一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
NS2025-124(2025-10)

クロスファイア攻撃の効率性分析

上田　和輝†　　上山　憲昭†

† 立命館大学情報理工学部情報理工学科
〒567-8570 大阪府茨木市岩倉町 2-150
E-mail: †is0659ih@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

あらまし　近年，企業や組織を標的とした DDoS 攻撃 (分散型サービス拒否攻撃) による被害が深刻化しており，社会・経済活動に多大な影響を及ぼしている．特に本研究で扱う Crossfire Attack(CFA) は通常の DDoS 攻撃と異なり，攻撃対象がサーバではなくリンクである特徴を有する．そのため，従来の DDoS 攻撃の検知手法である，攻撃対象サーバでの検知や，異常なトラヒックを識別するといった対応が困難であり，CFA は検知が困難な攻撃である．これらの要因から，CFA は今後ネットワークに甚大な被害をもたらす可能性があり，CFA に脆弱なエリアの効果的・効率的な対策が必要である．そこで本研究では CFA の攻撃者にとっての費用対効果に基づく尺度を提案し，上記尺度に基づいた，CFA に対して脆弱なエリアの推定法を考案する．そのうえで CFA に脆弱なエリアの CFA 効率性を，小コストで効果的に低減する技術の確立を目的とする．本研究の第一段階として，攻撃者にとっての費用対効果を表す指標である，CFA 効率を考える．本研究で提案するターゲットエリア全体の平均 CFA 効率 $\overline{\eta}_{area}$ を，$\overline{\eta}_{area} = \frac{\overline{R}_{area}}{Cost_{total}}$ で定義する．ここで，$\overline{R}_{area}$ はターゲットエリアの境界リンクにおける遮断トラヒック量比率，$Cost_{total}$ は使用ボット数×ボットの相対コストである．ボットの相対コストは，攻撃に使用するボットの回線速度とコストに基づく相対コストであり，使用ボット数と相対コストを元に複数の攻撃シナリオを作成し，作成したシナリオにおける，各 TA についての CFA 効率を評価する．

謝辞　本研究は JSPS 科研費（JP25K03113, JP23K28078）の助成を受けたものである．ここに記して謝意を表す．
キーワード　CFA Attack, DDoS 攻撃, CFA 効率

Investigating Efficiency of Crossfire Attack

Kazuki UEDA† and Noriaki KAMIYAMA†

† College of Information Science and Engineering, Ritsumeikan University
2-150, Iwakura-cho, Ibaraki, Osaka 567-8570
E-mail: †is0659ih@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

Abstract　In recent years, damage from DDoS (Distributed Denial of Service) attacks targeting corporations and organizations has become increasingly severe, having a significant impact on social and economic activities. The Cross-Fire Attack (CFA), the focus of this research, is distinct from conventional DDoS attacks as it targets network links rather than servers. This characteristic makes it difficult to apply traditional DDoS detection methods, such as monitoring at the target server or identifying anomalous traffic, establishing CFA as a stealthy and hard-to-detect form of attack. These factors suggest that CFA poses a significant future threat to networks, necessitating effective and efficient countermeasures for vulnerable areas. This research, therefore, proposes a metric based on the cost–effectiveness for the CFA attacker and devises a method for estimating CFA-vulnerable areas based on this metric. The ultimate goal is to establish technology to effectively reduce the CFA efficiency of vulnerable areas at a low cost. As the first stage of this research, we consider the CFA efficiency as an index representing the cost-effectiveness for an attacker. The average CFA efficiency for an entire target area, $\overline{\eta}_{area}$, proposed in this study is defined by $\overline{\eta}_{area} = \frac{\overline{R}_{area}}{Cost_{total}}$. Here, the numerator $\overline{R}_{area}$ represents the blocked traffic ratio on the boundary links of the target area, while the denominator $Cost_{total}$ indicates the number of bots used multiplied by the relative cost of the bots. In our model, we define the relative cost of bots based on their connection speed and associated costs. Based on the number of bots and their relative costs, we construct several attack scenarios and investigate the CFA efficiency for each target area under these scenarios.

Key words　CFA Attack, DDoS Attack, CFA efficiency