainly consists of two parts they are

uploading file to the system and getting the detection graph.

## 5. CONCLUSION

We present MOTAG, a framework that employs dynamic, hidden proxies as moving targets to mitigate network flooding DDoS attacks. To reach the protected service, authenticated clients are assigned to individual proxy nodes that perform packet forwarding and session policing. When a DDoS attack is mounted against MOTAG proxies, the authenticated clients connected to the attacked proxies are re-assigned to alternative proxies at runtime, enabling them to evade the ongoing attack and maintain access to the protected service. With MOTAG, we can effectively hide the protected critical services from external attackers. Sophisticated attackers can only use insiders to locate our proxy nodes and attack them. MOTAG employs a novel, efficient shuffling mechanism to quarantine insiderassisted attacks. Our simulations show that MOTAG can protect a majority of innocent clients from DDoS attacks assisted by hundreds of insiders within a small number of shuffles. In addition, our experimental methodology and the results can be used to guide the implementation and deployment of MOTAGbased DDoS defense systems.

## 6. FUTURE ENHANCEMENT

Due to continuous reallocation of proxy servers it may consume more battery and system resources. In future enhancement, we have to reduce those resource consumptions.

## REFERENCES


[1] R. Dobbins and C. Morales, "Worldwide infrastructure security report vii," 2011. [Online]. Available: http://www.arbornetworks. com/report.

[2] T. Micro, "Russian underground 101," http://www.trendmicro.com/cloud-content/us/ pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf, 2012.

[3] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling high bandwidth aggregates in the network," ACM Computer Communication Review, vol. 32, pp. 62–73, 2002.

[4] P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," RFC 2827 (Best Current Practice), Internet Engineering Task Force, May 2000, updated by RFC 3704.

[5] X. Liu, X. Yang, and Y. Lu, "To filter or to authorize: network-layer dos defense against multimillion-node botnets," in Proceedings of the ACM SIGCOMM 2008 conference on Data communication. New York, NY, USA: ACM, 2008, pp. 195–206.

[6] T. Anderson, T. Roscoe, and D. Wetherall, "Preventing internet denialof-service with capabilities," SIGCOMM Comput.Commun.Rev., vol. 34, no. 1, pp. 39–44, 2004.

[7] A. Yaar, A. Perrig, and D. Song, "Siff: A stateless internet flow filter to mitigate ddos flooding attacks," in IEEE Symposium on Security and Privacy, 2004, pp. 130–143.

[8] X. Yang, D. Wetherall, and T. Anderson, "Tva: a dos-limiting network architecture," IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1267–1280, 2008.

[9] X. Liu, X. Yang, and Y. Xia, "Netfence: preventing internet denial of service from inside out," in Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM, ser. SIGCOMM '10. New York, NY, USA: ACM, 2010, pp. 255–266. [Online]. Available: http://doi.acm.org/10.1145/1851182.1851214.

[10] A. D. Keromytis, V. Misra, and D. Rubenstein, "Sos: Secure overlay services," in Proceedings of ACM SIGCOMM, 2002, pp. 61–72.

[11] A. Stavrou and A. D. Keromytis, "Countering dos attacks with stateless multipath overlays," in Proceedings of the 12th ACM conference on Computer and communications security, ser. CCS '05. New York, NY, USA: ACM, 2005, pp. 249–259. [Online]. Available: http://doi. acm.org/10.1145/1102120.1102153.

[12] D. G. Andersen, "Mayday: distributed filtering for internet services," in USITS'03: Proceedings of the 4th conference on USENIX Symposium on Internet Technologies and Systems. Berkeley, CA, USA: USENIX Association, 2003, pp. 3–3.

[13] R. Stone, "Centertrack: an ip overlay network for tracking dos floods," in SSYM'00: Proceedings of the 9th conference on USENIX Security Symposium. Berkeley, CA, USA: USENIX Association, 2000, pp. 15–15.

[14] A. Mahimkar, J. Dange, V. Shmatikov, H. Vin, and Y. Zhang, "dfence: Transparent network-based denial of service mitigation," in NSDI, 2007.

[15] C. Dixon, T. Anderson, and A. Krishnamurthy, "Phalanx: withstanding multimillion-node botnets," in Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, ser. NSDI'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 45–58. [Online]. Available: http://dl.acm.org/citation. cfm?id=1387589.1387593.

[16] T. Aura, P. Nikander, and J. Leiwo, "Dos-resistant authentication with client puzzles," in Security Protocols Workshop, 2000, pp. 170–177.

[17] D. Dean and A. Stubblefield, "Using client puzzles to protect tls," in Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, ser. SSYM'01. Berkeley, CA, USA: USENIX Association, 2001, pp. 1–1. [Online]. Available: http://dl.acm.org/citation.cfm?Id = 1251327.1251328.

[18] B. Waters, A. Juels, J. A. Halderman, and E. W. Felten, "New client puzzle outsourcing techniques for dos resistance," in Proceedings of the 11th ACM conference on Computer and communications security, ser. CCS '04. New York, NY, USA: ACM, 2004, pp. 246–256. [Online]. Available: http://doi.acm.org/10.1145/ 1030083.1030117.

[19] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. Maggs, and Y.-C. Hu, "Portcullis: Protecting connection setup from denial-of-capability attacks," in Proceedings of the ACM SIGCOMM, August 2007.

[20] N. Johnson and S. Kotz, Urn Models and Their Applications: An Approach to Modern Discrete Probability Theory. New York: Wiley, 1977, ch. 1.3.2.

[21] M. Matsumoto and T. Nishimura, "Mersenne twister: a 623- dimensionally equidistributed uniform pseudo-random number generator," ACM Trans. Model. Comput.Simul., vol. 8, no. 1, pp. 3–30, Jan. 1998. [Online]. Available: http://doi.acm.org/10.1145/272991.272995.

[22] "Iperf," http://iperf.sourceforge.net.

[23] M. Abliz, "Internet denial of service attacks and defense mechanisms," University of Pittsburgh, Tech. Rep. TR-11-178, Mar 2011.

[24] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The secondgeneration onion router," in In Proceedings of the 13 thUsenix Security Symposium, 2004.

[25] L. Overlier and P. Syverson, "Locating hidden servers," in Proceedings of the 2006 IEEE Symposium on Security and Privacy, ser. SP '06, Washington, DC, USA, 2006, pp. 100–114.

[26] V. Kambhampati, C. Papadopoulos, and D. Massey, "Epiphany: A location hiding architecture for protecting critical services from ddos attacks," in The 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012), 2012.

[27] X. Wang and M. K. Reiter, "Wraps: Denial-of-service defense through web referrals," in 25th IEEE Symposium on Reliable Distributed Systems. IEEE Computer Society, 2006, pp. 51–60.

[28] S. Antonatos, P. Akritidis, E. P. Markatos, and K. G. Anagnostakis, "Defending against hitlist worms using network address space randomization," in Proceedings of the 2005 ACM workshop on Rapid malcode, ser. WORM '05. New York, NY, USA: ACM, 2005, pp. 30–40. [Online]. Available: http://doi.acm.org /10.1145/1103626.1103633.