5ZC-02

暗号通貨ネットワークにおける Eclipse 攻撃に対するルーティングテーブルシミュレーション

松岡 主馬 *1　　鈴木 常彦 †1　　伊藤 秀昭 ‡1

[1] 中京大学工学研究科 §

1　はじめに

暗号通貨ネットワークに定義されているノードのルーティングテーブルを，攻撃者の情報で埋めることにより，そのノードをネットワークから分離する Eclipse 攻撃が 2015 年に提案された [2]．本論文では，Bitcoin[1] に基づくネットワーク情報を用いて，任意の規模の攻撃者とその標的を設定できる Eclipse 攻撃のシミュレータを作成した．さらに，Eclipse 攻撃の対策について検討をした．

2　Eclipse 攻撃

Eclipse 攻撃は，十分な数の IP アドレスリソースを制御する攻撃者が標的ノードのすべてのピア接続を独占して，標的ノードをネットワーク上の他のノードから孤立させる攻撃である．攻撃が成功すると，攻撃者は孤立した標的ノードに正しくデータを伝搬しなかったり，暗号通貨の二重使用などの二次攻撃を起こす可能性がある．

[2] では，Eclipse 攻撃の対策として 10 個の手段を提案しており，そのうちのいくつかは Bitcoin クライアントソフトウェアのパッチとして実装されている [3][4]．

3　シミュレータの作成

Bitcoin ノードの IP アドレス情報を使用して，任意の規模の攻撃者とその標的を設定できる Eclipse 攻撃のシミュレータを作成した．シミュレータ内のノードは，ピア接続しているノードを格納するテーブル（ルーティングテーブル）と，将来新たにピア接続をする可能性がある候補ノードを格納するテーブル（予備テーブル）とを有している．シミュレーション開始時に，自動的にこれらのテーブルを作成する．

攻撃者の目的は，攻撃の標的となるノードのルーティングテーブルを，攻撃者のノードで占領することである．標的ノードの予備テーブルを占領することは，標的ノードが新しいピア接続を選択する際に攻撃者ノードを選択する確率が高まるので攻撃として有効である．これを実現するために攻撃者は，標的ノードにピア接続を常に試みる．

4　Eclipse 攻撃の対策と検証

この節では，本研究で作成したシミュレータを用いて，Eclipse 攻撃対策の検討と対策の効果を測定したシミュレーション結果を示す．ルーティングテーブルへの占領率の推移を図 1 に示す．占領率は，標的であるノード群のルーティングテーブルに攻撃者ノードが占めている割合である．図 1 は，本章で紹介する各対策を施したとき，時間経過に伴う占領率がいかに変化するかを示している．

対策を施していないときのシミュレーション結果を図 1 の「対策なし」に示している．対策をしていない場合は，24 時間後の占領率が約 60% であった．

4.1　対策 1：予備テーブル挿入制限

対策 1 は，予備テーブルにノード情報を追加するために制限を設ける方法である．すなわち，予備テーブルのサイズが指定された閾値以上であるとき，外部から受け取った新しいノード情報を予備テーブルに追加できなくする．これによって，攻撃者ノードは標的ノードの予備テーブルに空きがあったとしてもノード情報を挿入できない．

図 2 は，各対策を施したときに予備テーブルの占領率がどのように変化するかを示している．対策 1 を施すことで，予備テーブルへの攻撃を鈍化できる．しかし，ルーティングテーブルへの攻撃には効果が小さいことが図 1 で示された．したがって，対策 1 のみを施すことは，攻撃の対策としては効果が小さいことが示唆される．

4.2　対策 2：広告

対策 2 は，一定間隔ごとに自分の情報をピア接続先に広告して新しい接続先情報を取得する対策である．各ノードは一定間隔ごとにノードのルーティングテーブルからランダムにピアを α 個選び（攻撃者ノードが選択される場合がある），それぞれのピアから新しいノード情報を β 個ずつ取得する．

図 1 から，対策 2 ($\alpha = 2, \beta = 2$) のときは，24 時間後の占領率が約 22% であり，対策 2 を施していない場合の占領率が約 60% である．したがって，対策 2 が攻

Routing Table Simulation against Eclipse Attacks in Cryptocurrency Networks

* Kazuma Matsuoka
† Tsunehiko Suzuki
‡ Hideaki Ito
§ Graduate School of Engineering, Chukyo University

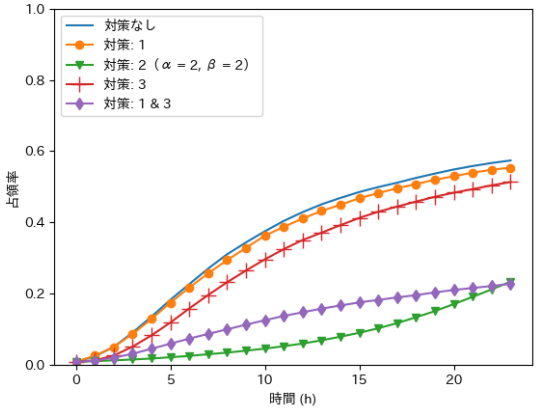

図 1　ルーティングテーブル占領率の推移

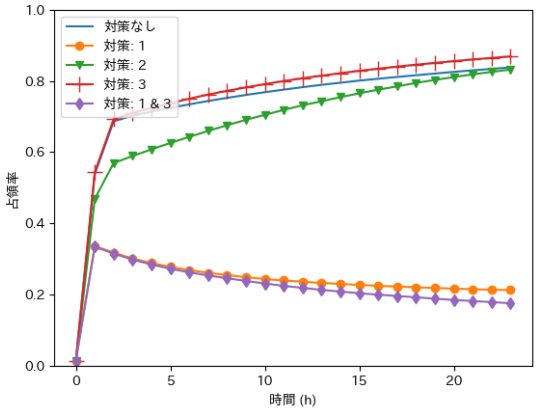

図 2　予備テーブル占領率の推移

撃に対して効果があることが示された．

α と β の値を変えて占領率の変化を検証した結果を図 3 に示す．α と β の値を増やすと，ルーティングテーブルへの占領率が鈍化することが示された．ただし，$(\alpha = 2, \beta = 2)$ と $(\alpha = 3, \beta = 2)$ を比較すると，占領率の変化が少ないことから，単に広告するノード情報数を増やしても対策として有効ではなく，広告する数（α と β）を調節する必要がある．

4.3　対策 3：ピア接続の制限

対策 3 は，ルーティングテーブルへのノード情報を追加するとき，外部からの直接ピア接続を禁止する，という制限を設ける対策である．対策 3 を施していない場合にピア接続が増える場面は 2 つある．1 つ目は外部から直接ピア接続要求をされたときである．2 つ目は，ノードの予備テーブルからピア接続相手を選択するときである．

図 1 から，対策 3 のみを適用した場合は，占領率を低下させる効果が限られていることがわかる．対策 3 を施すのみでは，攻撃者は標的ノードの予備テーブルに空きがあるとき，自由にノード情報を挿入できる．したがって，対策 3 のみでは Eclipse 攻撃の対策としては不十分である．そこで，予備テーブルへの挿入を制限する対策 1 と対策 3 を併用した場合，予備テーブルの占領率が低下する（図 2 参照）．その結果として，ルーティングテーブルへの占領率が大きく減少している（図 1 参照）．

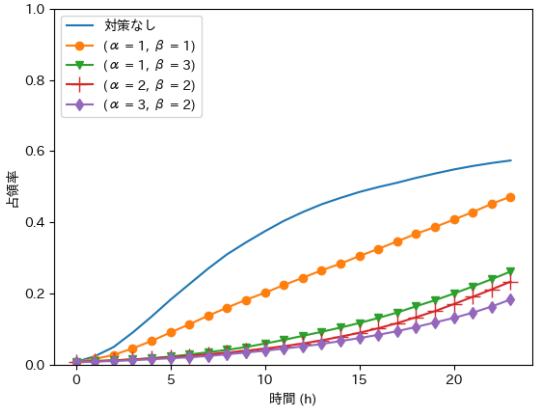

図 3　対策 2 の効果

5　まとめ

本研究では，実際の Bitcoin クライアント情報を用いて Eclipse 攻撃のシミュレータを作成した．Eclipse 攻撃に対する対策としては，定期的に自分の情報をピア接続している他のノードに広告する対策 2 が効果的であることが示された．また，予備テーブルへの挿入制限だけでは対策としては不十分であるが，ピア接続に関する制限を組み合わせることで占領率が低下することが示された．[2] は Bitcoin のみを対象にした対策を提案している．本研究では，特定の暗号通貨システムを想定していない．本研究で検証した対策は，Eclipse 攻撃の対策を全く行なっていないシステムに対して有効である．

今後の研究として，実際の暗号通貨に対しての対策を検討するために，各暗号通貨クライアントのピア接続に関する実装を比較する必要がある．

参考文献

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, 2022 年 12 月 28 日参照.

[2] Heilman, Ethan, et al. “Eclipse attacks on Bitcoin’s peer-to-peer network.” 24th USENIX Security Symposium (USENIX Security 15), 2015.

[3] https://bitcoin.org/en/release/v0.10.1, 2022 年 12 月 28 日参照.

[4] Heilman, E. Bitcoin: Added test-before-evict discipline in addrman, feeler connections. https://github.com/bitcoin/bitcoin/pull/6355, 2022 年 12 月 28 日参照.