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

クロスファイア攻撃における攻撃戦略と費用対効果の分析

上田　和輝†　　上山　憲昭†

† 立命館大学 情報理工学部　〒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分散型サービス拒否攻撃 (DDoS: distributed denial of service) 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. 特に本稿で扱う 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といった特徴を持つ. 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と言える. 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. そこで本稿では攻撃者にとっての費用対効果を測定するため，攻撃者ごとの動員可能ボット数を設定し，ネットワーク内の各エリアに配置されたボットから攻撃を実行するシミュレーションを行い，攻撃者の予算やボット選択手法によって，CFA に対するネットワークの脆弱性がどのように変化するのかについて評価する.

キーワード　DDoS, CFA, 費用対効果, 脆弱性分析

Relationship between Attack Strategy and Cost-Effectiveness in Crossfire Attacks

Kazuki UEDA† and Noriaki KAMIYAMA†

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

Abstract　In recent years, damage caused by Distributed Denial-of-Service (DDoS) attacks targeting enterprises and organizations has become serious, significantly impacting social and economic activities. In particular, the Crossfire Attack (CFA) addressed in this study differs from conventional DDoS attacks as it targets network links rather than servers. Consequently, conventional DDoS detection methods, such as detecting attacks at the target server or identifying abnormal traffic, are difficult to apply, making CFA a hard-to-detect attack. Due to these factors, CFA poses a potential threat of causing immense damage to networks, necessitating effective and efficient countermeasures for vulnerable areas. In this study, to measure the cost-effectiveness for an attacker, we set the number of available bots per attacker and conduct simulations of attacks initiated from bots distributed across network areas. We evaluate how network vulnerability to CFA varies depending on the attacker's budget and bot selection strategy.

Key words　DDoS, CFA, Cost-effectiveness, Vulnerability Analysis

1. はじめに

1.1 研究背景と CFA の脅威

近年，インターネットは社会基盤として不可欠な存在となる一方で，企業や組織を標的とした分散型サービス拒否攻撃 (DDoS: Distributed Denial of Service) による被害は深刻化の一途をたどっている．攻撃手法は年々高度化・巧妙化しており，既存の防御策を突破する事例が後を絶たず，インターネット基盤を利用する多くのサービスは，常に可用性が脅かされるリスクに晒されている．特に，本稿で着目する Crossfire Attack (以下，CFA と記す) は，特定のサーバではなく，通信経路上のリンク（Target Link）を標的とするリンクフラッディング攻撃であり，DDoS 攻撃の一種である．CFA において攻撃者は，ターゲットエリア (Target Area: TA) 周辺のデコイサーバに向けて大量の低レートなトラヒックを送信することで，TA に接続する重要なリンクを間接的に輻輳させ，TA 全体をネットワークから孤立させる．CFA は，攻撃トラヒックが正当な通信と見分けがつかない低レートなものである点や，TA 内のサーバは直接攻撃を受けない点から，従来のサーバ側での検知や異常トラヒックの識別による防御が極めて困難である．

1.2 従来研究の課題と本稿の目的

CFA の脅威に対し，これまで機械学習を用いた検知手法や，SDN を用いた経路変更などの防御手法が数多く提案されてきた．しかし，これらの既存研究の多くは防御側の視点に留まっている．攻撃者がどのエリアを標的とすれば最も少ないリソースで最大の被害を与えられるかといった，攻撃者視点での費用対効果 (ROI: Return on Investment) や，攻撃リソース（ボット）の地理的分布に基づく攻撃戦略の定量的分析は十分になされていない．効果的な防御策を構築するためには，攻撃者の行動原理や，攻撃効率の良い脆弱なエリアを特定し，あらかじめ対策を講じることが不可欠である．そこで本稿では，攻撃者の視点に基づき，CFA に対するネットワークの脆弱性を分析することを目的とする．具体的には，攻撃者の予算規模やボットの地理的配置に応じた攻撃シミュレーションを行い，ネットワーク構造や攻撃リソースの偏在が攻撃効率に与える影響を定量的に評価する．また，マルウェア市場の調査結果に基づくコストモデルを導入することで，より現実的な脅威分析を行う．

1.3 本稿の構成

本稿の構成は以下の通りである．第 2 節では，CFA の攻撃原理および検知困難性について概説する．第 3 節では，CFA に関する検知・防御手法および攻撃リソースに関する関連研究について述べ，本稿の立ち位置を明確にする．第 4 節では，攻撃効果を定量的に評価するために提案する 3 つの指標 (RTR, ACR, BTR) およびコストモデルについて定義する．第 5 節では，実際の米国商用 ISP ネットワークトポロジを用いたシミュレーション評価の結果を示し，ネットワーク構造や予算規模が攻撃効率に与える影響について考察する．最後に第 6 節で本稿をまとめる．

2. Crossfire Attack (CFA)

2.1 攻 撃 手 法

Crossfire Attack (CFA) は探索フェーズと攻撃フェーズの 2 つの段階で構成されている．探索フェーズでは，図 1 に示す通り，攻撃者は多数の Bot host を用いて，TA 内の一般サーバや TA 周辺に存在する多数の Decoy server に対して，traceroute パケットの送信を行う．その後，取得した情報に基づき，Target Link の選定を行う．Target Link として選定するべきものとしては，TA に対して多くの通信が少ないリンクに集中している箇所であり，このような特徴を持つリンクをフラッディングさせることで，効率的に TA と外部エリアの通信を遮断することができる．

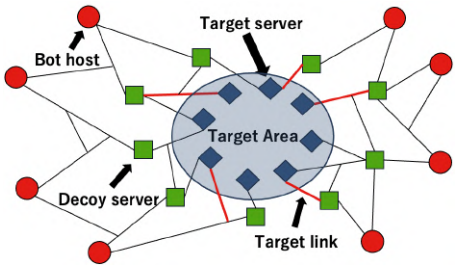


図 1: Structure of Crossfire Attack

2.2 特徴 -検知困難性-

CFA は従来の DDoS 攻撃と異なり，以下に挙げる特性から検知および防御が非常に困難である．はじめに，CFA は攻撃の前兆や攻撃可能性を測定することが出来ないといった特徴がある．そのため，既存の防御策では，攻撃を素早く検出した上で，適切な対策を行うことが困難であり，攻撃対象となる TA の予測も難しい．次に，CFA は少量のトラヒックを送信するため，通常ユーザの通信と酷似しているといった特徴がある．そのため，このような少量フローでは，Target Link に接続されたルータによる攻撃フロー検知や，トラヒック遮断が困難である．最後に，CFA の攻撃対象である TA は直接攻撃を受けるのではなく，Decoy server に向けて攻撃されるといった特徴がある．そのため，TA 内のサーバは攻撃されていることに気づくことが困難であり，既存の通信フローに対する異常検知システムでは，攻撃の存在自体を見逃す可能性がある．

3. 関 連 研 究

CFA の概念は Kang ら [1] によって提唱されて以来，様々な検知および防御手法が提案されている．既存研究は主に，攻撃フェーズにおける検知と，ネットワーク構造を利用した防御に大別できる．

検知手法としては，GCN (Graph Convolutional Network) や Deep Learning，SVM などの機械学習を用いて，低レートな攻撃フローの相関関係やトラヒックの特徴を学習・識別する手法が多く提案されている [2] [3] [4]．また，SDN 環境におけるリンク統計値の監視 [5] や，探索フェーズにおける traceroute の挙動分析による検知手法 [6] も提案されている．

防御手法としては，SDN を活用して探索フェーズにおける traceroute を欺く手法や，仮想トポロジの展開，Route Mutation による経路変更など，攻撃者に対してネットワーク構成を隠蔽または動的に変更する Moving Target Defense (MTD) のアプローチが主流である [7] [8] [9].

攻撃リソースに関しては，Caballero ら [10] がマルウェア配布市場 (PPI) の実態調査を行い，地域ごとのインストール単価を明らかにしている．しかしながら，上述した既存研究の多くは防御側の視点に留まっており，攻撃者が「どのエリアを狙えば最も効率が良いか」という費用対効果 (ROI) の観点や，地理的・経済的制約に基づいた攻撃戦略の定量的な分析は十分になされていない．本稿では，[10] の調査結果をコストモデルの基礎とし，攻撃者視点での脆弱性分析を行う点で独自性を有する．

4. CFA の効果の定量分析法

本節では，Crossfire Attack の脅威をより現実的かつ定量的に評価するために，新たに提案する 4 つの指標について説明する．また，ボットの獲得コストに関するモデル化についても述べる．

4.1 評価指標の提案

本稿では，攻撃者の視点から攻撃の効果と効率を評価するために，以下に述べる，RTR，ACR，BTR の 3 つの指標を定義する．

Regular Traffic Ratio (RTR)

RTR (Regular Traffic Ratio) は，正規トラヒックの分布を表す指標であり，平常時の通信において対象となる Target Link の占有割合を示す．RTR の算出手順は以下の通りである．

（1） TA V_{in} と外部エリア V_{out} を接続する Target Link の集合 $L_{boundary}$ を特定する．

（2） 全ての $s \in V_{out}, t \in V_{in}$ のペアについて最短経路 P_{st} を導出する．

（3） 各リンク $l \in L_{boundary}$ について，全最短経路の中で l を通過する経路の数 $Count(l)$ を集計する．

（4） 総経路数 N_{total} で除算し，正規化を行う．

$$RTR(l) = \frac{Count(l)}{N_{total}} \tag{1}$$

Attack Concentration Ratio (ACR)

ACR (Attack Concentration Ratio) は，攻撃トラヒックの集中率を表す指標であり，特定のボット組み合わせにおける各攻撃シナリオにおいて，対象の Target Link に攻撃トラフィックがどれだけ集中しているかを示す．本稿では，モンテカルロ法を用いて以下の手順で ACR を推定する．

（1） N 回の試行を行う（本稿では $N = 1,000$）．

（2） 各試行 i において，ボット集合から n_b 個，デコイ集合から n_d 個のノードをランダムに抽出する．

（3） 抽出されたボット・デコイ間の全ペア（$n_b \times n_d$ 通り）について最短経路を導出する．

（4） 各リンク l について，その試行で通過したフロー数 $Count_i(l)$ を計測し，その試行における集中率 $r_i(l)$ を算出する．

$$r_i(l) = \frac{Count_i(l)}{n_b \times n_d} \tag{2}$$

（5） 全試行終了後，平均値を算出して最終的な ACR とする．

$$ACR(l) = \frac{1}{N} \sum_{i=1}^{N} r_i(l) \tag{3}$$

Blocked Traffic Ratio (BTR)

BTR (Blocked Traffic Ratio) は，遮断トラヒック量比率を表す指標であり，攻撃者が予算（ボット数）の制約条件下で攻撃を実行した結果，TA に流入出する正規トラヒックの何割が遮断されるかを示す．本稿では，攻撃者が合理的判断に基づき，費用対効果 (ROI) を最大化する戦略（貪欲法）をとると仮定し，以下の手順で BTR を算出する．

（1） 全ての Target Link 候補について，攻撃コスト $Cost(l)$ を算出する．前述の通り，ACR が高いリンクは攻撃トラフィックが集中しやすいため，より少ないボット数で帯域を枯渇させることが可能である．したがって，攻撃コストは ACR に反比例するものと想定し，係数 α を用いて次式で表す．

$$Cost(l) = \frac{\alpha}{ACR(l)} \tag{4}$$

続いて，この $Cost(l)$ と $RTR(l)$ を用いて，各リンクの費用対効果 (ROI) を算出する．

$$ROI(l) = \frac{RTR(l)}{Cost(l)} \tag{5}$$

（2） 全てのリンクを ROI の降順にソートし，リスト L_{sorted} を作成する．

（3） L_{sorted} の先頭から順にリンクを選択し，累積コストが攻撃者の総予算 ($Budget$) を超えない範囲で攻撃対象集合 S に追加する．

$$\sum_{l \in S} Cost(l) \le Budget \tag{6}$$

（4） 集合 S に含まれるリンクの RTR の総和を，最終的な遮断トラヒック量比率 ($BTR(l)$) とする．

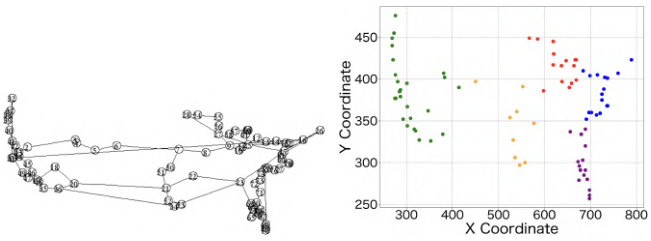
$$BTR(l) = \min\left(\sum_{l \in S} RTR(l), 1.0 \right) \tag{7}$$

4.2 ボットの相対コストの定義

本稿では，先行研究 [7] で言及された「アメリカ，イギリス地域ではボットが 1,000 インストールあたり$100-180 で取引されている」という点に着目し，同じネットワーク内でも地域によってボットの獲得コストに違いがあるという仮説を立てる．具体的には，アメリカ国内では「ボットの 1 インストールあたりの価格は，$0.1-0.18 の間で推移する」と設定し，これを元に各地域におけるボットの相対コストを定義する．

各ネットワークトポロジを構成するノードを対象とし，トポロジ上での位置座標を特徴量として，k-means 法によるクラスタリングを行う．具体的には，ネットワーク全体を 5 つのエリア（Cluster）に分割し，それぞれの Cluster 内のノード数に比例するよう相対コストを定義する．

各ネットワークのトポロジ図および k-means 法によりクラスタリングされた Cluster 図について，AGIS ネットワークを図 2，Allegiance Telecom を図 3，At Home Network を図 4 に示す．また，各クラスタに対応する色，地理的配置，およびボットの 1 インストールあたりの価格（Cost per Install）をまとめたものを，それぞれ表 1，表 2，表 3 に示す．

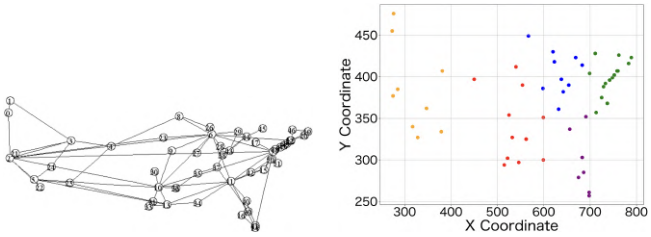


(a) Topology (b) Cluster Classification

図 2: AGIS Network Topology and Cluster Classification

表 1: Cluster Information for AGIS Network

Cluster	Color	Location / Cost per Install
0	Blue	東海岸北部・$0.1376
1	Orange	大陸中央部・$0.1000
2	Green	西海岸・$0.1800
3	Red	大陸北部・$0.1282
4	Purple	東海岸南部・$0.1282

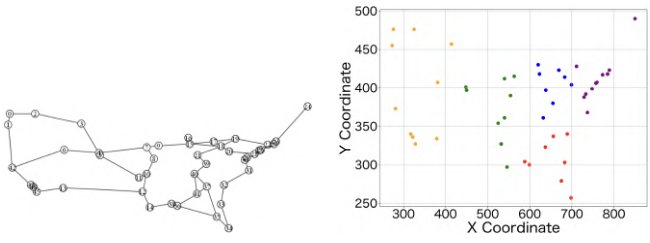


(a) Topology (b) Cluster Classification

図 3: Allegiance Telecom Topology and Cluster Classification

表 2: Cluster Information for Allegiance Telecom

Cluster	Color	Location / Cost per Install
0	Blue	大陸北部・$0.1300
1	Orange	西海岸・$0.1200
2	Green	東海岸北部・$0.1800
3	Red	大陸中央部・$0.1500
4	Purple	東海岸南部・$0.1000



(a) Topology (b) Cluster Classification

図 4: At Home Network Topology and Cluster Classification

表 3: Cluster Information for At Home Network

Cluster	Color	Location / Cost per Install
0	Blue	大陸北部・$0.1000
1	Orange	西海岸・$0.1533
2	Green	大陸中央部・$0.1267
3	Red	東海岸南部・$0.1000
4	Purple	東海岸北部・$0.1800

5. 数 値 評 価

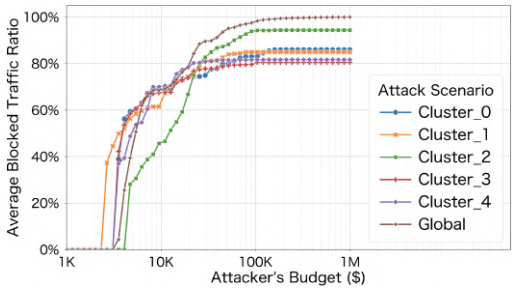
5.1 数値評価の概要と条件設定

本評価では，攻撃者の経済的規模として，**小規模** (1 万ドル)，**中規模** (10 万ドル)，**大規模** (100 万ドル) の 3 パターンを想定した．また，攻撃拠点の違いによる影響を明らかにするため，ボットの配置ノードの選択法として，k-means 法により分類された各エリアに限定してボットを選択する **Cluster 0 – Cluster 4 シナリオ**（5 通り）と，トポロジ全体からランダムに選択する **Global シナリオ**の計 6 つを比較する．

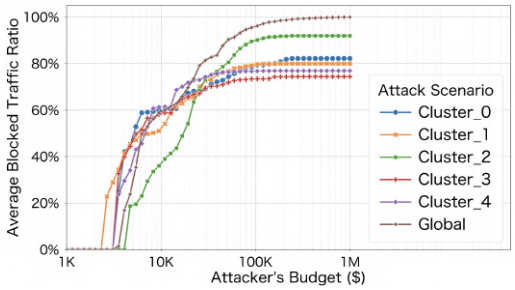
なお，各シナリオにおいて動員可能なボット数は，予算を各エリアのボット単価で除算することで算出される．これらの定義に基づき，本稿では TA の規模が攻撃効果に与える影響を分析する．具体的には，TA として選定する互いに連結した k 個のノード集合のサイズを 2，3，5 と変化させた各ケースについて，攻撃者の予算を 0 から最大 100 万ドルまで連続的に増加させた場合の平均遮断トラヒック量比率（トポロジ上で選択可能なサイズ k の連結ノード集合全てに対する平均値）の推移を評価する．これにより，3 つのネットワーク（AGIS，Allegiance Telecom，At Home Network）において，TA 規模の拡大が攻撃の費用対効果に与える影響を明らかにする．

5.2 AGIS ネットワークにおける評価結果

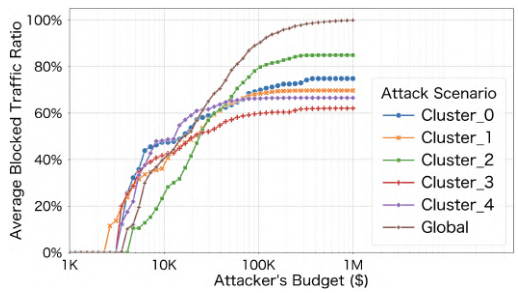
図 5 に，AGIS ネットワークにおいて TA サイズを 2，3，5 と変化させた場合の評価結果を示す．



(a)TA Size 2



(b)TA Size 3



(c)TA Size 5

図 5: Comparison of Cost-Effectiveness by TA Size in AGIS Network

a） TA サイズの変化による攻撃効果への影響

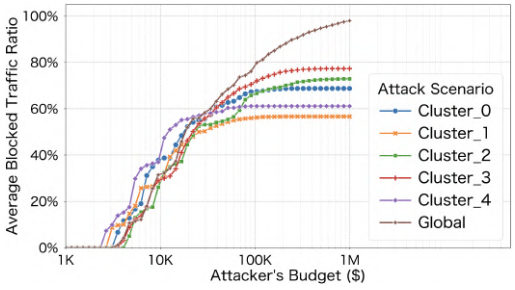
全域ランダム（Global）を除く攻撃シナリオについて，TA サイズと遮断率の関係に着目すると，TA サイズが 2 および 3 の段階では，多くのシナリオで平均遮断トラヒック量割合が約 80% と比較的高水準で推移している．TA サイズ 2 から 3 への変化における性能低下は軽微である．しかし，TA サイズが 5 に拡大すると，全域ランダム以外のシナリオ全体で遮断率が 10% ~ 15% 程度急激に低下する傾向が確認された．一方で，全域ランダム戦略は TA サイズが 5 になっても依然として 100% に近い遮断率を維持しており，ターゲット規模が拡大するほど，局所的な攻撃に対する耐性が増し，広域分散攻撃の優位性が高まることが示された．

b） Cluster 2（西海岸エリア）に見られる特異な挙動

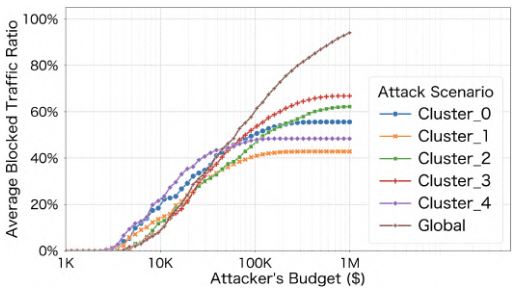
Cluster 2 は，予算 5 万ドル未満では最も平均遮断トラヒック量比率が低いが，それ以上では傾向が逆転した．他のシナリオが飽和状態となる中，Cluster 2 のみが値を伸ばし続け，最終的には Global シナリオに次ぐ高い攻撃効果を達成した．これは，Cluster 2 が西海岸に偏在しているためである．低予算時は地理的偏りが非効率となるが，リソース増大に伴い，大規模ハブからの集中攻撃が有効に機能したと考えられる．したがって，AGIS への攻撃は，低予算時は他エリア，高予算時は西海岸へ拠点をシフトさせる戦略が有効であると結論付けられる．

5.3 Allegiance Telecom における評価結果

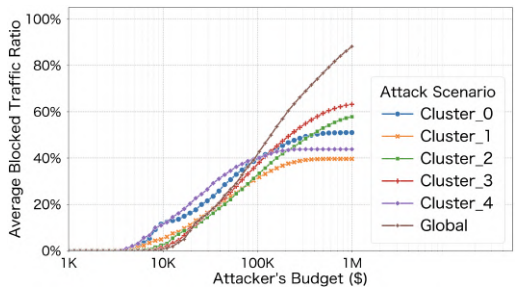
図 6 に，Allegiance Telecom において TA サイズを 2，3，5 と変化させた場合の評価結果を示す．



(a)TA Size 2



(b)TA Size 3



(c)TA Size 5

図 6: Comparison of Cost-Effectiveness by TA Size in Allegiance Telecom

a） 高い堅牢性と低い遮断率

Allegiance Telecom は，比較対象とした 3 つのネットワークの中で，Crossfire Attack に対して最も構造的に堅牢なネットワークであると言える．その根拠として，平均遮断トラヒック量比率の推移が挙げられる．TA サイズ 2（小規模）の段階であっても，全域ランダム攻撃ですら平均遮断率が 100% に到達していない．さらに，TA サイズ 5 に拡大した場合，最も効果的でない攻撃シナリオにいたっては，遮断率は 40% 程度まで低下しており，これは 3 つのネットワークの中で最も低い数値である．

b） 構造的要因：ノード数に対するエッジ数の比率

この高い堅牢性の主たる要因は，TA の連結数やノード・エッジ数そのものよりも，ネットワークの密度（Complexity）にあると考えられる．

本考察において，ネットワークを構成するノード集合を V，エッジ集合を E とし，その要素数をそれぞれ $|V|$, $|E|$ と表す．また，ネットワークの複雑さを示す指標として，ノード数に対するエッジ数の比率（リンク密度）を R と定義し，式 (8) のように表す．

$$R = \frac{|E|}{|V|} \tag{8}$$

表 4 に，各ネットワークにおける $|V|$, $|E|$，TA サイズが 5 の時の連結 TA 数，および算出された R の値を示す．

表 4: Comparison of Link Density R and Number of Connected TAs

Network	Nodes ($\|V\|$)	Edges ($\|E\|$)	Ratio (R)	TAs
AGIS	82	92	1.12	478
At Home Network	46	55	1.20	232
Allegiance Telecom	53	88	**1.66**	**7817**

表 4 に示す通り，AGIS および At Home Network においては，R の値が約 1.1 ~ 1.2（AGIS: $R \approx 1.12$，At Home: $R \approx 1.20$）であるのに対し，Allegiance Telecom では $R \approx 1.66$ と突出して高い値を示している．

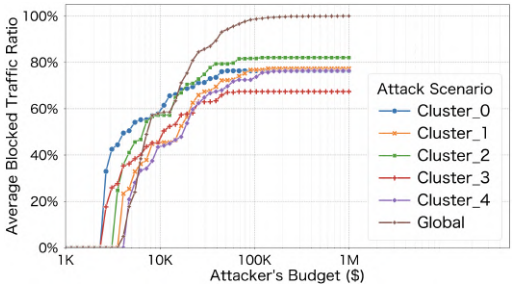
1 つのノードから接続されるエッジ数が多い（すなわち R の値が高い）ことは，ネットワーク構造が複雑であり，迂回経路が豊富に存在することを意味する．これにより，攻撃者が Target Link を溢れさせるために必要なボット数や経路数が増加し，結果として平均遮断トラヒック量比率が低く抑えられていると結論付けられる．

c） 連結 TA 数の爆発的増加と遮断率の推移

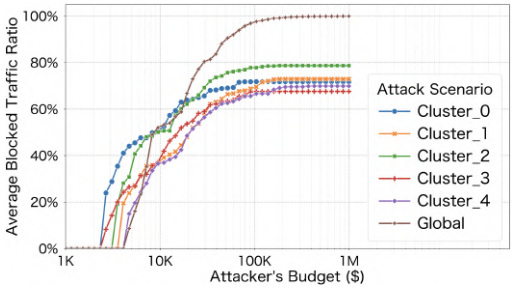
ネットワークの複雑さは，連結 TA（有効なターゲット候補）の数にも表れている．表 4 の通り，TA サイズ 5 において，他のネットワークが数百件程度であるのに対し，Allegiance Telecom のみ 7817 件と，膨大な数の連結 TA が存在している．また，TA サイズの推移による遮断率の変化に着目すると，TA サイズが 2 から 3 へ変化する際に遮断率が急激に低下する一方で，3 から 5 への変化による低下幅は比較的緩やかである．このことから，ある程度の複雑さを持つネットワークにおいては，TA サイズを大きくすることによる防御効果よりも，リンク密度が高いことによる防御効果の方が支配的であると言える．以上の分析より，Allegiance Telecom における低い攻撃成功率は，単なるノード規模の問題ではなく，高いリンク密度による構造的な堅牢性に起因するものであることが明らかとなった．

5.4 At Home Network における評価結果

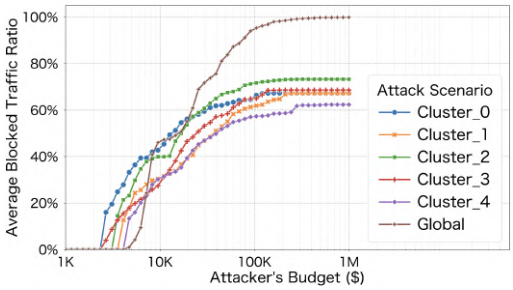
図 7 に，At Home Network において TA サイズを 2，3，5 と変化させた場合の評価結果を示す．



(a) TA Size 2



(b) TA Size 3



(c) TA Size 5

図 7: Comparison of Cost-Effectiveness by TA Size in At Home Network

a） 評価結果に見られる特異性

図 7 の結果において，他の Cluster では TA サイズの拡大や予算の増加に伴い遮断率が変動するのに対し，Cluster 3 を用いた攻撃シナリオでは，TA サイズや予算を変化させても平均遮断トラヒック量比率が約 70% 付近で停滞し，それ以上の成果が得られないという傾向が示された．

b） 到達不能通信トラフィックの割合による要因分析

Cluster 3 に見られる特異性の要因を明らかにするため，各 Cluster を攻撃元とした場合の，TA サイズと到着不能通信トラフィックの割合の関係を分析した．図 8 はその推移を示したものである．

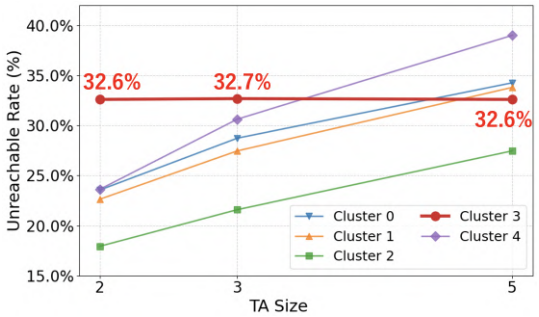


図 8: Transition of Unreachable Rate with Varying TA Sizes

このグラフから読み取れるように，Cluster 3 以外の攻撃元（Cluster 0，1，2，4）では，TA サイズが大きくなるにつれて，ターゲットへ届かなくなる通信の割合が右肩上がりに増加している．これは，TA が広域化することでボットから TA までのネットワーク内の迂回経路が増加し，攻撃パケットが Target Link を回避する確率が高まるためである．一方で，Cluster 3 のみ値が約 33% で横ばいとなっており，TA サイズを増加させた場合でも，到達不可能な通信の割合が増加していない．

c） 構造的要因と攻撃特性

到達不可能な通信の割合が増加しないという特性こそが，攻撃者が TA サイズを大きく設定した際に，Cluster 3 以外の Cluster では平均遮断トラヒック量比率の値が大きく下落しているのに対し，Cluster 3 のみが値を維持している主たる要因である．表 3 より，Cluster 3 は東海岸南部に位置し，主要な Target Link に対して地理的に近接している．この位置関係により，初期段階から約 3 割のトラフィックが構造的にターゲットへ到達しないため，全体の遮断率は約 70% で頭打ちとなる．しかし，この構造的限界は，ターゲットの規模を拡大してもそれ以上悪化しないという特性も意味している．結論として，Cluster 3 は最大火力こそ他の Cluster に劣るが，攻撃者がより広範囲（大規模 TA）をターゲットとして設定した場合であっても，その規模変化の影響を受けにくく，極めて安定した攻撃能力を維持し続ける特性を持つことが示唆された．

6. ま と め

本稿では，Crossfire Attack (CFA) に対するネットワークの脆弱性を評価するため，攻撃者の視点に立ち，ネットワーク構造，ボットの地理的分布，および攻撃予算という多角的な観点からシミュレーション評価を行った．本節では，得られた知見を以下の 3 つの観点から総括する．

6.1 ネットワーク構造と堅牢性の関係

ネットワークの構造的特性と CFA に対する耐性の関係について，ノード数に対するエッジ数の割合（リンク密度）が決定的な要因であることが明らかとなった．Allegiance Telecom の事例が示すように，リンク密度の比率が高いネットワークほど，迂回経路の選択肢が豊富に存在するため，攻撃による通信遮断が発生しにくくなる．具体的には，リンク密度が増加するにつれて，ネットワーク全体の平均遮断トラヒック量割合は低下する傾向にある．このことから，CFA に対する堅牢性を確保するための防御策として，単にリンク容量を増強するだけでなく，リンクの冗長性を高め，構造的な複雑さを持たせることが有効な手段であると言える．

6.2 ボットの地理的分布における攻撃可能エリアの推移

ボットの地理的配置と TA の規模との関係において，攻撃到達性は一様ではなく，攻撃元の位置関係に強く依存することが確認された．At Home Network における評価結果が示すように，一般的な攻撃シナリオでは，TA サイズが増加するに伴い，ターゲットへの経路が分散するため，到達不可能な通信の割合が増加し，攻撃効率は低下する．しかし，Cluster 3（東海岸南部）のように，主要な Target Link に対して地理的に近接し，かつ構造的な近接回避が発生する位置にあるボット群においては，TA サイズを増加させても到達不可能な通信の割合が変化せず，横ばいで推移するといった性質が見られた．これは，特定の地理的条件下においては，攻撃者が TA の規模を拡大しても，攻撃の到達性を低減させる比率が限定的であることを示唆している．

6.3 攻撃者の予算増加に伴う最適な攻撃戦略の変化

攻撃者の予算規模（動員可能なボット数）と攻撃効率の関係は線形ではなく，予算の多寡によって最適な攻撃拠点が変化することが明らかとなった．AGIS ネットワークにおける Cluster 2（西海岸）の事例では，低予算時には地理的な偏りと経路分散により，他のエリアと比較して低い遮断率しか記録できなかった．しかし，予算が増加し，大量のボットを動員可能になった段階で，その評価は逆転し，高い遮断トラヒック量比率を記録する高効率な攻撃拠点へと変化した．このことから，攻撃者にとっての最適な戦略は固定的なものではなく，自身の予算規模に応じて，分散型（低予算時）から集中型（高予算時）へと，攻撃に使用するボットの選定エリアを動的に変更する必要があることが示された．

6.4 総　　括

以上の特徴は，特定のネットワークに限らず，CFA の原理上，他の一般的なネットワークに対しても適用可能な知見である．ネットワーク上で特定地域の孤立を狙う CFA の攻撃者にとって，標的となるネットワークのリンク密度，自身のボットが配置された地理的・構造的位置関係，および動員可能な予算規模の 3 要素を総合的に分析し，これらの特徴に基づいた攻撃戦略を立案することで，費用対効果（ROI）を最大化する攻撃が可能となる．逆に防御側にとっては，これらの攻撃特性を逆手に取り，構造的な複雑性の向上や，攻撃効率が高まる特定のボトルネック箇所の重点的な監視や補強といった対策が求められる．

謝辞　本研究は JSPS 科研費（25K03113, 23K28078）の助成を受けたものである．ここに記して謝意を表す．

文　　献

[1] M. S. Kang, S. B. Lee, and V. D. Gligor, ”The Crossfire Attack,” in *Proc. IEEE Symposium on Security and Privacy*, 2013, pp. 127-141.

[2] Wang Tianyu, 上山 憲昭, “クロスファイア攻撃に対して脆弱なエリアの GCN を用いた選定法“, 信学会 IA 研究会, IA2024-67, 奄美大島, 2025 年 3 月

[3] A. R. Narayanadoss, T. Truong-Huu, P. M. Mohan, and M. Gurusamy, ”Crossfire Attack Detection Using Deep Learning in Software Defined ITS Networks,” in *Proc. IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, Kuala Lumpur, Malaysia, 2019.

[4] M. Rezazad, M. R. Brust, M. Akbari, P. Bouvry, and N.-M. Cheung, ”Detecting Target-Area Link-Flooding DDoS Attacks using Traffic Analysis and Supervised Learning,” *arXiv preprint arXiv:1903.01550*, 2019.

[5] W. Rafique, X. He, Z. Liu, Y. Sun, and W. Dou, ”CFA Defense: A Security Solution to Detect and Mitigate Crossfire Attacks in Software-Defined IoT-Edge Infrastructure,” in *Proc. IEEE 21st International Conference on High Performance Computing and Communications (HPCC)*, 2019.

[6] K. Sakuma, H. Asahina, S. Haruta, and I. Sasase, ”Traceroute-based Target Link Flooding Attack Detection Scheme by Analyzing Hop Count to the Destination,” in *Proc. 23rd Asia-Pacific Conference on Communications (APCC)*, Perth, Australia, 2017.

[7] A. Aydeger, N. Saputro, K. Akkaya, and M. Rahman, ”Mitigating Crossfire Attacks Using SDN-Based Moving Target Defense,” in *Proc. IEEE 41st Conference on Local Computer Networks (LCN)*, 2016.

[8] L. Guo, S. Jing, L. Wei, and C. Zhao, ”Crossfire Attack Defense Method Based on Virtual Topology,” in *Proc. 19th International Conference on Mobility, Sensing and Networking (MSN)*, 2023.

[9] H. Qiao and X. Xu, ”Security-oriented Deception on Network Topology against Crossfire Attack,” in *Proc. 4th International Symposium on Computer Engineering and Intelligent Communications (ISCEIC)*, 2023.

[10] J. Caballero, C. Grier, C. Kreibich, and V. Paxson, ”Measuring Pay-per-Install: The Commoditization of Malware Distribution,” in *Proc. 20th USENIX Security Symposium*, 2011.