SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

SDNを用いたDDoS攻撃に対する防御機構構築
Defense Mechanism Against DDoS attacks using SDN

徳山 凌 * 布田 裕一 † 鈴木 彦文 ‡ 岡崎 裕之 §
Ryo Tokuyama Yuichi Futa Hikofumi Suzuki Hiroyuki Okazaki

キーワード DoS, DDoS, SDN

あらまし

近年,DDoS 攻撃 (Distributed Denial-of-Service Attacks) による被害が増えている.2020 年の第 2 四半期の DDoS 攻撃数は前年比 3 倍とのレポートも出ている.DDoS 攻撃とは DoS 攻撃を複数のコンピュータから行う攻撃手法である. 標的となるコンピュータに対して複数のマシンから大量の処理負荷を与えることでサービスを機能停止状態へ追い込む手法である. この攻撃を担う複数マシンには事前に不正なプログラムなどが組み込まれている. このようなプログラムを遠隔から利用することで一斉に攻撃することが可能である．鈴木ら [1] の研究では, 実機を用いたネットワーク環境で外部からの DDoS 攻撃を実行し，攻撃を評価している．この結果, 300 万パケットを受信したところで攻撃対象となったネットワークの最も外側にある UTM が停止し，ネットワーク全体が機 能不全に陥ることが判明した．この実験のように, 実機環境で DDoS 攻撃を発生させると，ネットワーク全体への影響が大きいため，頻繁に発生させて防御機構を評価することが困難である. 我々の研究では異なる実環境においても容易に防御機構の評価が可能な攻撃環境を構築し，意図的に DDoS 攻撃を発生させる環境を仮想環境として，実環境と同等の性能を持つことを確認した.

本稿では柔軟なネットワーク構成を実現するために SDN を用いて防御機構を構築する．SDN を実現するために，OpenFlow プロトコル対応の Open vSwitch を使用し，Mininet で構築を行う．OpenFlow コントローラには Python 言語で書かれた Ryu を使用する．SDN により，攻撃の可能性が高いとされるパケットの遅延，破棄を行う．今回はスイッチを階層型に組み，攻撃の可能性があるパケットをマーキングし，マークされたパケットがスイッチを通過する間に次に送信されてくるパケットからマークされたパケットの送信元を攻撃可能性があるかどうかを判定する．マークされたパケットはスイッチを通過させる際に遅延処理を行う．最終的にしきい値を超えたパケット送信元からのパケットについては破棄処理を行う．今回対象とする DDoS 攻撃は TCP SYN Flood である．構築した防御機構は構築済みの攻撃評価環境を使用して得られた結果から改良を行う.

* 東京工科大学大学院 バイオ情報メディア研究科　コンピュータサイエンス専攻〒 192-0982 東京都八王子市片倉町 1404-1. Tokyo University of Technology Graduate School Department of Computer Science , 1404-1, Katakuramachi, Hachioji City, Tokyo, 192-0982, JAPAN.
† 東京工科大学 コンピュータサイエンス学部〒 192-0982 東京都八王子市片倉町 1404-1. Tokyo University of Technology Department of Computer Science , 1404-1, Katakuramachi, Hachioji City, Tokyo, 192-0982, JAPAN. 1
‡ 信州大学 総合情報センター 〒 380-8553 長野県長野市若里 4-17-1. Integrated Intelligence Center, Shinshu University. 4-17-1, Wakasato, Nagano City 380-8553, JAPAN.
§ 信州大学 学術研究院 (工学系) 〒 380-8553 長野県長野市若里 4-17-1. Faculty of Engineering, Shinshu University 4-17-1, Wakasato, Nagano City 380-8553, JAPAN.

参考文献

[1] Hikofumi SUZUKI, Tetsuya UI, Sumire FURUKAWA, Daijiro YUHARA ,Shin, NARUSE, Yoshifumi ASAKAWA, Kazuya NAGAI, Osamu HASEGAWA, Consideration on Implementation of Pseudo Attack by Distributed Denial-of-Service Attack and Verification of UTM, JIPS Japan, Vol.21,21–28 (2017)

[2] DDoS attacks in Q2 2020. https://securelist.com/ddos-attacks-in-q2-2020/98077/. Accessed 1 Jan 2021