Computer Security Symposium 2017
23 - 25 October 2017

集中/分散切り替え型 Attestation のための爆発的相転移を用いたネットワーク構成方法

三好 一徳[†1]，小林 俊輝[†1]，濱本 亮[†1]，森田 佑亮[†1]，佐々木 貴之[†1]

概要：膨大な数の多様なデバイスが接続される IoT システムでは，従来の集中制御による Attestation は Scalability に課題がある．そのため，分散制御による Attestation が数多く提案されているが，それらはいずれかの段階でシステム全体での情報共有を必要とする．すなわちネットワークが複数のクラスタに分割された状態と，ネットワーク全体が 1 つのクラスタとなる状態の両方が必要となる．そこで本稿では，両者の切り替えを実現するために，爆発的パーコレーションを用いた方法を提案する．提案手法により，従来のメッシュ接続を行う場合に比べて 1/5 以下のコストで切り替え可能であることを示す．

キーワード：Attestation，爆発的パーコレーション，IoT

Network Configuration Method for Centralized/Distributed Attestation Using Explosive Percolation

Kazunori Miyoshi[†1] Toshiki Kobayashi[†1] Ryo Hamamoto[†1] Yusuke Morita[†1]
Takayuki Sasaki[†1]

Abstract: Attestation on IoT system, where many divergent devices are connected, has problems on scalability. Although enormous attestation methods have been proposed, they require some shared information at any point in time. That is, any attestation methods require both state between clustered network and non-clustered network. In this paper, a network configuration method for centralized/distributed attestation using the explosive percolation is proposed to suppress the switching cost between clustered network and non-clustered network less than 1/5 of the existing Achlioptas network.

Keywords: Attestation, Explosive percolation, IoT

1. はじめに

スマートシティをはじめとする IoT システムでは，多種多様，かつ多数のデバイスがネットワークに接続され，それらがデータを生成し，生成されたデータは様々な経路を用いて送受信される．このようなシステムでは，不正なデバイスが容易にシステムへ侵入する可能性があり，実際にシステム内を流通するデータが盗聴・改ざんされる，システムの正規コンポーネントの資源を使い果たしてシステムが停止させられる，といった被害が出ている[1-4]．このような脅威を防ぐためには，システムに接続されているデバイスの真正性を検証すること(Attestation)が必要条件となる．

一般に Attestation は，チャレンジ&レスポンス方式を用いて行われる[5]．Attestation では，1 台の信頼されたデバイス(Verifier)が，信頼されていないデバイス(Prover)を 1 対 1 で検証する．したがって，スマートシティのように接続されるデバイス数が膨大になると，集中制御型 Attestation 方式ではスケールしない．そのため，Attestation をネットワーク内で並列処理可能な分散型 Attestation 方式が必要である．近年，いくつかの分散型 Attestation 方式が提案されてはいるものの，例えば全域木を作るための情報をネットワーク内のノード全てで共有しなければならない，など結局は大域的な情報共有が必要となる．しかし一方で，大域的な情報共有のために常にネットワーク内の全てのリンクを通信可能な状態に維持しておくためにはコストがかかる．そこで，通常の運用時にはネットワークを部分的なネットワーク(以下, クラスタ)に分割して分散制御による Attestation を行い，必要なときにはネットワーク全体を接続させて集中制御による大域的な情報共有を行うための仕組みが必要である．

そのような仕組みを実現する手段の 1 つとして，パーコレーション転移[6]と呼ばれる相転移現象がある．ネットワークにおけるパーコレーション転移とは，クラスタに分断されていたネットワーク内の全てのノードが，接続されたリンクを介して互いに到達可能になる状態を言う．パーコレーション転移自体は古くから知られているが，最近になって，クラスタ間をある種の規則に従ってリンク接続すると，爆発的パーコレーション(Explosive percolation)という 2

†1 NEC セキュリティ研究所
Security Research Laboratories, NEC.

次の相転移が起こることが明らかにされ，注目を浴びている[7-10]. 爆発的パーコレーションでは，クラスタ間の少数のリンクを接続/削除するだけで，相転移が起こることが知られている．

そこで本稿では，爆発的パーコレーションを用いた集中/分散切り替え可能な Attestation 方式を提案する．また，通信ネットワークに適したリンク接続規則を用いることで，メッシュ接続を行った場合に比べて，切り替え時に必要なリンク数を 1/5 以下に削減できることを示す．

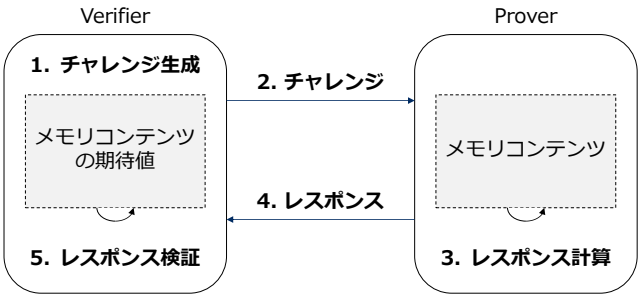

図 1　Attestation の仕組み

2. 関連文献

2.1 Attestation

典型的な Attestation は図 1 に示すようにチャレンジ&レスポンスプロトコルに従う．Attestation では，1 台の信頼されたデバイス(Verifier)が，信頼されていないデバイス(Prover)を 1 対 1 で検証する．Verifier は，事前に Prover の正しい内部状態(メモリコンテンツ)を知っているという仮定の下で，Prover に対してチャレンジを行う．Prover は，Verifier から受け取ったチャレンジと自身の内部状態に基づいてレスポンスを生成し，Verifier に返す．Verifier は Prover から受け取ったレスポンスと，自身が生成したレスポンスの期待値とを比較し，それらが合致すれば Prover は正規なデバイスであると判断する．

Attestation は従来，隣接するデバイス同士でなければ実現できなかった[11-13]が，最近ではネットワーク内の隣接しないデバイス間でも Attestation 可能な方式(Remote Attestation)が多数提案されている[14-16].

SEDA[14]は，センサネットワークのような多数の非力なデバイスで構成されたネットワーク向けに提案された方式である．SEDA は 1 台の Verifier，1 台の Swarm operator，そして多数の Prover で構成される．Swarm operator はネットワークに参加/離脱するデバイスの管理を行う．Attestation を行う場合，Verifier はネットワーク内からランダムに選んだデバイス(Prover)に対してチャレンジを行い，そのデバイスは Verifier にレスポンスを返す．次にそのデバイスは，事前に作成された全域木にしたがって，自身に接続されている子デバイスとの間で Attestation を行う．子デバイスは，孫デバイスとの間で Attestation を行う．以下，同様にして，全域木の葉ノードまで Attestation されると，葉ノードから全域木を逆順に辿って，各 Attestation の結果が Verifier に返送される．

以上のように，SEDA[14]ではネットワークに関する大域的な情報を必要とせず分散的に Attestation を行うが，全域木を作るために，事前にネットワーク全体に大域的なセッション ID を配信しておく必要がある．大域的な情報共有は，その後に提案された DARPA[15]では公開鍵の共有，SENA[16]では Aggregator 間のトークン共有という形で必須要素となっている．

2.2 パーコレーション転移

2.1 で述べた大域的な情報共有をグラフ理論の文脈で考えると，パーコレーション転移という現象で表すことが出来る．ここでは，まず従来知られている Erdös-Rényi モデル[17]に基づくパーコレーション転移について説明した後，2009 年に Achlioptas らが示した爆発的パーコレーションについて述べる．

(1) Erdős-Rényi(ER)モデルに基づくパーコレーション転移

まず，N 個の孤立したノードで構成されるグラフから始めて，1 ステップ毎に一様かつランダムに異なる 2 個のノードを選び，リンクを接続していく．ここで，ステップ数を T とし，$t = T/N$とすると，ある臨界ステップ値t_cに対して，$t < t_c$では，グラフは小規模なクラスタ(接続されたノードの集合)で構成されている．ここで，C をグラフ内の最大クラスタとし，$|C|$をそのサイズとすると，$N \to \infty$の熱力学的極限では，$t_c = 0.5$で 2 次の相転移を起こし，$t < t_c$では N に対して対数的に増加していた$|C|$が，$t > t_c$では N に対して線形に増加する[8].

(2) 爆発的パーコレーション

Achlioptas らはノード間の接続規則を下記の Achlioptas 過程(図 2)のように修正することで，臨界ステップ値t_cの値を大きく出来ること，また，t_cにおいて最大クラスタサイズ$|C|$が爆発的に(当初は 1 次の相転移だと考えられたが，現在は 2 次の相転移であることが示されている[8])増大することを示し，爆発的パーコレーション(Explosive percolation)と名付けた[7].

爆発的パーコレーションが発生するための接続規則や臨界ステップ値については，その後様々な研究が成されている．リンク候補の両端のノードに接続されるクラスタのサイズの和が最小となるリンクを追加する方法や，リンク重みを最小にするリンクを追加する方法などいくつかのリンク接続規則において，爆発的パーコレーションが起こることが報告されている[7-10].

Achlioptas 過程(以下，AP 過程)：図 2

(手順 1)　グラフ内から 1 ステップ毎に一様かつランダムに m 本のリンク候補$\{e_1, e_2, \cdots, e_m\}$を選択する．

(手順 2)　各リンク候補の両端のノードに接続されるクラスタのサイズの積を比較し，その積が最も小さくなるリンクをグラフに追加する．

(手順 3)　手順 1 に戻る．

図 3 の実線で示すように，爆発的パーコレーションが起こるようなリンク接続を行ったグラフでは，相転移が起こるために必要なステップ数が小さく，クラスタ間の少数のリンクを切断するだけでグラフをクラスタに分割できる．一方，図 3 の点線で示すように，ランダムにリンク接続を行ったグラフでは，クラスタ間およびクラスタ内がメッシュ接続となっているため，グラフをクラスタに分割するためには，爆発的パーコレーションを起こすために必要な数の 10 倍以上のリンクを切断しなければならない．

3.　集中/分散切り替え型 Attestation 方式

ここでは，本稿で提案する集中/分散切り替え型 Attestation 方式について説明する．

3.1　解くべき課題と提案手法のコンセプト

解くべき課題は，IoT システムにおける Attestation の集中制御と分散制御の切り替え時に要するリンク張替えコストをいかに小さく抑えるか，である．そこで，爆発的パーコレーションと，Attestation の集中制御と分散制御の切り替えとの間のアナロジについて説明する．

グラフにおけるノードは IoT システム内のコンポーネント(IoT デバイス，ゲートウェイ，Attestation サーバ，など)に相当し，リンクは Attestation 関係に相当する．

2.2 で述べたように，パーコレーション転移とはクラスタに分断されたグラフにリンクを追加していくことで，グラフ全体が 1 つのクラスタになる，という現象である．また爆発的パーコレーションは，図 3 から明らかなように，分断されたグラフを 1 つのクラスタにするための追加リンク数が極めて少数である，という特徴を有している．

つまり，爆発的パーコレーションを用いれば，IoT システムにおける Attestation の集中制御と分散制御の切り替え時に要するリンク張替えコストが非常に小さく抑えられることを意味している．

3.2　前提条件

ネットワークは 1 台のサーバ，複数のゲートウェイ(以下，GW)，および GW に接続される複数の IoT デバイスで構成されるものとする(図 4)．GW 間および GW-IoT デバイス間は有線接続または無線接続可能とする．サーバは，集中的な Attestation を行う場合の検証サーバとしての機能の他に，全ての GW および IoT デバイスの接続情報を管理・制御する機能を有する．

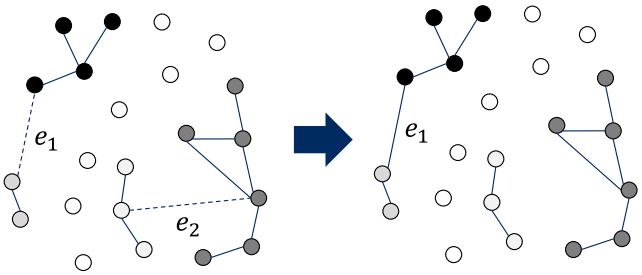

図 2　AP 過程に基づくリンク接続の様子(m=2 の場合)

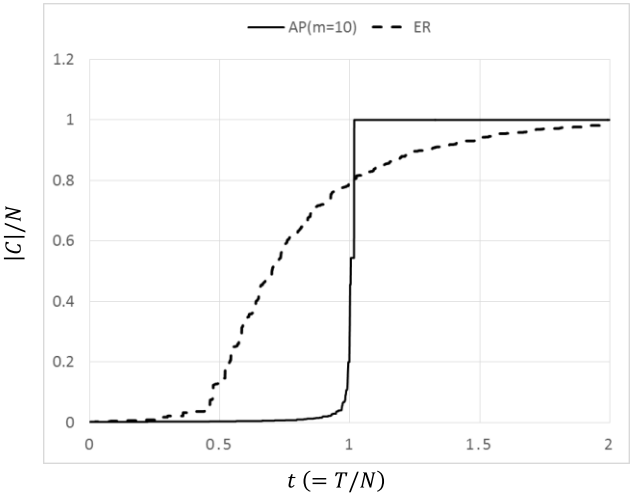

図 3　相転移の様子(N=1000)
(実線＝AP 過程(m=10)の場合，点線＝ER モデルの場合)

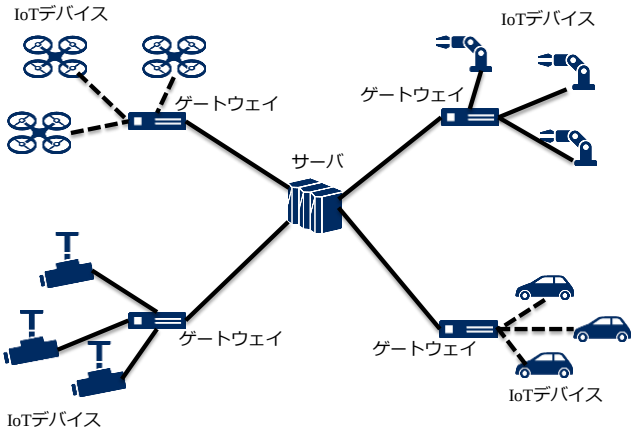

図 4　想定するネットワーク構成イメージ

3.3　手順

本方式は，下記 3 つの手順で構成される．まず，爆発的パーコレーションを起こすように，Achlioptas 過程に従ってネットワークを生成する(手順 1)．次に爆発的パーコレーションを起こすために必要なリンクを選択する(手順 2)．最後に，集中的または分散的に Attestation を行う(手順 3)．ここで，(手順 2)が必要な理由は，以下の 2 つである．

・(手順 1)では，追加するリンクの順序が必ずしもクラス

タ間を接続するものほど後にならないため.

・Achlioptas 過程では, クラスタ内でループとなる接続が発生するため.

(手順 1)　ネットワークの生成(AP 過程)

(手順 1-1) サーバは，ネットワーク内から 1 ステップ毎に一様かつランダムに，異なる m 本のリンク候補 $\{e_1, e_2, \cdots, e_m\}$を選択する.

(手順 1-2) 既に存在するリンクの重複リンクを選択した場合は(手順 1-1)に戻る.

(手順 1-3) サーバは，各リンク候補の両端のノードに接続されるクラスタのサイズの積を比較し，その積が最も小さくなるリンクをグラフに追加する.

(手順 1-4) (手順 1-1)に戻る.

(手順 1-5) ネットワーク内の全てのノードが 1 つのクラスタとして連結されると(手順 1)を終了する.

(手順 2) リンク選択

(手順 2-1) サーバは，ネットワークをクラスタに分割する際の最大クラスタサイズの閾値を決める.

(手順 2-2) サーバは，(手順 1)で生成されたリンクを逆順に，GW-IoT デバイス間リンクを除いてマークしていき，そのマークしたリンクを削除した場合のネットワーク内の最大クラスタサイズを計算する.

(手順 2-3) サーバは，(手順 2-2)で計算した最大クラスタサイズが，(手順 2-1)で決定した閾値に達した時点でマークを止める.

上記(手順 2-3)でマークされたリンクを論理的に切断/接続することで，ネットワークを所望のクラスタサイズに分割すること/ネットワークを 1 つのクラスタで構成することができる.

(手順 3) 集中/分散 Attestation の実行

(手順 3-1) 通常時，サーバは(手順 2-3)でマークされたリンクを論理的に切断し，各クラスタ内の GW および IoT デバイスは分散的に Attestation を行う.

(手順 3-2) ネットワーク全体での情報共有や集中的な Attestation が必要になった時点で，サーバは(手順 3-1)で切断していた論理リンクを接続し，ネットワーク全体を 1 つのクラスタとして構成する.

ここで，(手順 1)のネットワーク生成手順として，下記の改良 AP 過程を併せて提案する．Attestation を行う上では，クラスタの論理トポロジは tree であれば良く，ループを必要としない．そこで改良 AP 過程では，3.3 で記した(手順 1-2)にネットワークを生成する際にループを発生させないための機能を追加し，さらにリンク候補数が指定の値に満

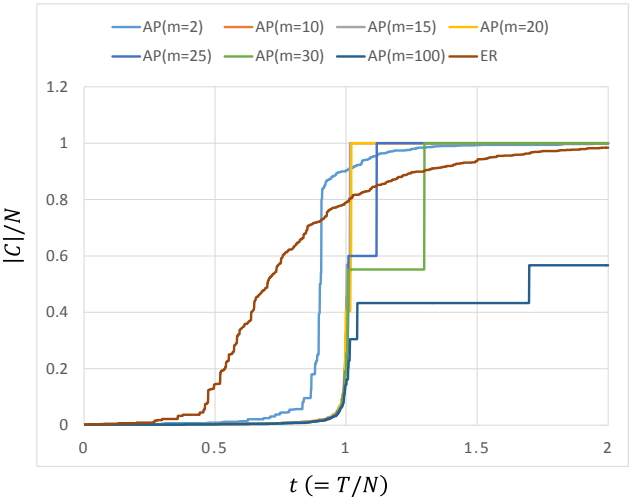

図 5　相転移の様子

(AP 過程および ER モデルに基づくリンク接続の場合)

たない場合にはリンク候補数を徐々に減少させる(手順 1-2")を追加した. (手順 1-2")は便宜的なものであるが, (手順 1-2')の追加によって，ネットワークをクラスタに分割するために必要なリンク数は大幅に削減可能と考えられる.

(手順 1')　改良 AP 過程：

(手順 1-1) サーバは，ネットワーク内から 1 ステップ毎に一様かつランダムに，異なる m 本のリンク候補 $\{e_1, e_2, \cdots, e_m\}$を選択する.

(手順 1-2')既に存在するリンクの重複リンクを選択した場合，およびループを構成するリンクを選択した場合は再選択する.

(手順 1-2") リンク候補が m 本に満たない場合は，リンク候補を－1 して(手順 1-1)を再実行する.

(手順 1-3) サーバは，各リンク候補の両端のノードに接続されるクラスタのサイズの積を比較し，その積が最も小さくなるリンクをグラフに追加する.

(手順 1-4) (手順 1-1)に戻る.

(手順 1-5) ネットワーク内の全てのノードが 1 つのクラスタとして連結されると(手順 1')を終了する.

4. 評価

4.1 評価条件

1 台の GW に 9 個の IoT デバイスが接続されるような現実的な IoT ネットワークを想定し，特に断らない限り，全ノード数 N を 1000，最大クラスタサイズの閾値を 10 とする.

4.2 評価結果

(1) リンク候補数依存性

図 5 および図 6 に，AP 過程，ER モデル，改良 AP 過程

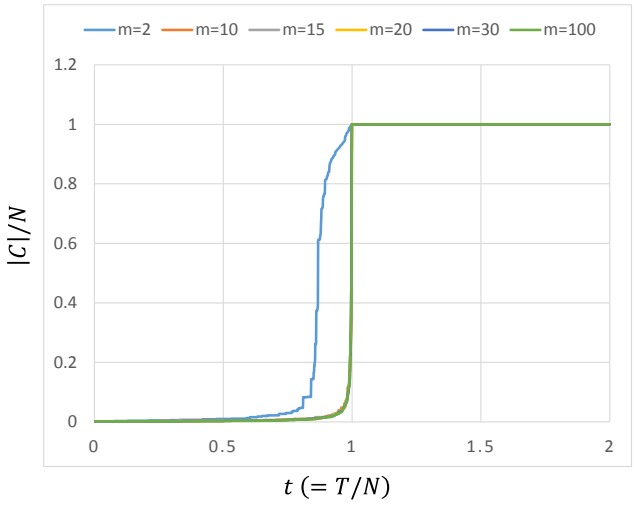

図 6　相転移の様子
(改良 AP 過程に基づくリンク接続の場合)

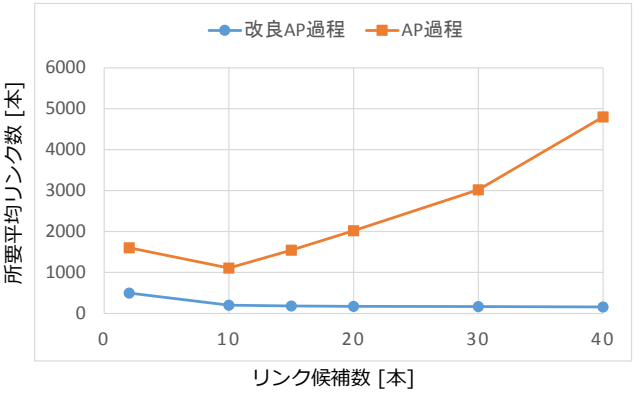

図 7　相転移に必要なリンク数の平均値

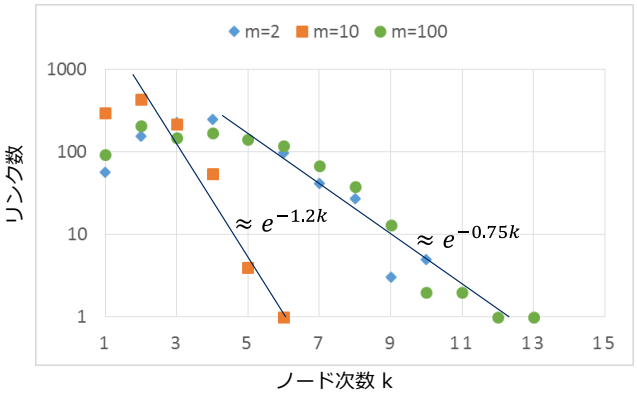

図 8　(手順 1)で生成されたネットワークの
ノード次数分布(AP 過程に基づくリンク接続の場合)

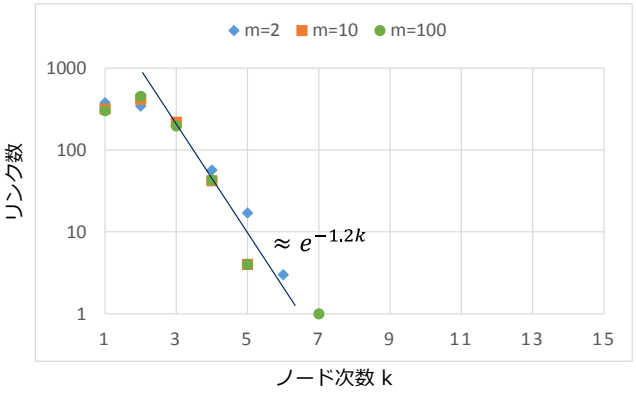

図 9　(手順 1)で生成されたネットワークの
ノード次数分布(改良 AP 過程に基づくリンク接続の場合)

に従ってネットワーク生成を行った場合のパーコレーション転移の様子のリンク候補数 m 依存性を示す.

図 5 から明らかなように，AP 過程ではリンク候補の数 m を増加させると，相転移を起こすために必要なリンク数は徐々に増加し(グラフの傾きが徐々に急峻になり), m＝10, 15，20 では爆発的パーコレーションが引き起こされる．しかし，さらにリンク候補数 m を増加させると，ステップ的な相転移を繰り返す．これは，AP 過程ではリンク候補としてループ接続の発生を許容しているためである．

一方，改良 AP 過程ではループ接続を許容しないようにしたため, 図 6 に示すようにリンク候補数 m を増加させても，常に爆発的パーコレーションが引き起こされる．

図 7 は，3.3 の(手順 2-1)で設定した最大クラスタサイズの閾値を 10 とした場合の相転移に必要なリンク数のリンク候補数 m 依存性を示している．なお，図 7 の値は，それぞれの場合について 10 個のグラフを作成した場合の平均値である．推測通り，改良 AP 過程では，AP 過程と比べて所要リンク数が約 1/5 以下に抑えられている．なお，標準偏差についても，改良 AP 過程では，AP 過程と比べてリンク候補数 m が 10 以上において 1/100 以下になることを確認している．

また図 7 より，改良 AP 過程ではリンク候補数を m≧10 に増加させても，相転移に必要なリンク数は大きく変化しないことが分かる．提案 AP 過程の計算量は，AP 過程と同様$O(m)$でスケールするため，リンク候補数 m を小さくすると計算量を小さくできる．したがって，改良 AP 過程は計算量の観点からも有効であることが分かる．

図 8 および図 9 は，それぞれ AP 過程および改良 AP 過程によって生成されたネットワークの次数分布を表している．両方の場合とも次数分布は指数分布を示すが，相転移に必要なリンク数が AP 過程において最小となるリンク候補数 m=10 では，ノード次数の最大値が，AP 過程で 6，改良 AP 過程では 5 と小さく，また両過程の次数分布は$\approx e^{-1.2k}$でほぼ同一である．

一方，図 8 において，リンク候補数 m=2 や 100 の場合，すなわち相転移に必要なリンク数が大きい場合には，次数分布の指数が−0.75 と大きく，ノード次数の最大値も 13 と大きくなっている．このことからも，AP 過程ではループを構成するリンクが多数接続されていることが推測できる．

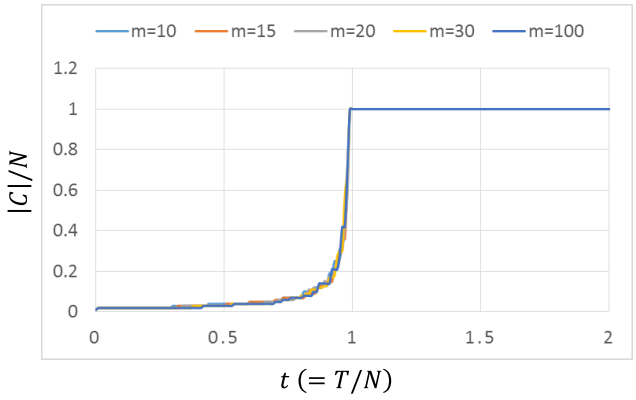

図 10　相転移の様子(N=100)
(改良 AP 過程に基づくリンク接続の場合)

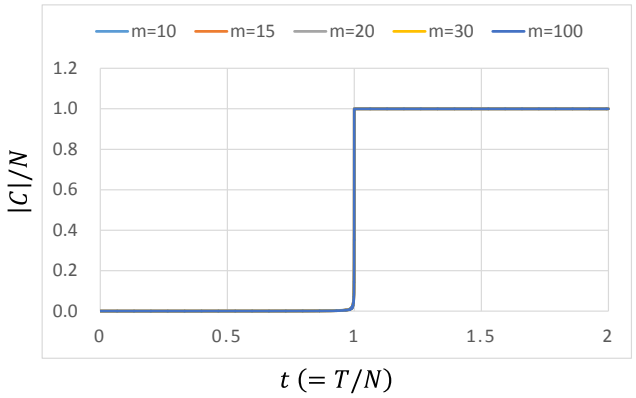

図 11　相転移の様子(N=10000)
(改良 AP 過程に基づくリンク接続の場合)

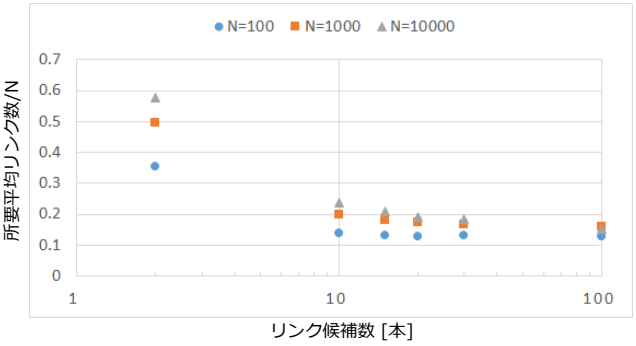

図 12　相転移に必要なリンク数の平均値
(改良 AP 過程に基づくリンク接続の場合)

(2)　ネットワークサイズ依存性

図 10 および図 11 に，AP 過程および改良 AP 過程に従ってネットワーク生成を行った場合の爆発的パーコレーションの様子を，ネットワークサイズ(全ノード数 N)を 100, 10000 と変えた場合についてそれぞれ示す．ネットワークサイズが増加するにしたがって，急激に相転移が起こることが分かる．図 12 には，相転移に必要なリンク数のネットワークサイズに対する比を示している．図 12 の値は，それぞれのネットワークサイズについて 10 個のグラフを作成した場合の平均値である．リンク候補数 m を 10 以上に選べばネットワークサイズを増加させても，相転移に必要なリンク数のネットワークサイズに対する比はほぼ変化しないことから，提案方式はネットワークサイズに対するスケーラビリティが高いと言える．なお，所要リンク数の標準偏差についても評価を行った結果，平均値と同様にその比はネットワークサイズに依存しないことが分かっている．

(3)　生成されるネットワークの類似性

上記(1)で述べたように，相転移に必要なリンク数が AP 過程において最小となるリンク候補数 m=10 の場合と，改良 AP 過程とで各々生成されるネットワークは次数分布の観点からは似た構造をしていることが推測できる．また図 9 の次数分布から，改良 AP 過程ではリンク候補数 m を 10 以上に選べば，生成されるネットワークは似た構造をしていることが推測できる．本節ではそれを定量的に示す．

ネットワークのグラフ構造としての非類似度を示す指標として，最近 Schiever らによる D-measure が提案されている[18]. D-measure は Hamming 距離[19]やグラフ編集距離[20]，Jaccard 指標[21]などの従来の類似性指標では識別できないようなグラフ間の類似度も表すことができ，次式で表される．

$$\mathrm{D}(\mathrm{G},\mathrm{G}') = w_1\sqrt{\frac{J_H(\mu_G,\mu_{G'})}{log2}} + w_2|NND(G) - NND(G')| + w_3\sqrt{\frac{J_H(P_{\alpha G^C},P_{\alpha G'^C})}{log2}} \quad \cdots (1)$$

$$NND(G) = \frac{J(P_1,\dots,P_N)}{log(d_G+1)}$$

$$J(P_1,\dots,P_N) = \frac{1}{N}\sum_{i,j} P_i(j)log\left(\frac{P_i(j)}{\mu_j}\right)$$

$$\mu_j = \frac{\sum_{i=1}^{N} P_i(j)}{N}$$

ここで，$P_i(j)$はノードiから距離jにあるノードの割合，$J_H(x,y)$は Jensen-Shannon divergence [22]，d_Gはグラフ G の直径である．また，$w_1 = 0.45$, $w_2 = 0.45$, $w_3 = 0.1$である．

図 13 および図 14 に評価結果を示す．図 13 は，リンク候補数 m を変えた AP 過程で生成されたグラフと，リンク候補数 m=10 の場合の改良 AP 過程で生成されたグラフとの D-measure の相図である．各リンク候補数について 10 個ずつグラフを生成し，グラフ間の D-measure をプロットしている．推測通り，リンク候補数 m=10 の場合，AP 過程で生成されたグラフと改良 AP 過程で生成されたグラフとは非常に良く似ていることが分かる．一方で，リンク候補数 m が 2 や 30 の場合の AP 過程で生成されたグラフと，リンク候補数 m=10 の場合の改良 AP 過程で生成されたグラフ

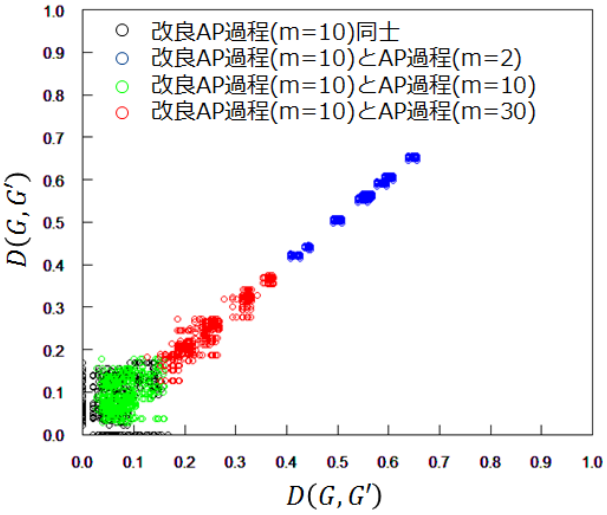

図 13　生成されたグラフ間の非類似度
(AP 過程と改良 AP 過程との比較)

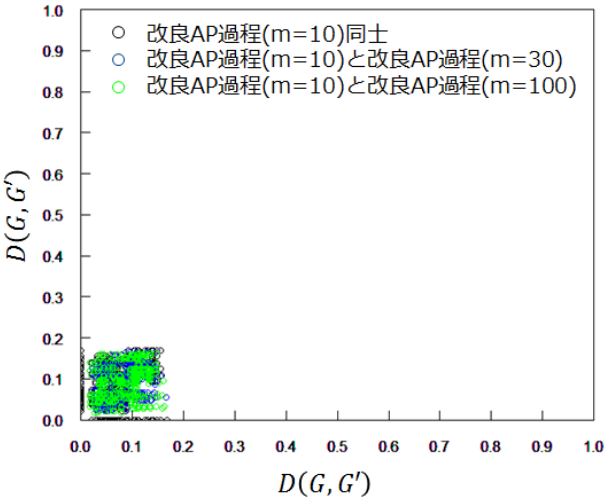

図 14　生成されたグラフ間の非類似度
(改良 AP 過程同士の比較)

は大きく異なることが分かる.

図 14 は，リンク候補数 m を変えた改良 AP 過程で生成されたグラフ同士の D-measure の相図である．図 14 から，リンク候補数 m が 10 以上であれば，改良 AP 過程で生成されるグラフの類似度は高いことが定量的に示された.

5. まとめ

膨大な数のデバイスがネットワークに接続される IoT システムでは，分散的に Attestation を行う場合と，大域的な情報共有を行う場合とが要求されると考えられる.そこで，本稿では集中/分散切り替え可能な Attestation を実現するために，爆発的パーコレーションを用いた方式を提案した．また，そのネットワーク生成手順として，既存の Achlioptas 過程を改良した手順を提案した．解析の結果，提案した方式を用いることで，通常の Achlioptas 過程の場合に比べて，切り替えに必要なリンク数を 1/5 以下に削減できることを示した．また，提案方式では切り替えに必要なリンク数のネットワークサイズに対する比がほぼ一定であり，ネットワークサイズに対するスケーラビリティが高いことを示した．さらに，Achlioptas 過程と提案方式で生成されたネットワークの類似度を D-measure を用いて定量的に評価し，AP 過程ではリンク候補数 m に応じて生成されるネットワーク構造が大きく異なるが，提案方式ではリンク候補数 m を 10 以上にすれば生成されるネットワーク構造の類似度が高いことを示した.

参考文献

[1] “Stuxnet worm 'targeted high-value Iranian assets”. http://www.bbc.com/news/technology-11388018 .
[2] “Major cyber attack hits Norwegian oil industry”. http://www.theregister.co.uk/2014/08/27/nowegian_oil_hack_campaign/ .
[3] “A Cyberattack Has Caused Confirmed Physical Damage”. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/ .
[4] “Iranian Hackers Claim Cyber Attack on New York Dam”. http://www.nbcnews.com/news/us-news/iranian-hackers-claim-cyber-attack-new-york-dam-n484611 .
[5] Steiner, R. V., & Lupu, E. (2016). Attestation in Wireless Sensor Networks: A Survey. ACM Computing Surveys (CSUR), 49(3), 51.
[6] Callaway, D. S., Newman, M. E., Strogatz, S. H., & Watts, D. J. (2000). Network robustness and fragility: Percolation on random graphs. Physical review letters, 85(25), 5468.
[7] Achlioptas, D., D'souza, R. M., & Spencer, J. (2009). Explosive percolation in random networks. Science, 323(5920), 1453-1455.
[8] Riordan, O., & Warnke, L. (2011). Explosive percolation is continuous. Science, 333(6040), 322-324.
[9] Oh, S. M., Son, S. W., & Kahng, B. (2016). Explosive percolation transitions in growing networks. Physical Review E, 93(3), 032316.
[10] Araujo, N. A., & Herrmann, H. J. (2010). Explosive percolation via control of the largest cluster. Physical review letters, 105(3), 035701.
[11] Seshadri, A., Perrig, A., Van Doorn, L., & Khosla, P. (2004, May). SWATT: Software-based attestation for embedded devices. In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on (pp. 272-282). IEEE.
[12] Seshadri, A., Luk, M., & Perrig, A. (2008, June). SAKE: Software attestation for key establishment in sensor networks. In International Conference on Distributed Computing in Sensor Systems (pp. 372-385). Springer Berlin Heidelberg.
[13] Seshadri, A., Luk, M., Perrig, A., van Doorn, L., & Khosla, P. (2006, September). SCUBA: Secure code update by attestation in sensor networks. In Proceedings of the 5th ACM workshop on Wireless security (pp. 85-94). ACM.
[14] Asokan, N., Brasser, F., Ibrahim, A., Sadeghi, A. R., Schunter, M., Tsudik, G., & Wachsmann, C. (2015, October). Seda: Scalable embedded device attestation. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 964-975). ACM.
[15] Ibrahim, A., Sadeghi, A. R., Tsudik, G., & Zeitouni, S. (2016, July). DARPA: Device attestation resilient to physical attacks. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 171-182). ACM.
[16] Ambrosin, M., Conti, M., Ibrahim, A., Neven, G., Sadeghi, A. R.,

& Schunter, M. (2016, October). SANA: Secure and Scalable Aggregate Network Attestation. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 731-742). ACM.
[17] Erdos, P., & Rényi, A. (1960). On the evolution of random graphs. Publ. Math. Inst. Hung. Acad. Sci, 5(1), 17-60.
[18] Tiago A. Schieber, Laura Carpi, Albert Díaz-Guilera, Panos M. Pardalos, Cristina Masoller and Martín G. Ravetti. (2017). Quantification of network structural dissimilarities. Nature Communications, 8, Article number: 13928.
[19] Hamming, Richard W. (1950). Error detecting and error correcting codes. Bell System Technical Journal. 29 (2): 147–160.
[20] Black, Paul E., ed. (14 August 2008), Levenshtein distance, Dictionary of Algorithms and Data Structures, U.S. National Institute of Standards and Technology, retrieved 2 November 2016.
[21] Jaccard, Paul (1901), Étude comparative de la distribution florale dans une portion des Alpes et des Jura, Bulletin de la Société Vaudoise des Sciences Naturelles, 37: 547–579.
[22] Endres, D. M.; J. E. Schindelin (2003). A new metric for probability distributions. IEEE Trans. Inf. Theory. 49 (7): 1858–1860.