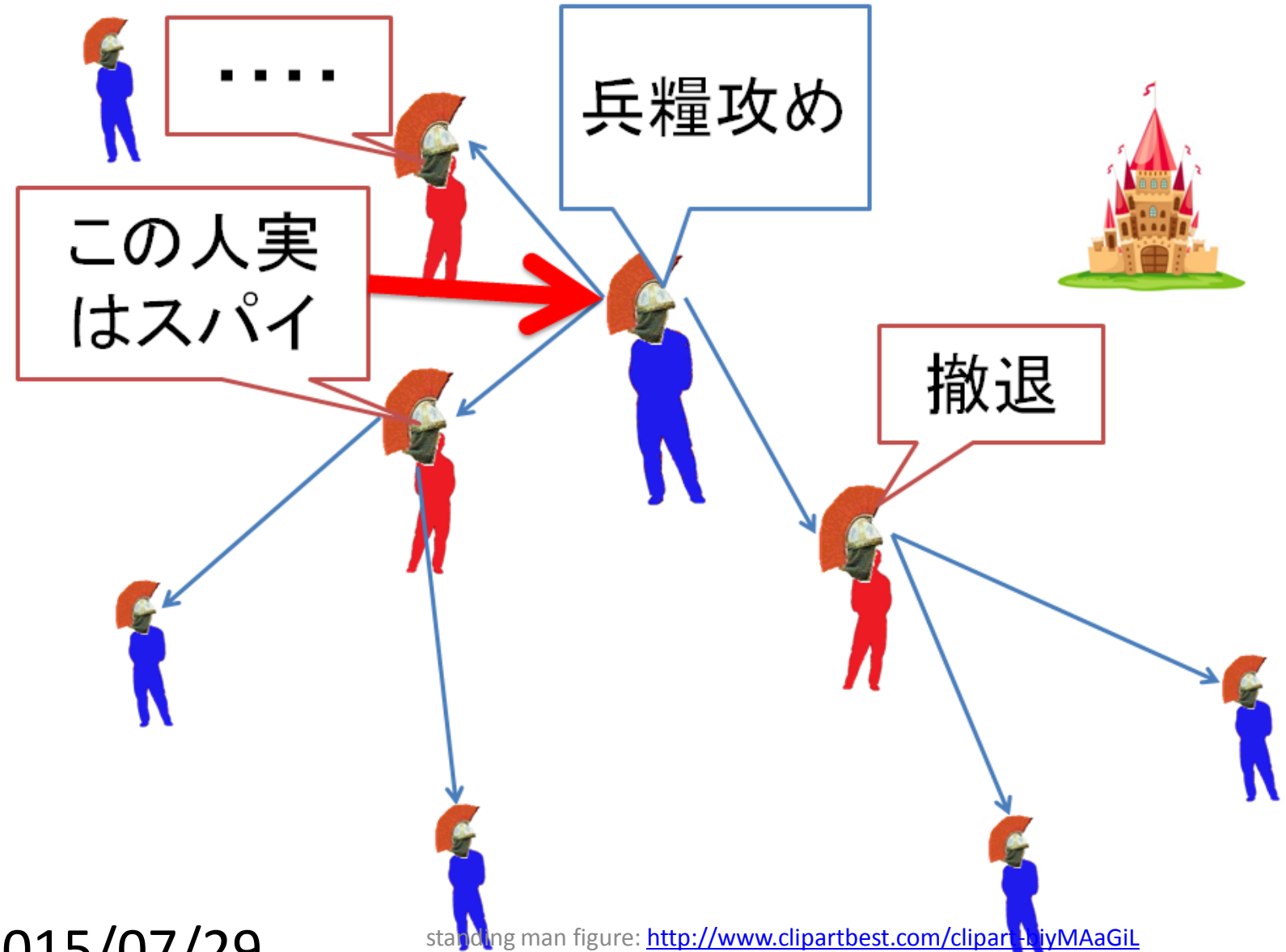
単一グローバル台帳暗号通貨のエクリプス攻撃脆弱性分析

Analysis of Eclipse-Attack Vulnerability on Single Global Ledger Cryptocurrencies

修士論文最終発表

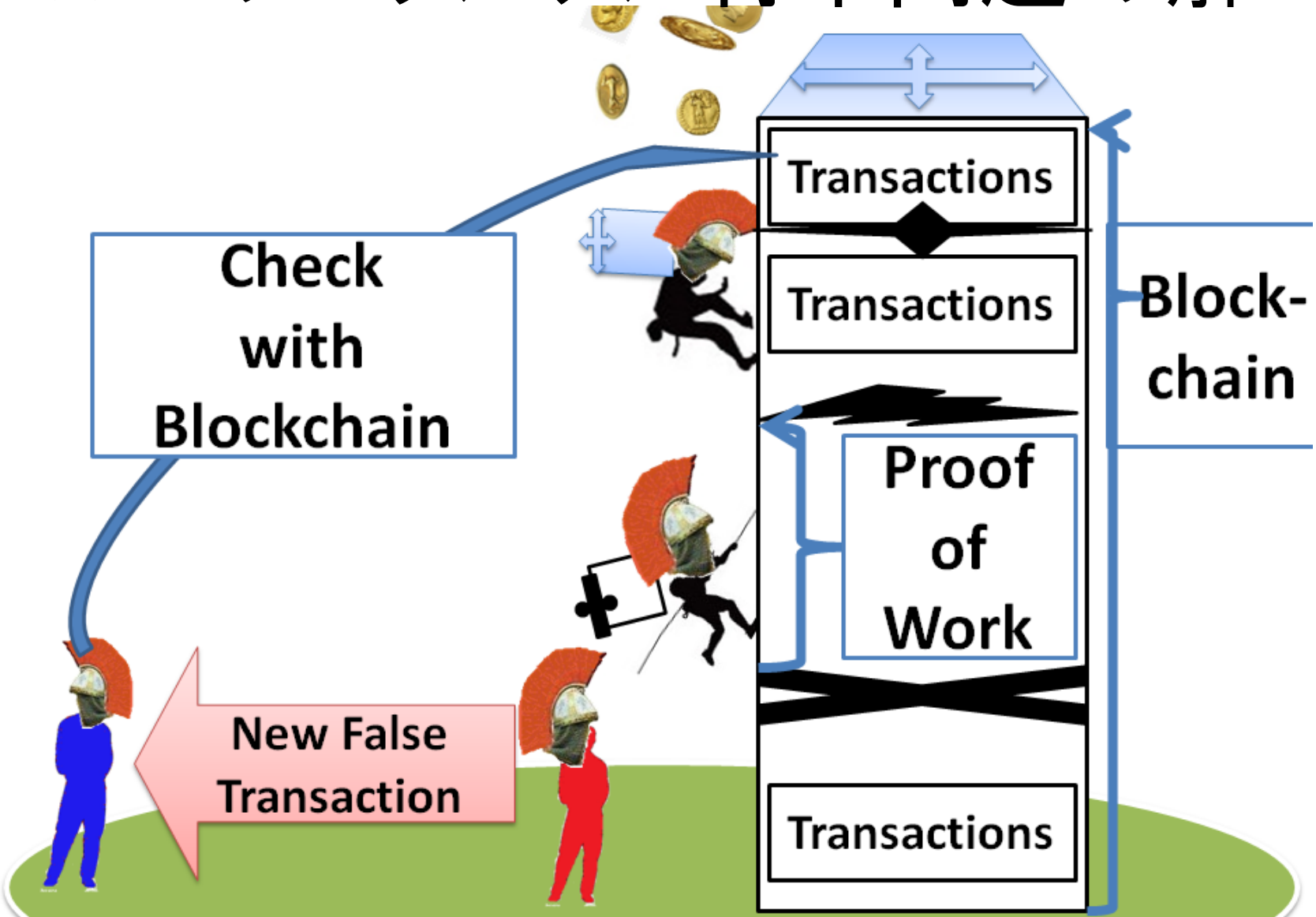
政策・メディア研究科　修士2年
村井純　研究室所属
澁田　拓也

P2Pの抱えるビザンチン将軍問題



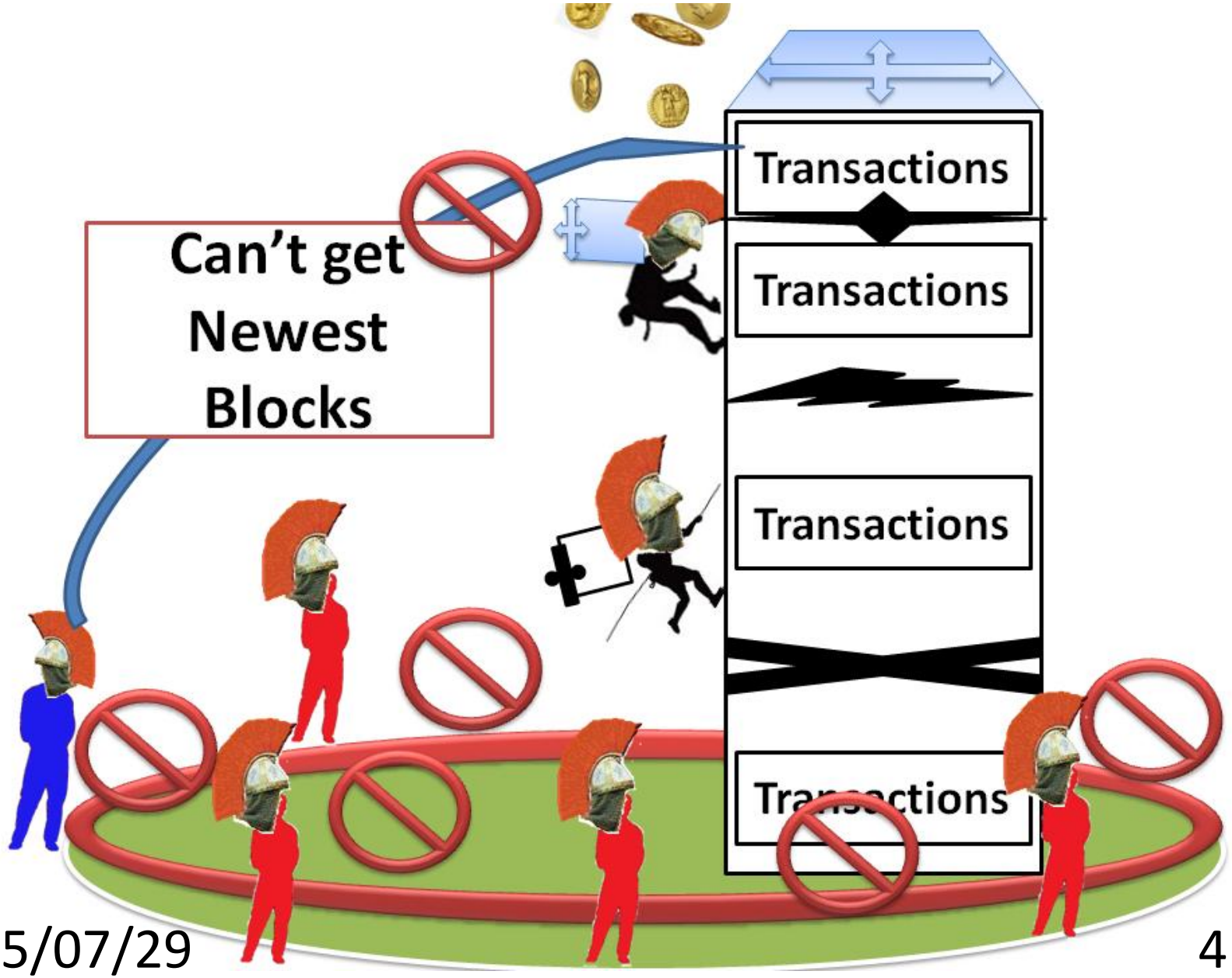
standing man figure: http://www.clipartbest.com/clipart-iiyMAaGiL
castle figure: 3lian.com http://free-illustrations.gatag.net/2014/01/11/020000.html

Bitcoinのビザンチン将軍問題の解



Supposedly post by Satoshi Nakamoto:
http://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html
climbers: http://kage-design.com/wp/?p=1648#more-1648

それがエクリプス攻撃に弱い



Bitcoinは、暗号に取り組んでる方などが作っているので、

エクリプス攻撃対策が不十分

エクリプス攻撃で多大な被害

Bitcoinとかを如何にエクリプス攻撃に対して強く出来るか

それを

- エクリプス攻撃に関する考察、段階分け
- 个に基づいた包括的なフレームワーク
- 構造化と体系だった防衛戦略と防衛機構群

今後のエクリプス攻撃の研究の基礎となるフレームワークによる貢献

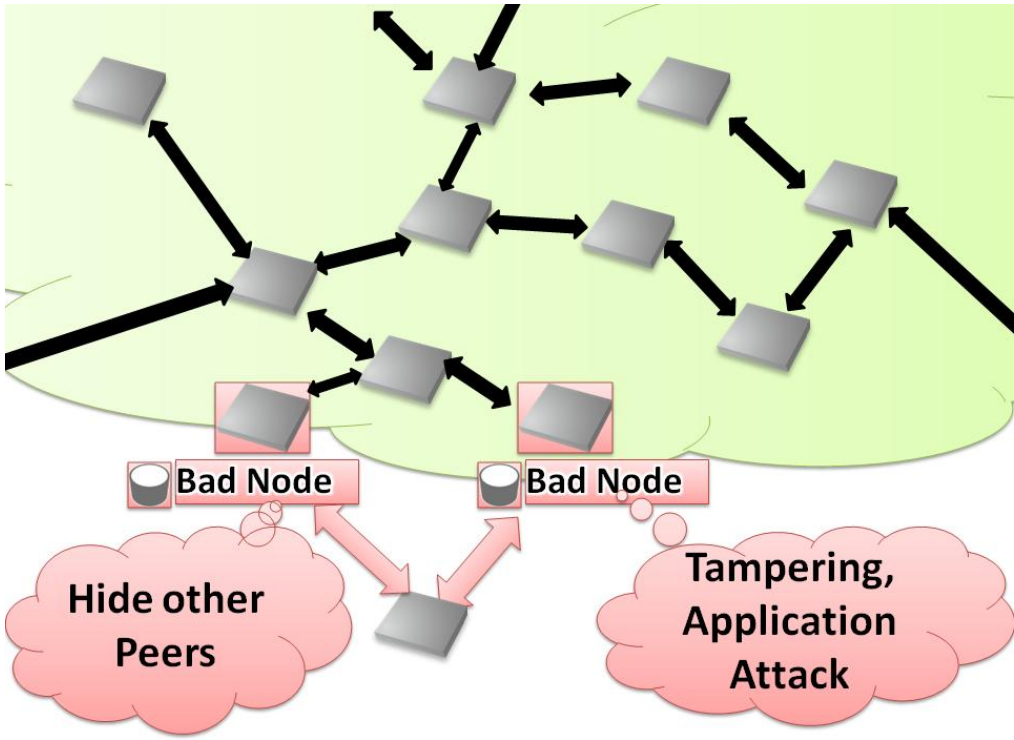
エクリプス攻撃とは

- P2P特有の攻撃
- システム/ネットワークの
  - 他ノード
  - オブジェクト等の情報を

トラフィックの掌握により

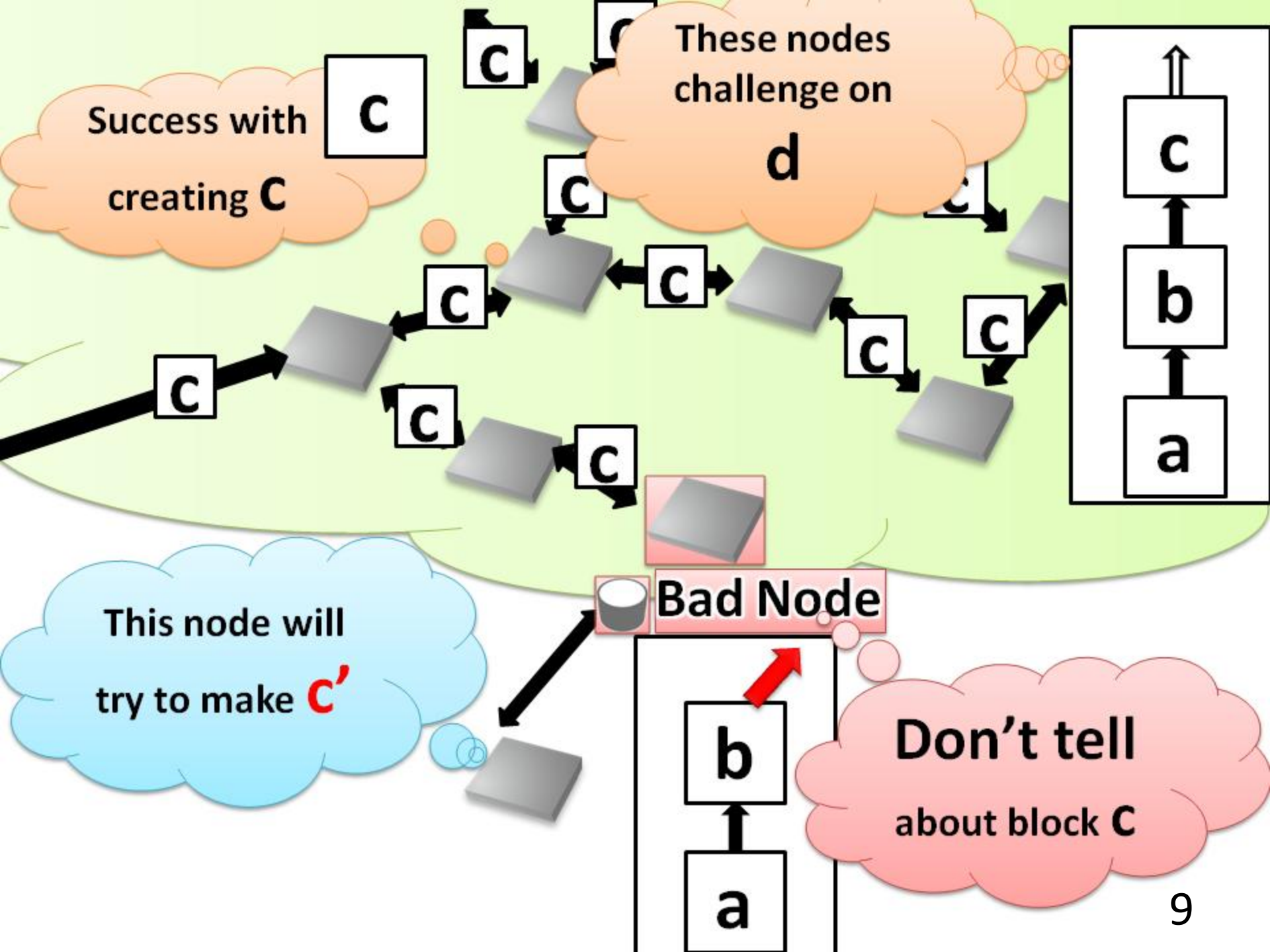
- 秘匿
- 改竄
- 偽情報の送付

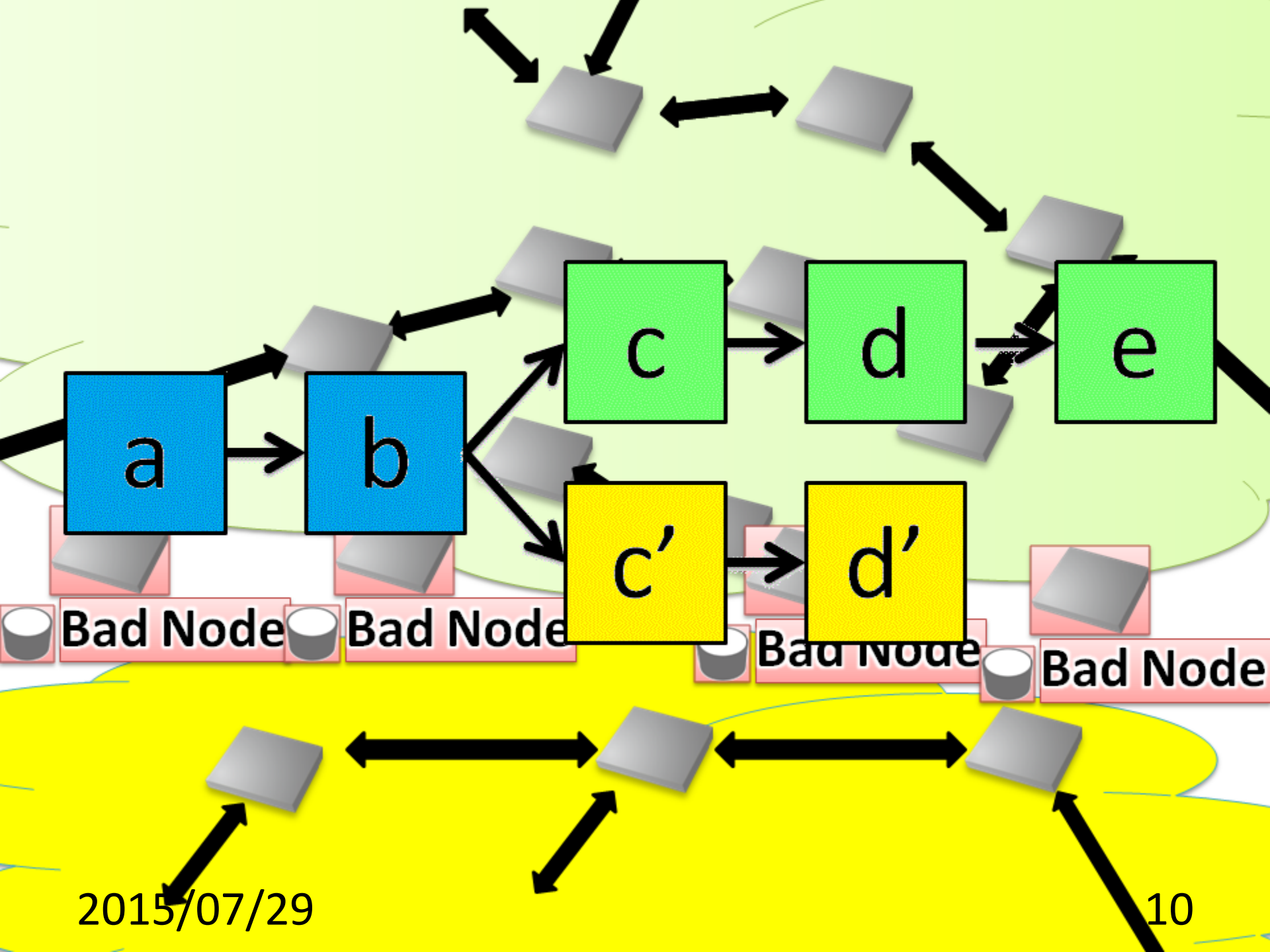
等を行う

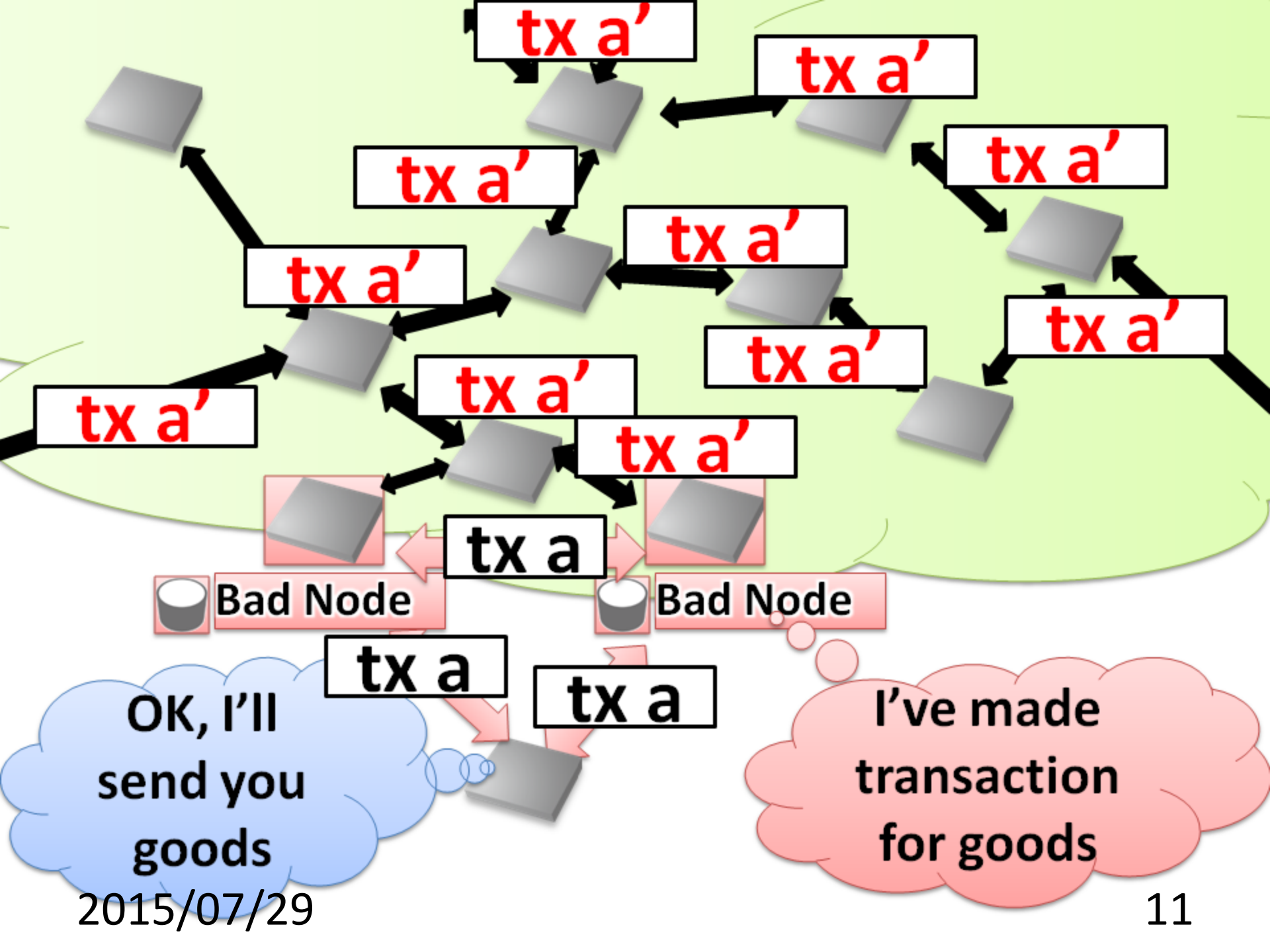


Nodes' figures by Japanese InterOp ShowNet Team:
http://www.f2ff.jp/interop/2014/noc/shownet-topology-map_5.php

Bitcoinがエクリプス攻撃されると


Success with creating C
C
These nodes challenge on d
c
b
a
This node will try to make C'
Bad Node
Don't tell about block C


a
b
c
d
e
c’
d’
Bad Node
Bad Node
Bad Node
Bad Node


tx a'
tx a'
tx a'
tx a'
tx a'
tx a'
tx a'
tx a'
tx a'
tx a'
tx a
Bad Node
Bad Node
tx a
tx a
OK, I'll send you goods
I've made transaction for goods

Heilman et al. の先行研究

“*Trash*”: Bitcoinネットワークに属しないIPアドレス

多数のノードに連続的に短期接続を行わせ、
*Trash*の多量送付によりアドレステーブルを汚染

対外接続スロットとアドレス管理により防衛

Connection枯渇攻撃の可能性を指摘

Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on bitcoin’s peer-to-peer network. 3 2015.

Heilman et al. の防衛策が導入されたが、それでも尚現状、

原理上117ノードあればBitcoinネットワークの全Connectionを枯渇させられる

Singh et al. のエクリプス攻撃に対する防衛

エクリプス攻撃
ノードの洞察

洞察を素にした
防衛戦略

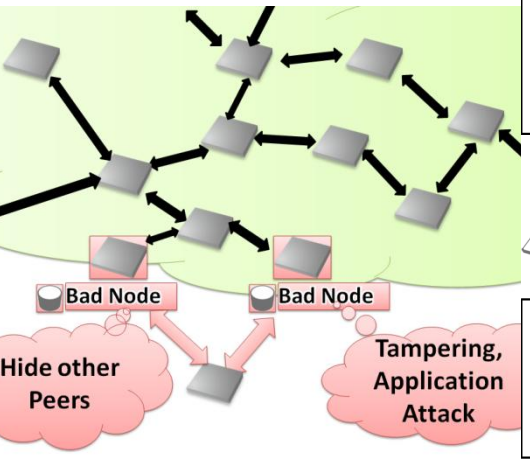
防衛戦略を素に
した防衛機構

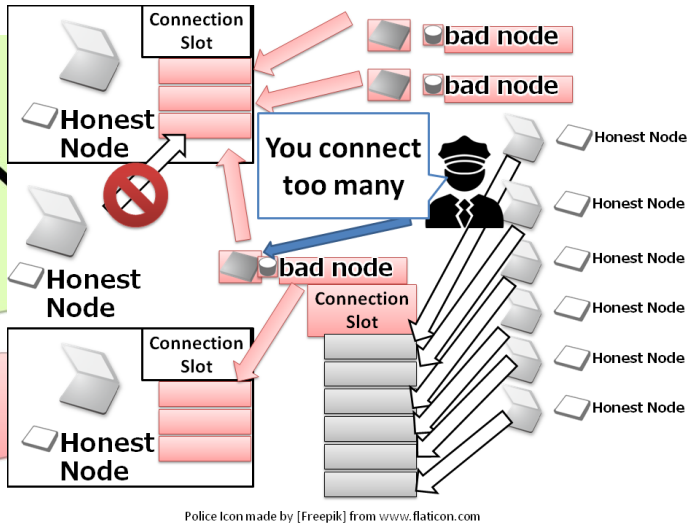
Eclipse Attack

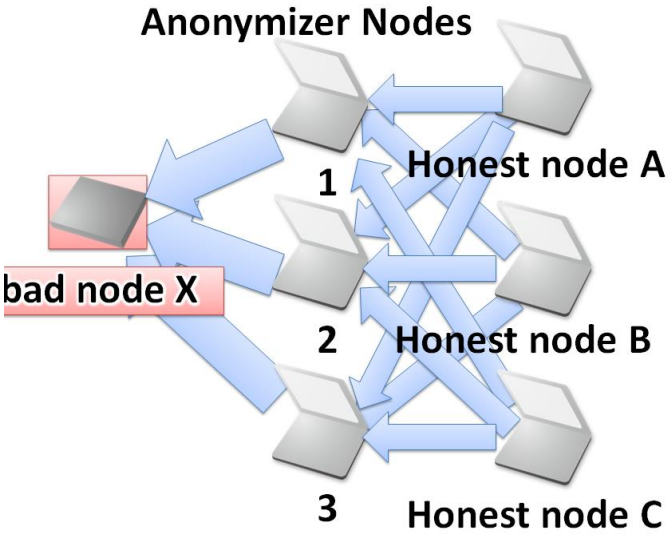
Degree Consumption

Degree Bounding

Anonymous Auditing







Atul Singh, Miguel Castro, Peter Druschel, and Antony Towstron. Defending against eclipse attacks on overlay networks. *Proceedings of the 11th ACM SIGOPS European Workshop, 9 2004.*

Singh et al. のモデルは体系だっているが

- エクリプス攻撃の一側面のみ
- 且つ構造型P2Pのみに対応

- 非構造型P2Pに対応し
- より包括的な防衛戦略

が求められる

本研究の仕事

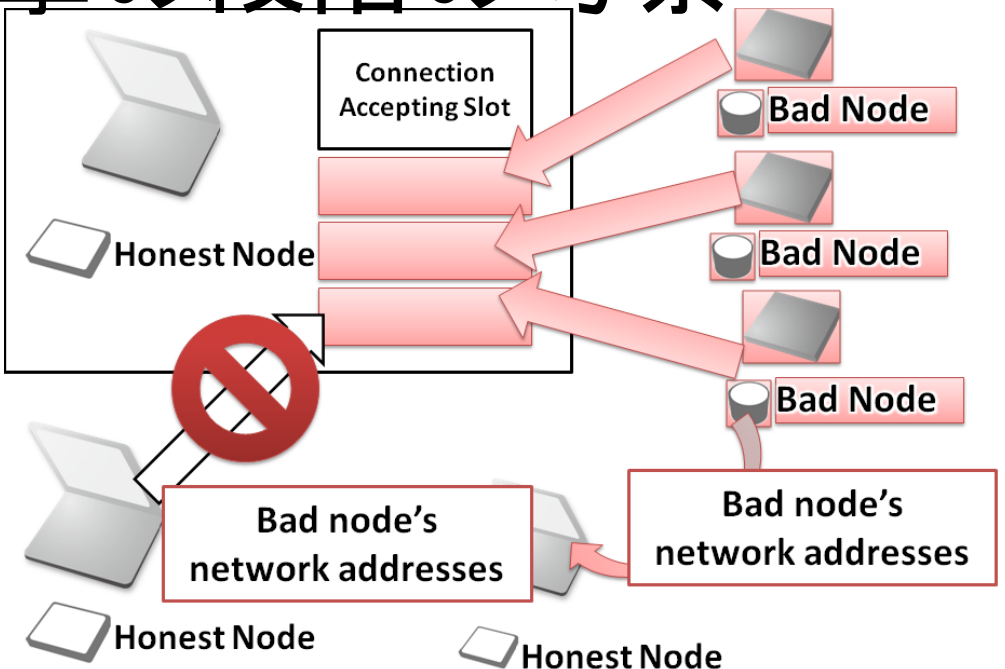
Bitcoin等を標的としたエクリプス攻撃防衛を、

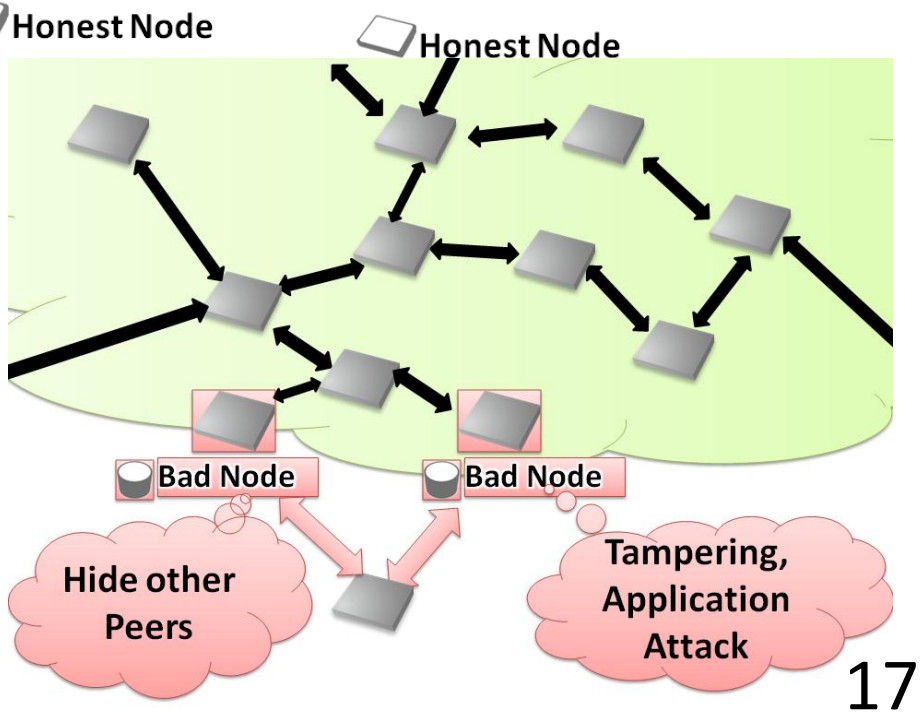
- エクリプス攻撃に関する考察、段階分け
- 个に基づいた包括的なフレームワーク
- 構造化と体系だった防衛戦略と防衛機構群

今後のエクリプス攻撃の研究の基礎となるフレームワーク

エクリプス攻撃の段階の考察

- 接続誘導
- Connection枯渇攻撃
- トラフィックの完全支配
- 意図的な情報操作





2015/07/29

エクリプス攻撃の本質は

正常なP2Pネットワークからの標的の

・分断

・孤立

による トラフィックの掌握・制御なので、

・接続対象の **多様化** / **安定化**

・接続誘導 / Connection枯渇 の**検知**

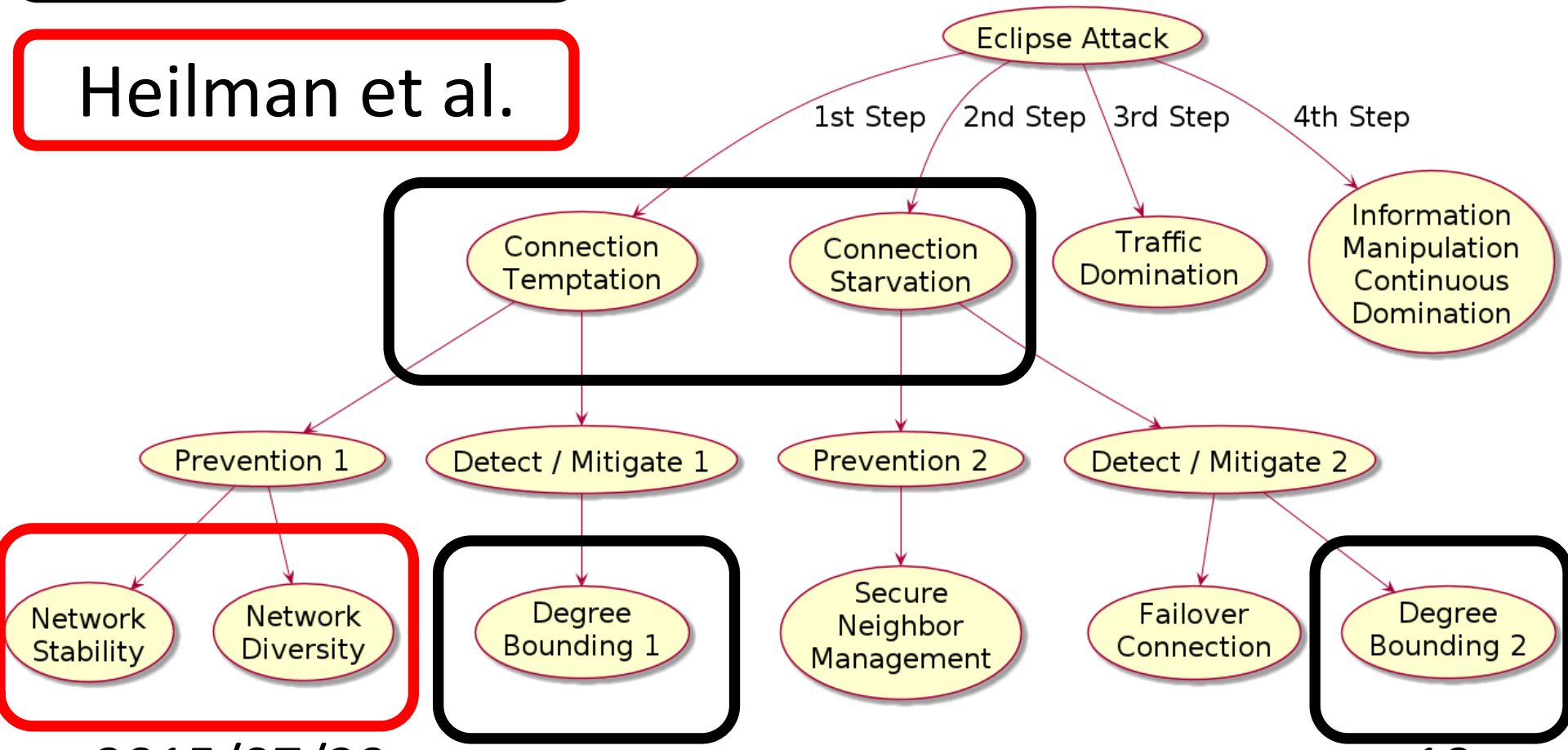
・非常時の通信チャンネル

により **[予防]** / **[対応]** が可能

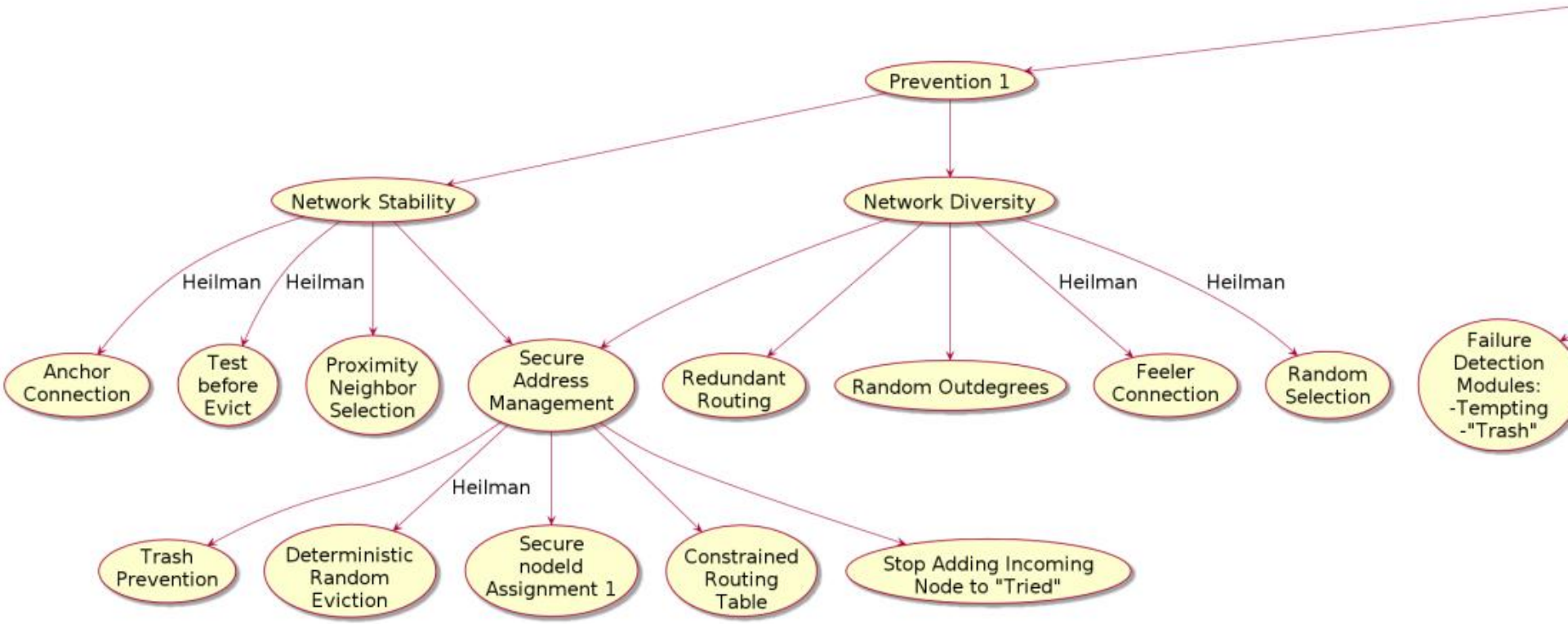
Singh et al. の研究をベースにエクリプス攻撃段階分けして、モデルを発展させてみた

Singh et al.

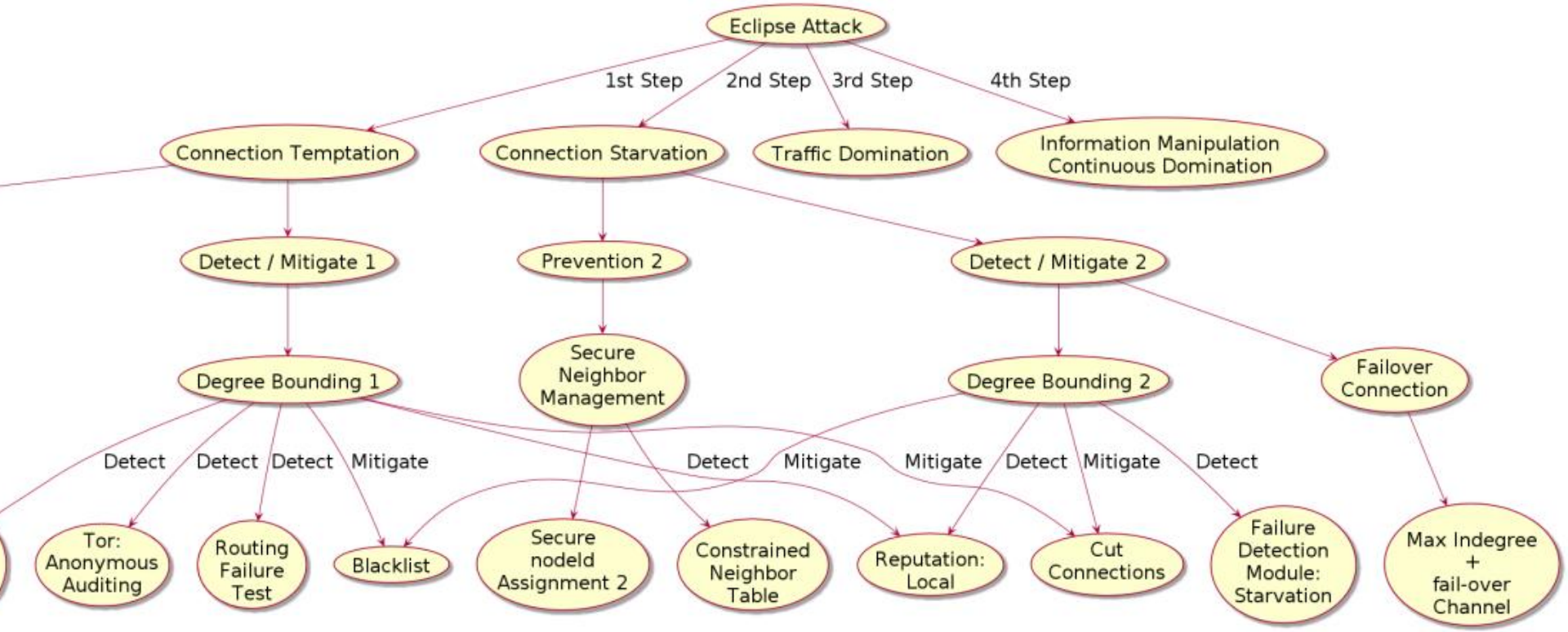
Heilman et al.



防衛機構群


Prevention 1
Network Stability
Network Diversity
Heilman
Heilman
Heilman
Heilman
Heilman
Anchor Connection
Test before Evict
Proximity Neighbor Selection
Secure Address Management
Redundant Routing
Random Outdegrees
Feeler Connection
Random Selection
Failure Detection Modules: -Tempting -"Trash"
Heilman
Trash Prevention
Deterministic Random Eviction
Secure nodeId Assignment 1
Constrained Routing Table
Stop Adding Incoming Node to "Tried"

防衛機構群


Eclipse Attack
1st Step
2nd Step
3rd Step
4th Step
Connection Temptation
Connection Starvation
Traffic Domination
Information Manipulation
Continuous Domination
Detect / Mitigate 1
Prevention 2
Detect / Mitigate 2
Degree Bounding 1
Secure
Neighbor
Management
Degree Bounding 2
Failover
Connection
Detect
Detect
Detect
Mitigate
Detect
Mitigate
Mitigate
Detect
Mitigate
Detect
Tor:
Anonymous
Auditing
Routing
Failure
Test
Blacklist
Secure
nodeId
Assignment 2
Constrained
Neighbor
Table
Reputation:
Local
Cut
Connections
Failure
Detection
Module:
Starvation
Max Indegree
+
fail-over
Channel

上位互換性のある防衛機構群

基本的に
　どのノードに接続するか
　どの様にアドレス情報を扱うか

- Heilman et al.’s defence
- Proximity Neighbor Selection(PNS)
- Randomized Max Outdegree
- Secure Address Management
- Modularized Attack Detector
  - Trash attack detector
- Secure Neighbor Management

上位互換性の無い防衛機構群

プロトコルに規定の無い
隣接ノード情報のやり取り

- Modularized Attack Detector
  - Tempting attack detector
  - Starvation attack detector

(自身の受付Connection枯渇時点で接続受付中のノードの疑わしさ評価だけなら上位互換性あり)

- Anonymous Auditing over Tor
- Failover Connection

(隣接ノードリスト受信以外なら上位互換性あり)

他のP2Pオーバーレイへの応用

IPプロトコルにより築き上げられた
インターネットの上で稼働する、

IPオーバーレイ・ネットワーク
でなら原理上応用可能

Worked / Researcher	Comprehensive Defence Strategy Eclipse attack in steps	Evaluati-on	Unstructured P2P	Degree Bounding	Secure NodeId	Other Defence
Shibuta. 2015	☑		☑	☑	☑	☑
Singh et al. 2006		☑		☑	☑	☑
Heilman et al. 2015		☑	☑			☑
Anceaume et al. 2011		☑		☑	☑	☑
Parmer et al. 2014				☑	☑	
Vhora et al. 2015				☑	☑	

貢献(終わり)

やった事

- エクリプス攻撃に関する考察、段階分け
- 个に基づいた包括的なフレームワーク
- 構造化と体系だった防衛戦略と防衛機構群

今後のエクリプス攻撃の研究の基礎となるフレームワークによる貢献

防衛機構群

接続誘導に対する
ネットワークの多様性及び安定性による予防

- Heilman等によるBitcoinのネットワーキング改善による防衛:
  - Anchor/Feeler Connections
  - Test before Evict
  - Random Selection
  - Deterministic Random Eviction
- Proximity Neighbor Selection(PNS)
- Randomized Max Outdegree
- Secure Address Management

Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. 3 2015.

接続誘導に対する モジュールとDegree Boundingによる検出/防衛

- モジュール化された攻撃検知機構
  - Trash attack detector
  - Tempting attack detector

- Torを用いたanonymous auditing

Vadim Drabkin, Roy Friedman, and Marc Segal. Efficient byzantine broadcasst in wireless ad-hoc networks. *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, pages 160–169, 2005.*

Connection枯渇攻撃への防衛

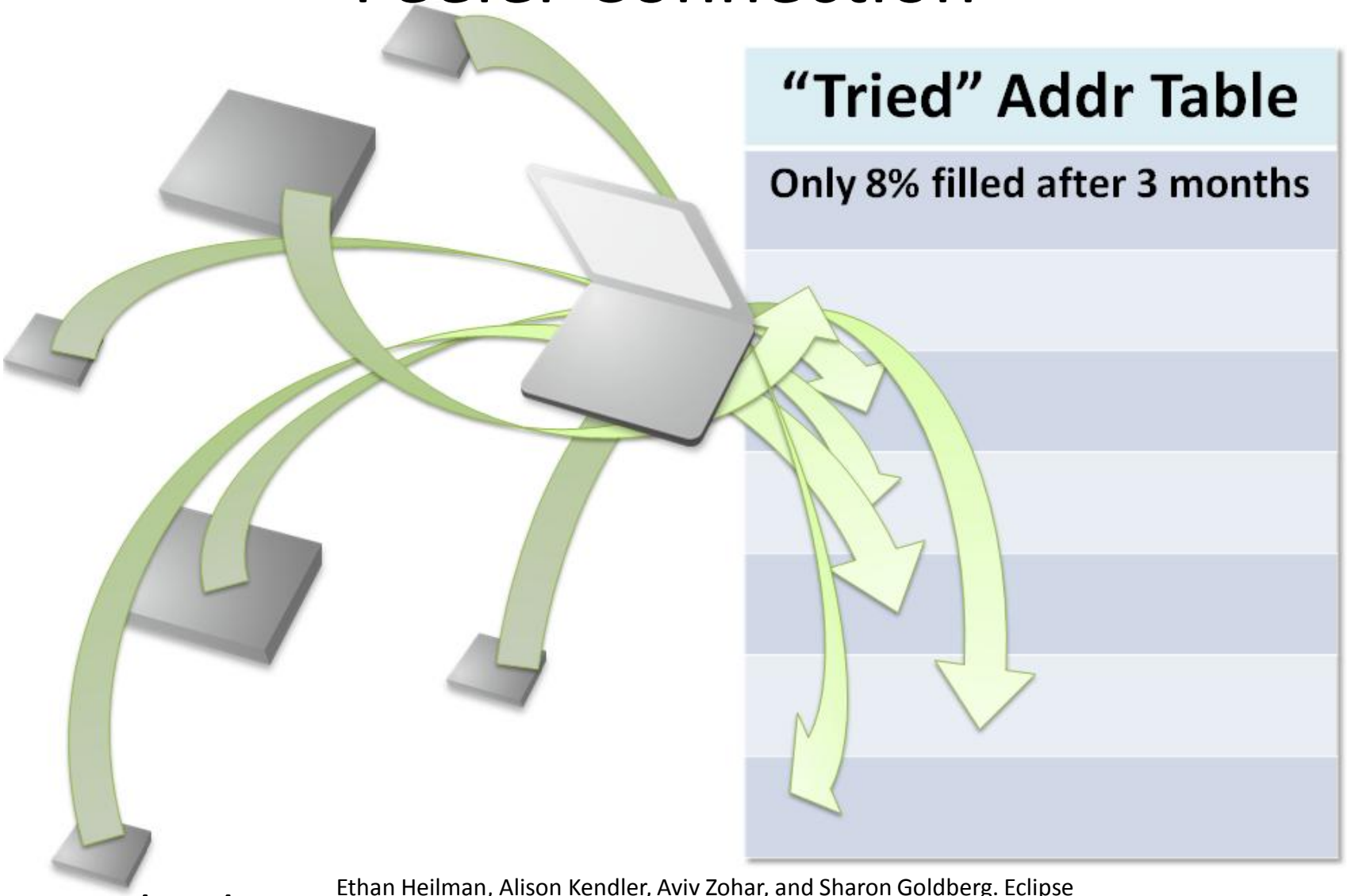
予防

- Secure Neighbor Management

検出/防衛

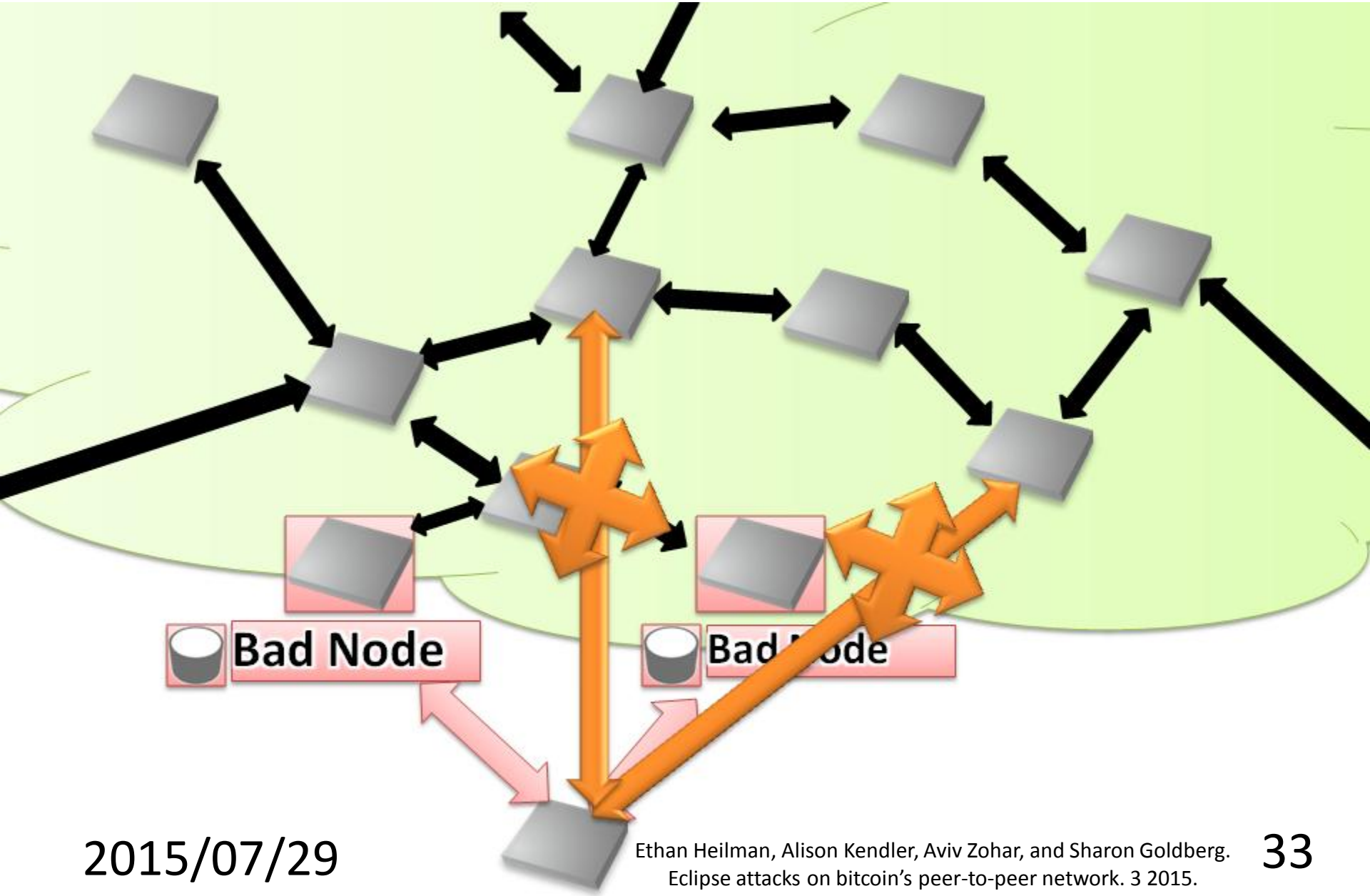
- Failover Connection
- 个を用いたConnection枯渇攻撃の確率論的検知
- モジュール化された攻撃検知機構
  - Starvation attack detector

Heilman et al.’s defence
Feeler Connection



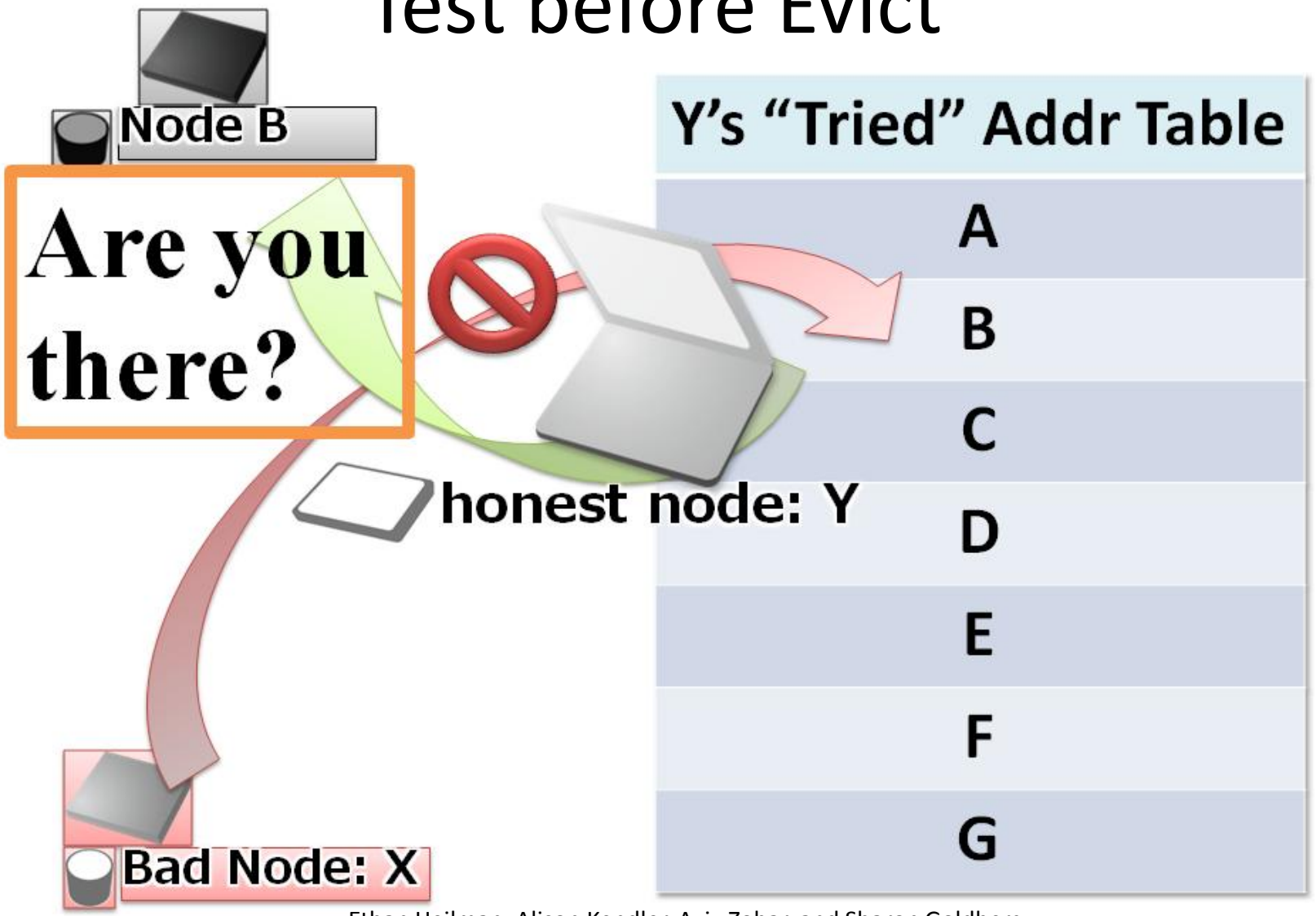
Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on bitcoin’s peer-to-peer network. 3 2015.

Heilman et al.'s defence
Anchor Connection



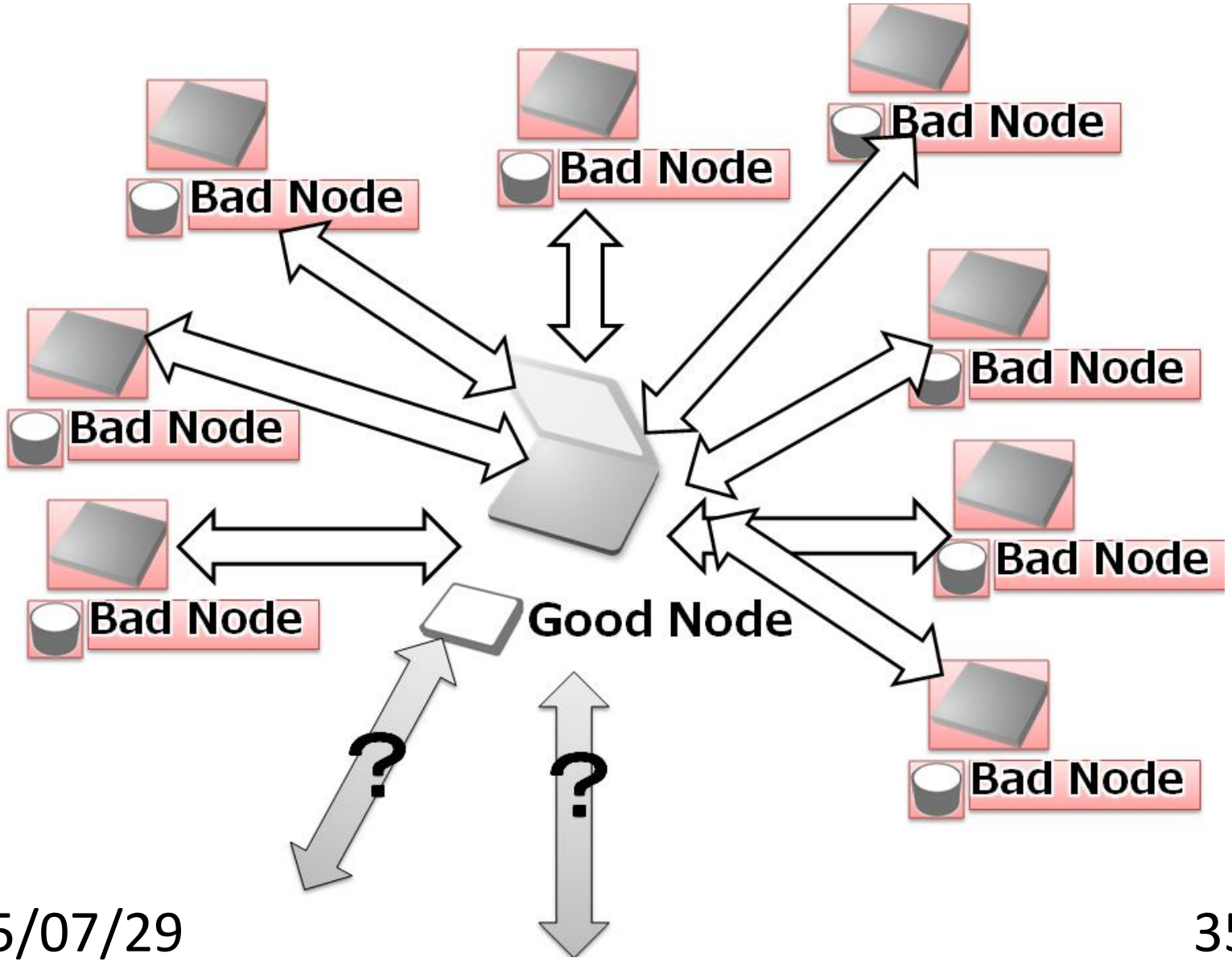
Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on bitcoin's peer-to-peer network. 3 2015.

Heilman et al.’s defence
Test before Evict



Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. Eclipse attacks on bitcoin’s peer-to-peer network. 3 2015.

Randomized Outdegree



Temptation / Starvation Detection+Mitigation

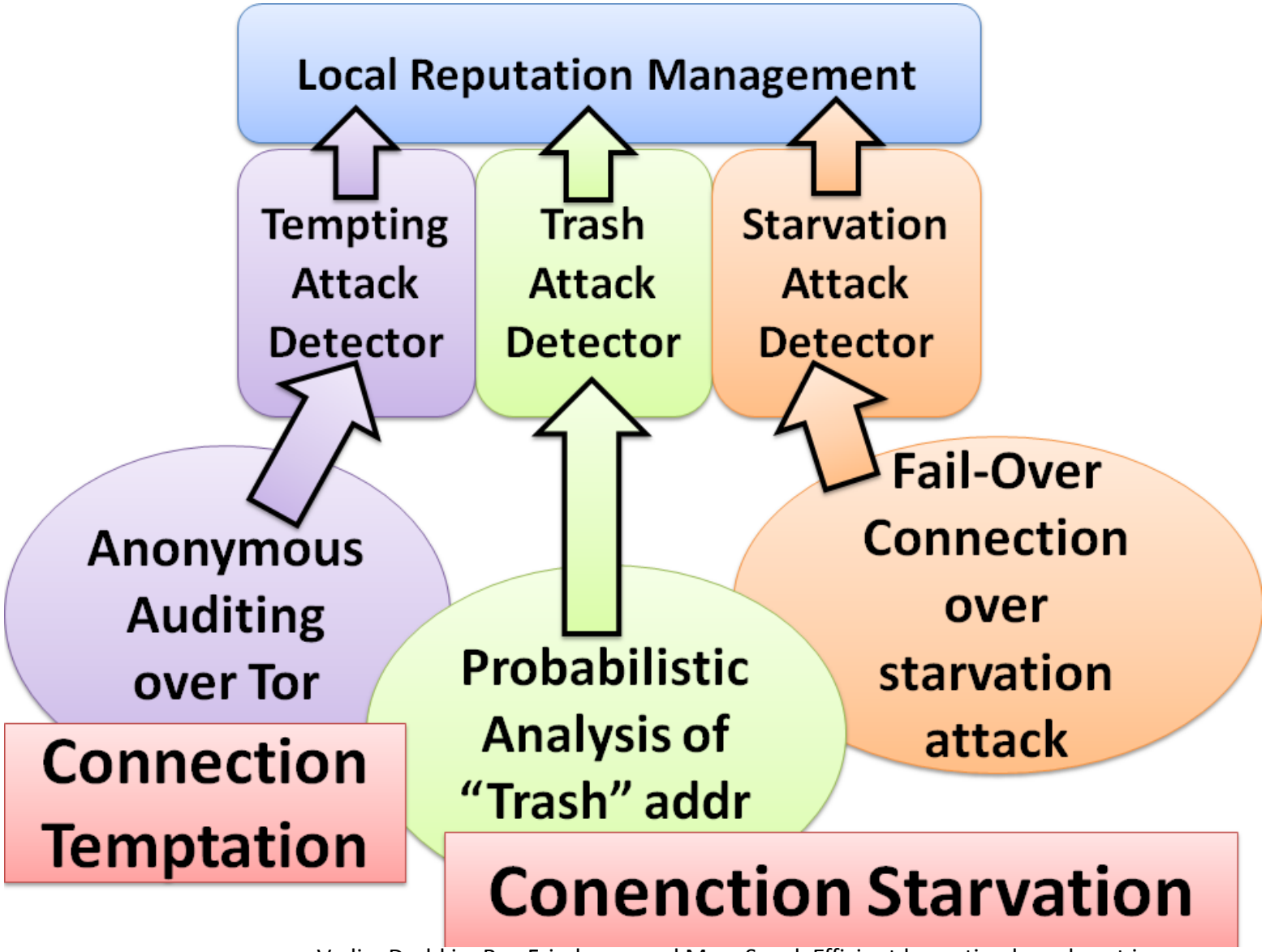
Detection / Reputation Modules

Degree Bounding

&

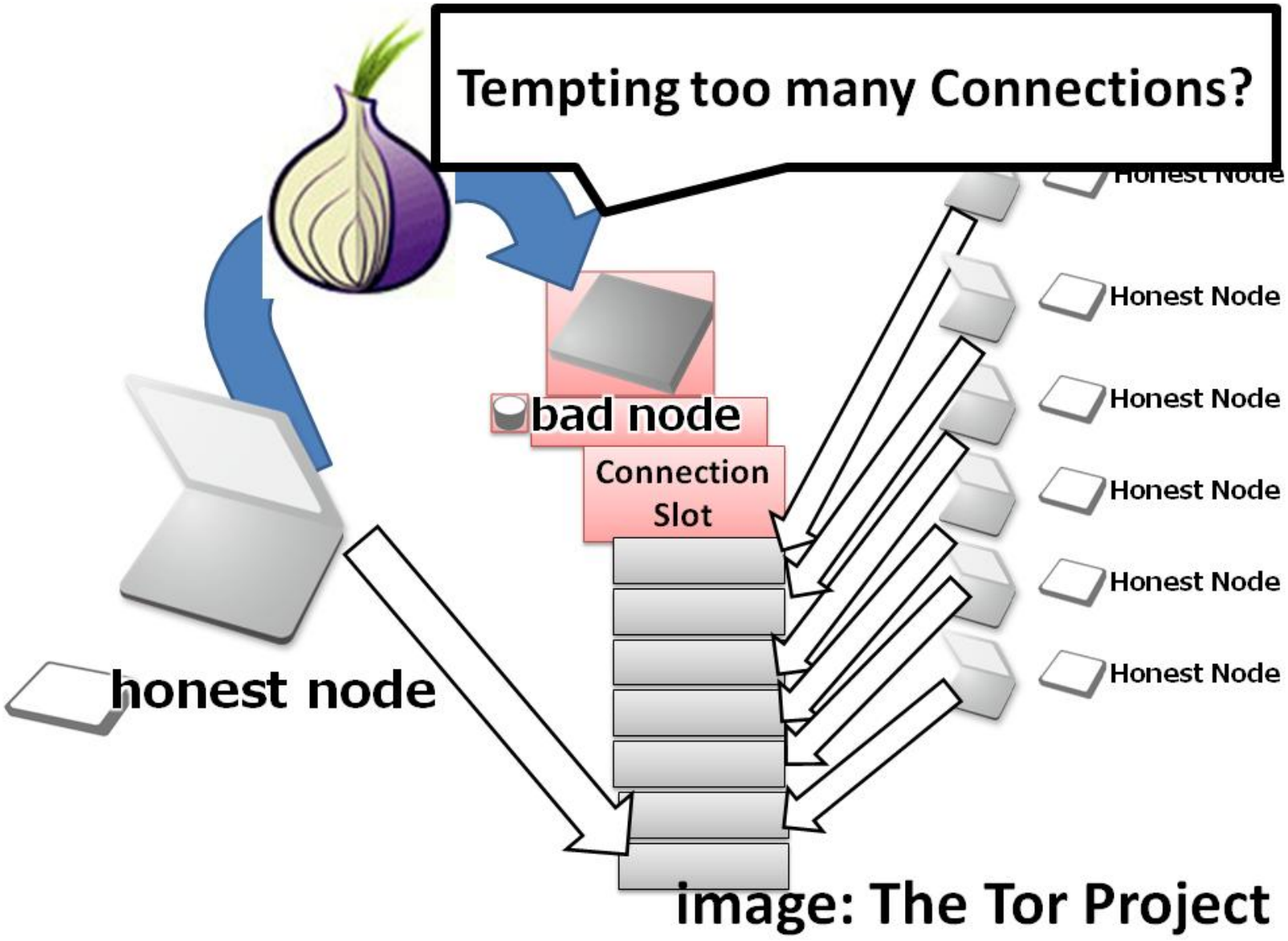
Fail-Over Connection

Modularized Attack Detector



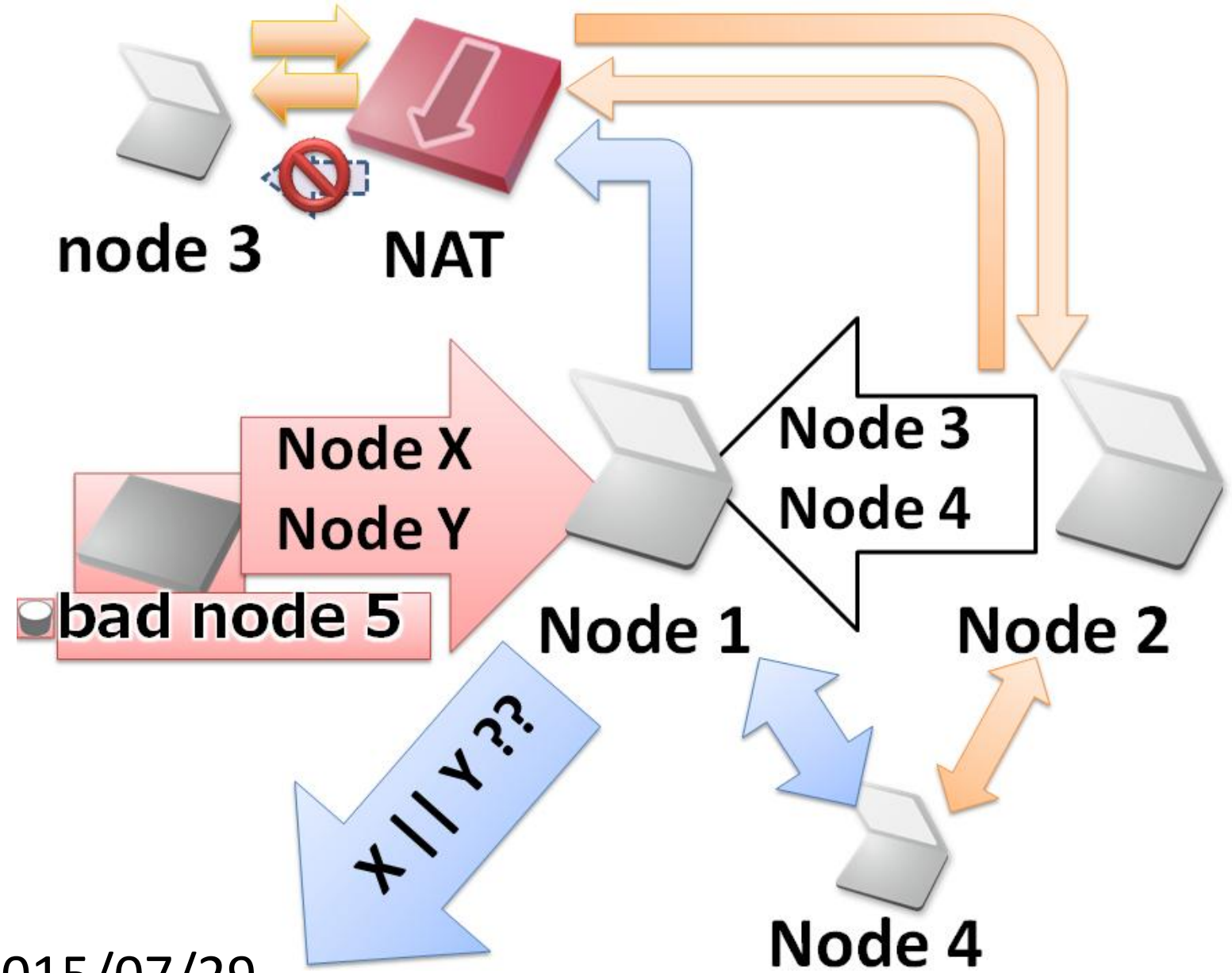
Vadim Drabkin, Roy Friedman, and Marc Segal. Efficient byzantine broadcasst in wireless ad-hoc networks. Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, pages 160–169, 2005.

Anonymous Auditing over Tor



Atul Singh, Miguel Castro, Peter Druschel, and Antony Towstron. Defending against eclipse attacks on overlay networks. *Proceedings of the 11th ACM SIGOPS European Workshop, 9 2004.*

Probabilistic Analysis of “Trash” addr



Starvation Attack Detection

Failover Connection over
Connection Starvation Attack

Botnet型攻撃者の弱点

- NATのポート開放やファイアウォールの設定を出来る善良なユーザ群でも外部からの接続を受け付けているのは
  - 1/3程
- Botnetの場合それを更に下回り、またbot化されたPCの利用者のPC利用状況に応じて
  - IPアドレスの変更
  - シャットダウン
  - NAT/Firewall (しかも設定出来ない)

等に阻まれ、その割合は低くなると思われる

2010年のWang et al. の論文時点では割合が不明

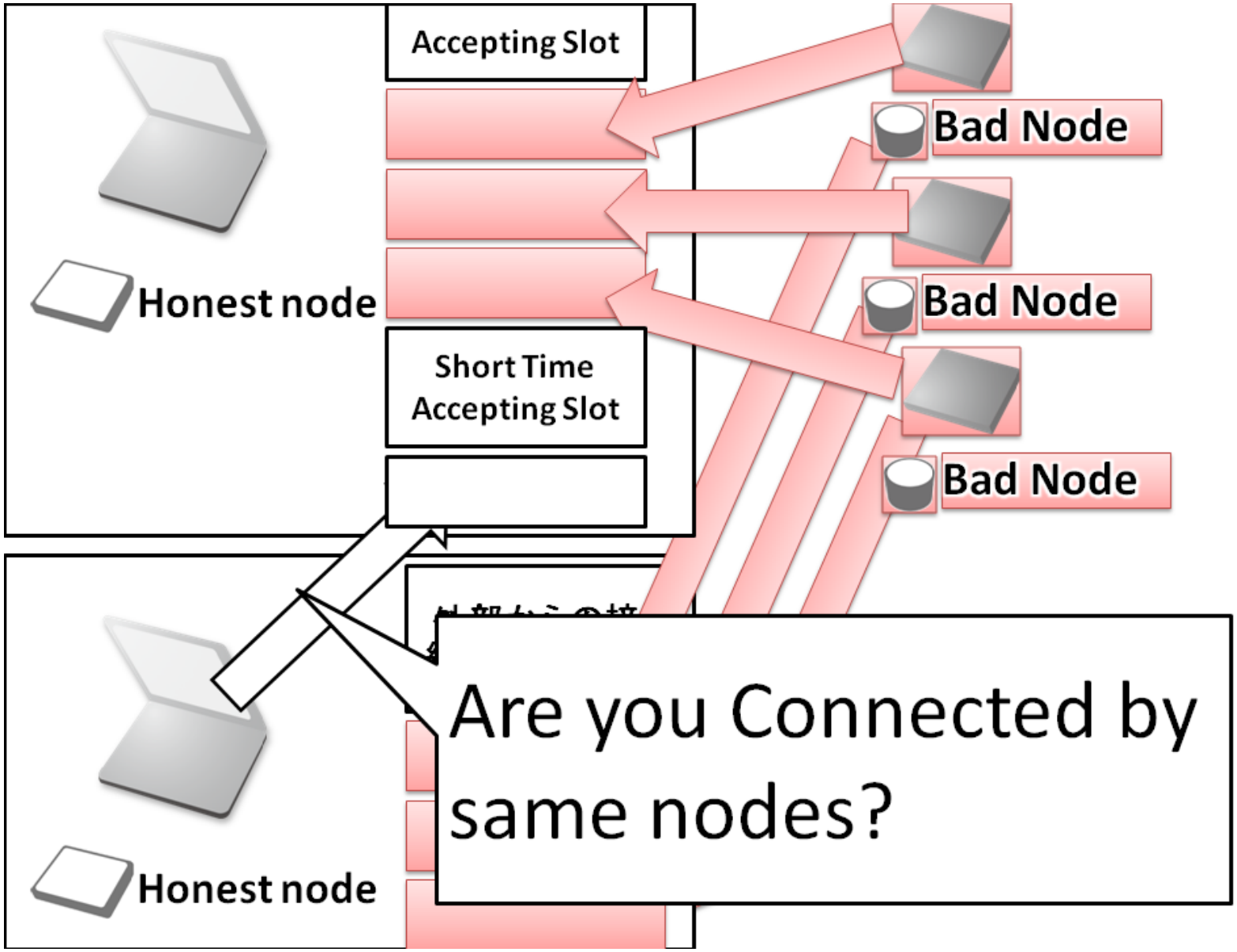
PingWang, Sherri Sparks, and Cliff C. Zou. An advanced hybrid peer-to-peer botnet. *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL 7, 2010.*

である為

外部からの接続を受け付けるノードに対して、直接接続を行いその隣接ノードを問い合わせた場合

ビザンチン、すなわちその応答内容が善良なノードを攻撃者として見なさせる物で無い確立が高い

Fail-Over Connection Over Starvation Attack



Secure Address Management

Castro氏曰く:「理想的なルーティングテーブルは、ネットワーク全体に占める攻撃者ノードの割合を f とした場合、それ以上の割合で攻撃者ノードのエントリがテーブルを占めない」

現状のBitcoin等のアドレステーブルの挙動はそのようになっていない

無批判に全ての新規に受信したアドレスを、旧弊なアドレスの削除と引き換えに登録

Miguel Castro, Peter Druschel, Ayalvadi Ganesh, Antony Rowstron, and Dan S. Wallach. Secure routing for structured peer-to-peer overlay networks. *ACM SIGOPS Operating Systems Review - OSDI '02, 36:299–314, 2002.*

バージョン0.11 でも未だに自ら接続する事による”*Tried*”バケツの汚染が可能

```
void CAddrMan::Good_(const CService& addr, int64_t nTime)
{
     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

    // move nId to the tried tables
    MakeTried(info, nId);
}
```

```
if (((CNetAddr)pfrom->addr) == (CNetAddr)addrFrom)
{
    addrman.Add(addrFrom, addrFrom);
    addrman.Good(addrFrom);
}
```

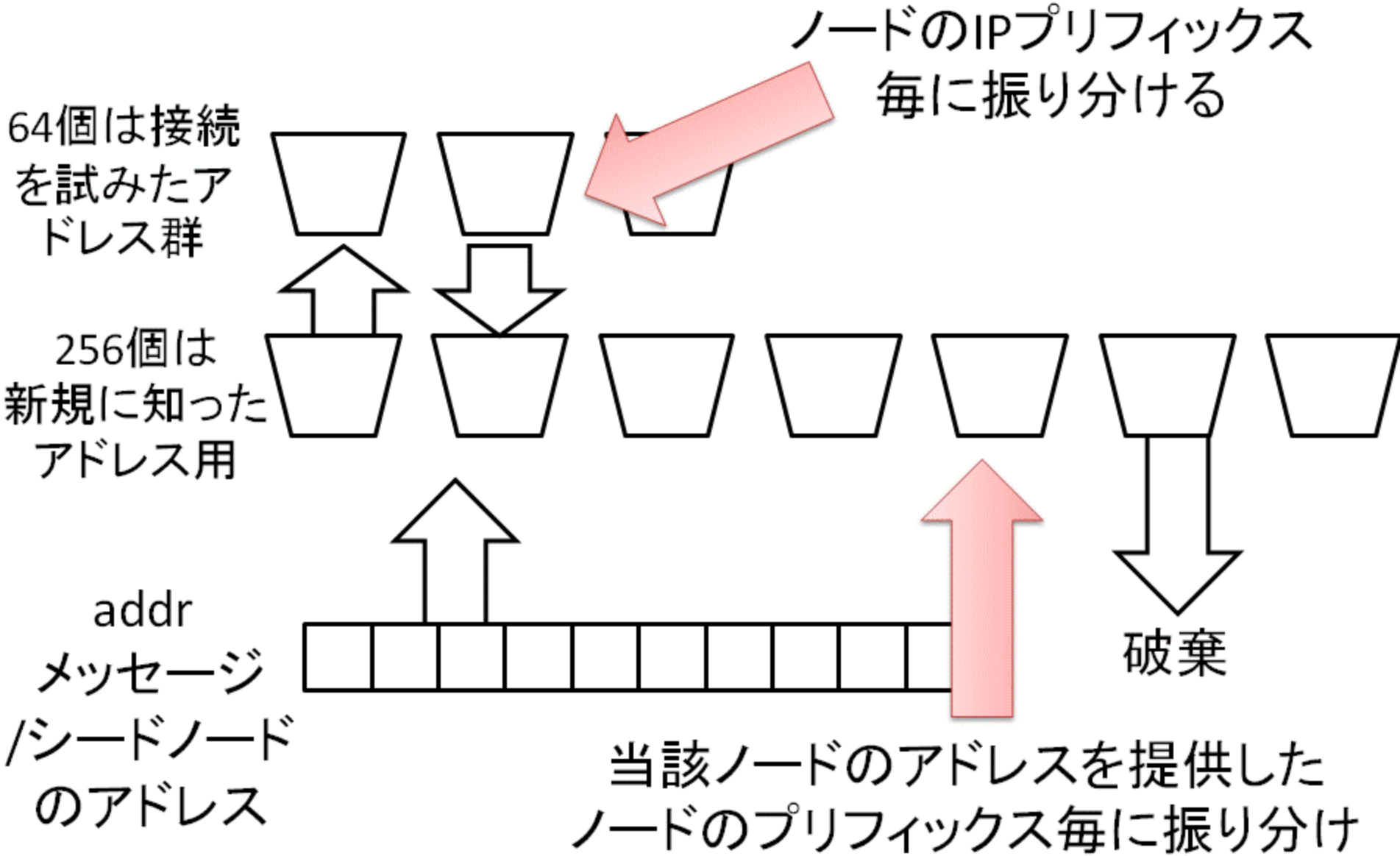
Bitcoin.org. bitcoin/src/main.cpp. https://github.com/bitcoin/bitcoin/blob/0.11/src/main.cpp#L4002 . Accessed: 2015-06-26.
https://github.com/bitcoin/bitcoin/blob/a903ad7e9cafb73f65dc78601dbef1c3c7b4fe0f/src/addrman.cpp#L196 . Accessed 2015/07/12

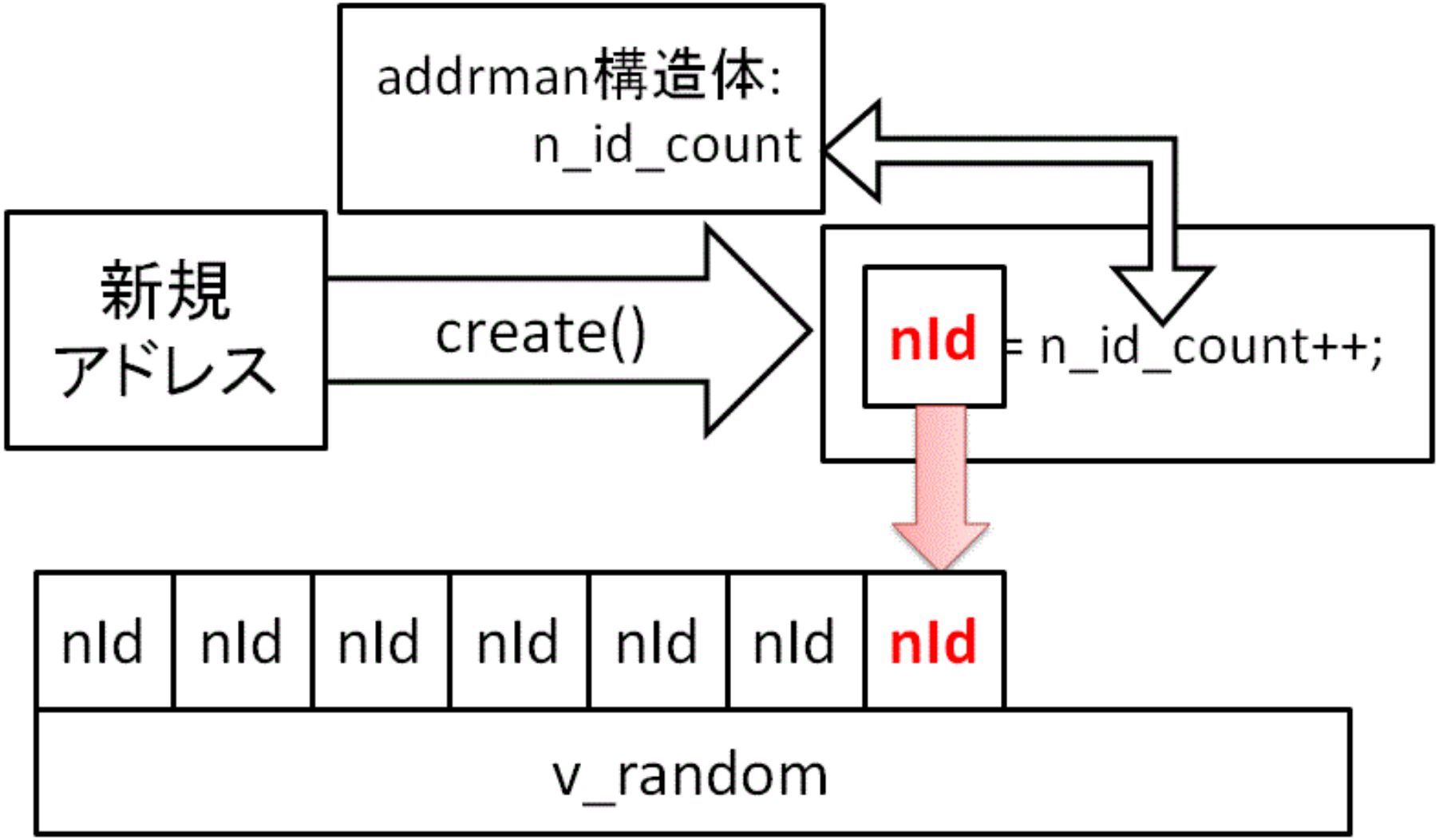
強靭なアドレステーブル機構
Addrman

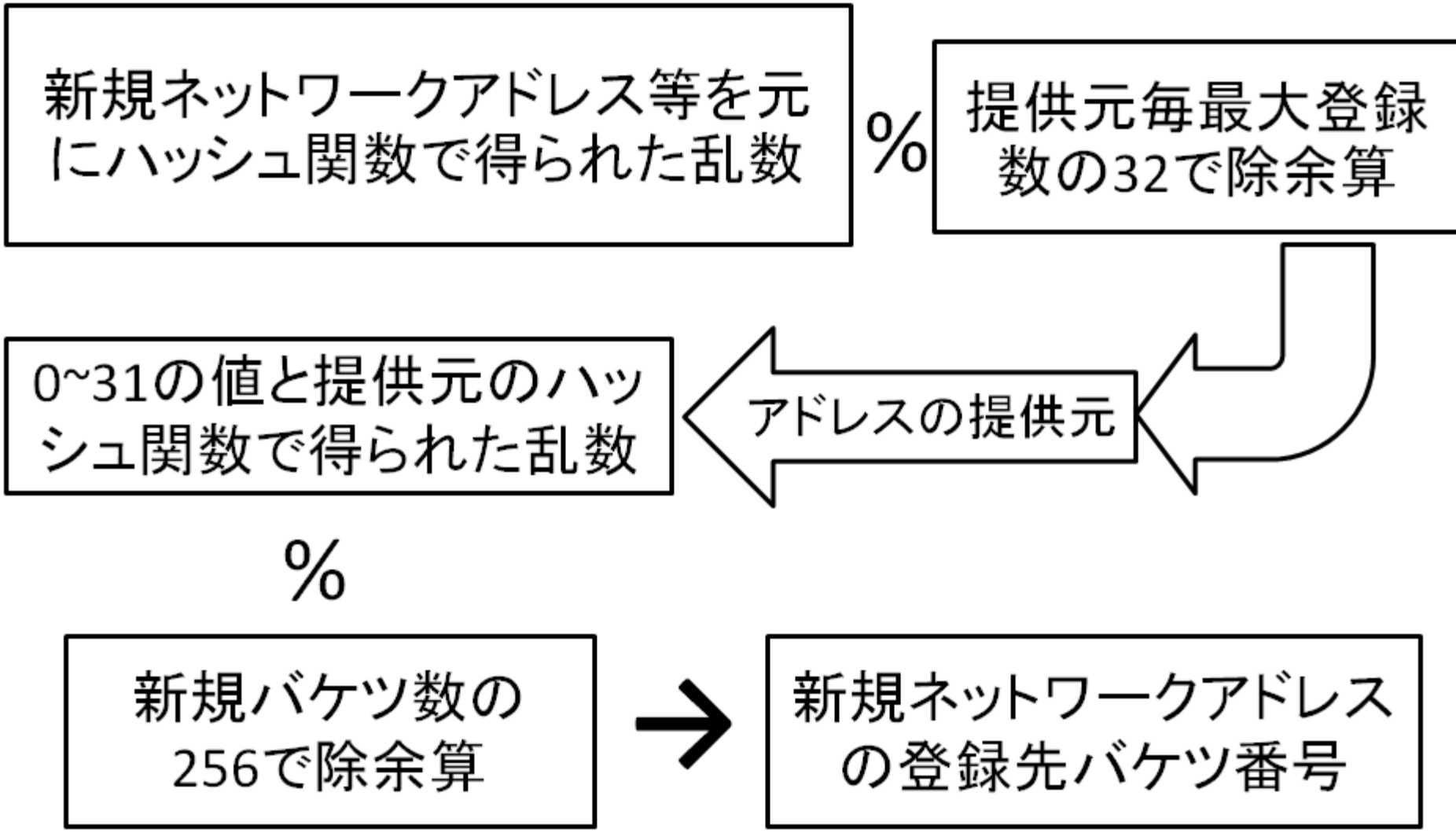
Addrmanのデザインの目的

- 限られた数のネットワークアドレスのみの保有を行う事で公式クライアント実装の起動の高速化
- 攻撃者が同一ネットワークセグメントに存在する悪しきノードのみで、ネットワークアドレステーブルを汚染しきれない事
- 攻撃者が幾重ものアドレス送付によりネットワークアドレステーブルの汚染を試みても、限られた範疇の影響しか受けない事

https://github.com/bitcoin/bitcoin/blob/master/src/addrman.h#L91
CAddrMan: Stochastic IP address manager
http://comments.gmane.org/gmane.comp.bitcoin.devel/707


ノードのIPプリフィックス
毎に振り分ける
64個は接続
を試みたア
ドレス群
256個は
新規に知った
アドレス用
addr
メッセージ
/シードノード
のアドレス
破棄
当該ノードのアドレスを提供した
ノードのプリフィックス毎に振り分け


addrman構造体:
n_id_count
新規
アドレス
create()
nId = n_id_count++;
nId
nId
nId
nId
nId
nId
nId
v_random


新規ネットワークアドレス等を元にハッシュ関数で得られた乱数
%
提供元毎最大登録数の32で除余算
0~31の値と提供元のハッシュ関数で得られた乱数
アドレスの提供元
%
新規バケツ数の256で除余算
新規ネットワークアドレスの登録先バケツ番号

117台でシステム全体のノード
をエクリプス出来るデザイン

プロトコル一覧

version	新規に他ノードと接続を求める際に使用するメッセージ、尚接続 要求相手も接続に応じる場合 verack と共に当該メッセージを送信する
verack	version メッセージを受信した旨を伝えるメッセージ
getaddr	送信相手に対して既知の活動中のノードに関する情報を要求
addr	getaddr に対する応答。活動中のノードのタイムスタンプ、提供する サービス、IP アドレス、及びポート番号が組み込まれている
inv	送信相手に新規のオブジェクトを保有してる旨を伝えるメッセージ、 オブジェクトは決済、block、block のヘッダで、そのハッシュを内包する
getdata	inv メッセージに内包されているハッシュを元に当該オブジェクトを 保有してないか判断し、保有してない場合要求として送信する
getblocks	特定の高さまでの block 全てを得る為 inv メッセージを要求
getheaders	特定の高さまでの block ヘッダを要求。主に軽量な実装において 短時間に最新の blockchain を取得するのに使われる
notfound	getdata を受領し、リクエストされたデータを自ノードが保有して いない場合の返答に用いられる
tx	getdata に対する応答。決済の情報を内包する
block	getdata に対する応答。決済等の情報を含む block を送信する

Bitcoin.org. https://en.bitcoin.it/wiki/Protocol_specification

プロトコル一覧2

headers	getheaders に対する応答。block のヘッダを内包する
ping	当該メッセージ送信対象との TCP/IP リンクが健在であることの確認。他のメッセージ等の送信中のエラー等が接続の遮断と推察される為送信
pong	ping メッセージへの応答。ping メッセージ内の noce 値を内包
mempool	送信対象に正当性が確認されたが、未承認の決済に関する情報を要求。応答として送信対象の mempool に存在するそれらの決済データのハッシュ値を含んだ inv メッセージが送信される
submitorder	IP 決済に用いられていたが非推奨となっており使われていない
reply	IP 決済に用いられていたが非推奨となっており使われていない
reject	メッセージを拒絶した際に送信する。
filterload	*Bloom filtering* 機能に用いられる [9]。
filteradd	*Bloom filtering* 機能に用いられる [9]。
filterclear	*Bloom filtering* 機能に用いられる [9]。
merkleblock	*Bloom filtering* 機能に用いられる [9]。
reject	ノード間通信を通じてネットワーク中に伝搬拡散し、Bitcoin 開発グループによるシグネチャが確認されたらエンドユーザに内容が表示される

Bitcoin.org. https://en.bitcoin.it/wiki/Protocol_specification

バージョン0.11 でも未だに自ら接続する事による”*Tried*” バケツの汚染が可能

```
void CAddrMan::Good_(const CService& addr, int64_t nTime)
{
     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

    // move nId to the tried tables
    MakeTried(info, nId);
}


if (((CNetAddr)pfrom->addr) == (CNetAddr)addrFrom)
{
    addrman.Add(addrFrom, addrFrom);
    addrman.Good(addrFrom);
}
```

Bitcoin.org. bitcoin/src/main.cpp. https://github.com/bitcoin/bitcoin/blob/0.11/src/main.cpp#L4002 . Accessed: 2015-06-26.

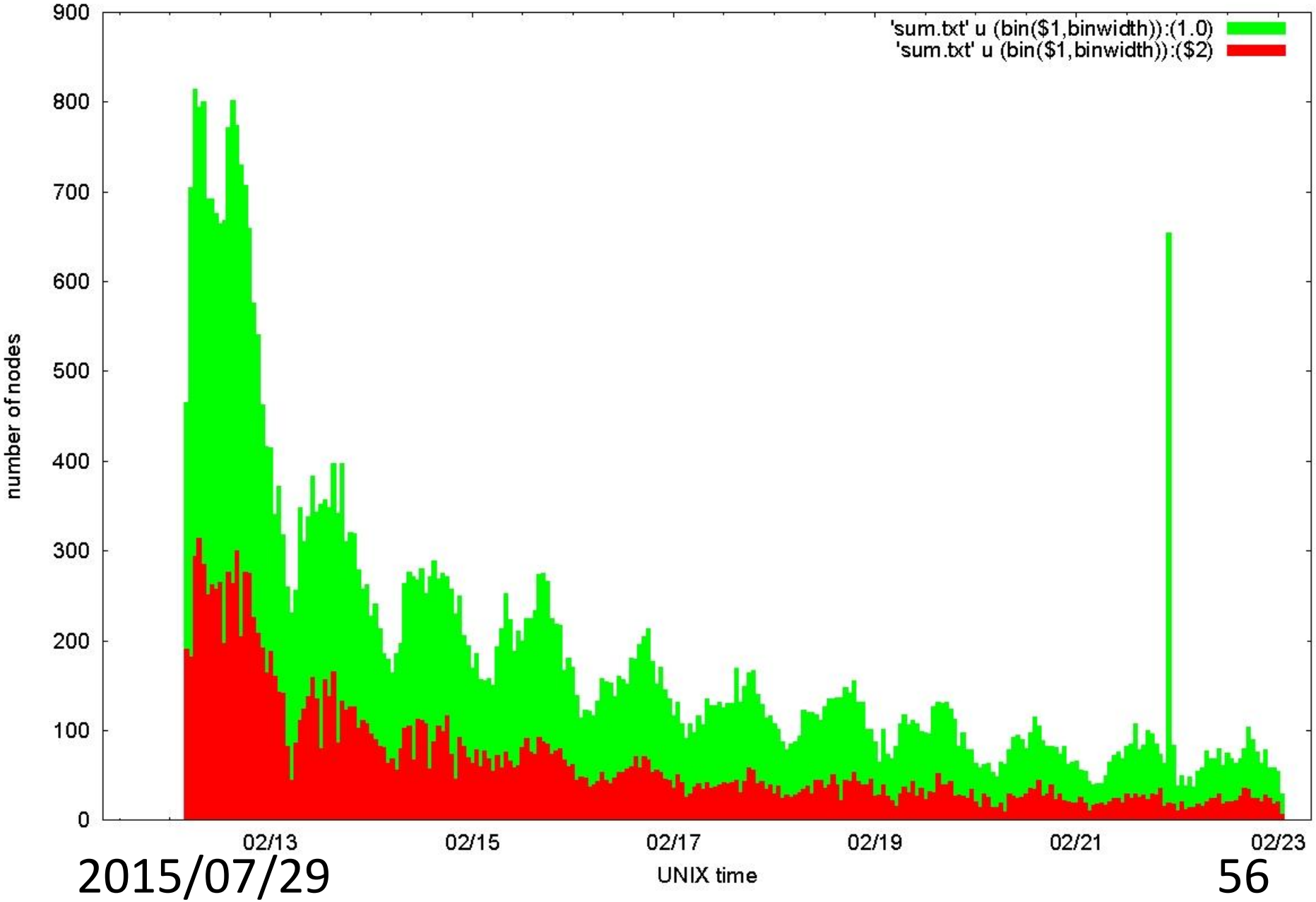
https://github.com/bitcoin/bitcoin/blob/a903ad7e9cafb73f65dc78601dbef1c3c7b4fe0f/src/addrman.cpp#L196 . Accessed 2015/07/12

広告機能を用いた"trash"による他のネットワークアドレスの駆逐

- ネットワークアドレスのタイムスタンプが現時刻から60 分以内である事
- 当該*addr* メッセージが10 以下のネットワークアドレスしか内包していない事
- *fGetAddr* フラグが当該ノードに対して立っていない事
- 当該アドレスがルーティング可能である事

Satoshi client node discovery 3.6.1 address relay. https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery 2014.

ネットワーク中のBitcoinノード



目標 GOAL (Problem Statement)

N: 全 Bitcoin ネットワークに 中のノード

f: 个の内攻撃者の管理運用している物

nat: 外部からの接続を受け付けないノードの割合

攻撃者がエクリプス攻撃敢行時に、

Connection枯渇攻撃を成功させるのに攻撃に要するノード数 ***F*** を:

F = N(1 - f)(1 - nat)117 *(1/8) 大体10万超え

保留

エクリプス攻撃

エクリプス攻撃に関する既存研究

そこで本研究の貢献

このモデルに基づいた

エクリプス攻撃に対する防衛機構

いらん子中隊

Bitcoin

- 2009年のオープンソースソフトウェアとしての公開以降商取引などが活発化
- Litecoin等の派生通貨を導出
- Blockchain {システム全体の台帳}に取引の記録
- 情報の同期は　Flooding　(隣接ノードへ拡散)

概要

- Bitcoin等は、既存の防衛機構やネットワーキングの仕組みを引き継げていない為、エクリプス攻撃に脆弱
- エクリプス攻撃を段階分けし、それをベースに構造化され、体系だったフレームワーク及び防衛戦略を作成
- 防衛戦略に則った防衛機構のサーベイ、検討
- 後のエクリプス攻撃の研究に貢献しうるフレームワークと防衛戦略

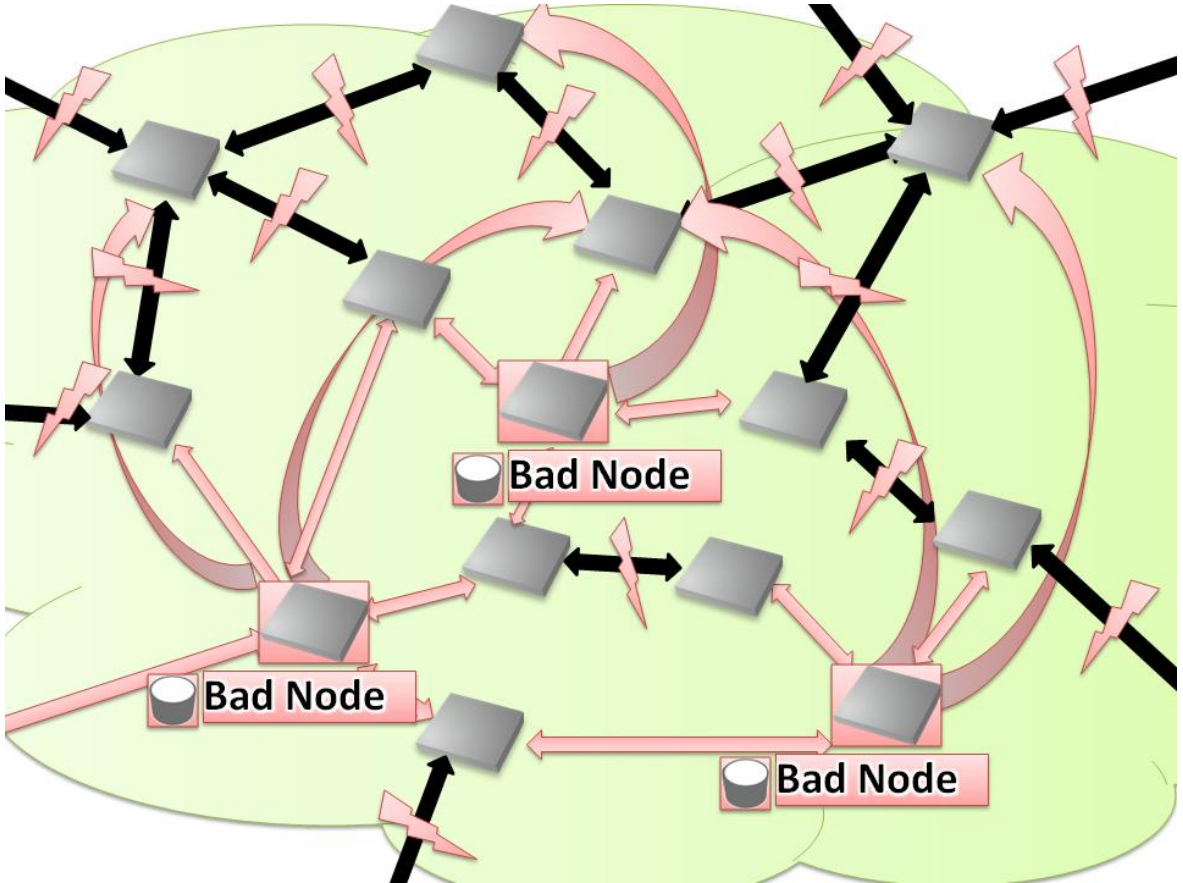
本研究で想定するエクリプス攻撃

- 接続実績のあるIPアドレステーブルの汚染
  - 善良なノードへの多数のノードを用いた短期接続
- 接続実績の無いIPアドレステーブルの汚染
  - IPアドレス広告伝搬機能を悪用した”Trash”拡散
  - ハンドシェイク時の”Trash”及び攻撃者ノードのIPアドレスの多量送付
- Connection枯渇攻撃
  - ネットワーク中の個々のノードが保有する117のConnection受付スロットを攻撃者ノードで接続し、枯渇

Bitcoin は優れた機構を持ちながら、

既存のP2Pの研究によるネットワーキング
と防衛機構の資産を引き継いでおらず

攻撃者ノード数 **F≧117** でシステム破綻



貢献

- エクリプス攻撃の段階分けしたモデル化によるフレームワーク
- それにより構造化され、体系だった単一グローバル台帳暗号通貨への包括的な防衛戦略及び防衛機構群
- 他の研究者がエクリプス攻撃に対する防衛でベースに出来るフレームワーク