Vol.2019-DPS-181 No.6
2019/12/26

隣接関係の解析を用いた位置検証に関する一考察

笹沼 涼介[†1]　小泉 佑揮[†1]　長谷川 亨[†1]

概要：ユーザがアップロードした位置情報を利用した様々な位置ベースサービスが提供される一方で，ユーザが申告する位置を偽装することは容易であり，位置ベースサービスにとって申告される位置の検証が課題となっている．この課題に対して，位置情報を提供するユーザに対して，位置ベースサービスの提供者に，近接無線通信などによる隣接関係を申告させ，隣接関係に基づいたグラフを解析することで，偽装された位置申告を検出する手法が提案されている．本稿では，隣接関係を用いたグラフ解析に基づく位置検証の利点および欠点について議論する．

1. はじめに

ユーザの位置に紐づいた情報（**位置情報**と呼ぶ）をアップロードする，クラウドソーシングベースの位置ベースサービスが普及している [1]．信頼性の高い位置情報をサービスとして提供するには，ユーザが申告する位置の正確さが鍵である．特に，位置情報として，自動車事故や火災の発生現場の写真などのクリティカルな情報を提供する場合には，悪意あるユーザが偽装した位置を申告できないように，ユーザが申告した位置を検証する**位置検証サービス**が必要となる．

これまでには，アドホック網や無線センサ網において，ユーザの端末（ノードと呼ぶ）が申告した位置の検証手法が，多数研究されている [2]．これらの多くは，基準となる地点に信頼できるノードを設置し，位置検証の対象であるノードに対して電波や音波などの信号を送信し，応答の信号受信までの往復時間から対象までの距離を推定することに基づいている [3]．しかしながら，これらの手法は，以下の観点から，位置ベースサービスで採用することは困難である．まず，信号の処理時間が位置の推定誤差の原因となるため，信号をソフトウェアでなくハードウェアで処理する必要があり，高価なハードウェアが必要となる．次に，位置ベースサービスでは，無線アドホック網と異なり，対象の範囲が広く，多数の信頼できるノードを設置する必要がある．

これに対して，位置ベースサービス *ViewMap* [4] では，ユーザに申告させた自身の位置と近接無線通信により発見したユーザとの隣接関係を用いて，ユーザが申告した位置を検証するサービスを提案している．ここで，ViewMap のような位置検証サービスでは，悪意のあるユーザ（攻撃ノード）が，隣接した架空の**偽装ノード**作成し，偽装した位置を申告する攻撃が行われる可能性が高い．この攻撃に対処するため，ViewMap では，TrustRank と呼ばれる隣接関係解析アルゴリズム [5] を用いて，ユーザのノード群が申告した隣接関係から作成したグラフ（**位置ベースグラフ**と呼ぶ）に生じる矛盾を解析することで，偽装された位置を検出する．具体的には，TrustRank は信頼できるノード（信頼の起点と呼ぶ）を配置し，その起点からスコアと呼ばれる値を流し，その値の大小で偽装ノードを検出する．

しかしながら，ViewMap では，TrustRank の偽装ノードを用いた攻撃への耐性を評価できていない．ViewMap では，検証対象が事前に決まっておらず，その時々に決定されるため，攻撃ノードは偽装ノードをサービス対象の領域にランダムかつ均等に配置する攻撃しか行えない．一方，一般的な位置ベースサービスでは，攻撃ノード自らが位置情報を指定すると想定されるため，ランダムな配置より効果の高い偽装ノードの配置を行える．

本稿では，ランダムな配置に加えて，偽装ノードへのスコアの流量が減少しない攻撃として，偽装ノードを直線上の配置する攻撃を取り上げ，TrustRank の攻撃に対する耐性を評価する．本稿の貢献は，以下の通りである．第一に，ViewMap と異なり，攻撃ノードが，位置情報が必要な位置を知っている一般的な条件で，位置の偽装を成功させやすい偽装ノードの配置を考案するとともに，考案した攻撃への TrustRank の耐性を評価した．第二に，TrustRank は，信頼の起点のノードから位置検証対象のノードへのホップ数が，偽装していないノード（正規ノードと呼ぶ）と比較して，偽装ノードが攻撃ノードを経過することでホップ数が

[†1] 現在，大阪大学 大学院情報科学研究科
Presently with Osaka University

ⓒ 2019 Information Processing Society of Japan

増加する特徴を活用して，両者のスコアを分離していることを明らかにした．第三に，この特徴より，TrustRank が信頼の起点から距離的に離れた偽装ノードと正規ノードを分離することが難しいことを明らかにした．

本稿の構成は以下の通りである．2 章で，位置検証サービスのシステムモデルを定義し，3 章で，TrustRank を用いた偽装位置検出について説明する．4 章では，位置検証サービスへの攻撃を定義し，5 章では，TrustRank の攻撃に対する耐性を評価する．6 章で関連研究を紹介し，最後に 7 章で本稿をまとめる．

2. 位置検証サービス

本章では位置検証サービスのシステムモデルを定義する．

2.1 システムモデル

位置検証サービスとして，図 1 に示すように，**ノードと位置検証サーバ** *(LVS: Location verification server)* から構成され，ノードが自発的にサービスに参加するクラウドソーシングベースを想定する．ノードは，位置検証で用いる自己証明可能な (self-certified) 識別子を持つ．ノードは，Wi-Fi や Bluetooth などの近接無線機能と GPS 機能を具備していることを仮定する．定期的に近接無線通信により識別子を交換し，LVS に，自身の識別子，位置，および，隣接したノードの識別子の集合を申告する．

LVS は，全てのノードが申告した隣接ノードの集合から隣接関係を抽出し，ノードを頂点，隣接関係を辺とする位置ベースグラフと呼ぶグラフを作成する．次に，TrustRank を用いて，位置ベースグラフを解析し，申告された位置の信頼度のスコアを計算し，偽装された位置を検出する．位置ベースグラフの構築と TrustRank を用いた位置検証法の詳細は，3 章で議論する．

ノードは，セキュリティの観点で，正しい位置を申告するオネストなノードと，LVS から見て正しい位置，あるいは偽装した位置のどちらを申告したかが分からないノードであるディスオネストなノードに分類できる．オネストなノードには，以下のノードがある．

- **信頼の起点**　正しい位置と隣接関係を申告する．

TrustRank では，この信頼の起点からスコアを注入して，各ノードのスコアを算出する．一方，ディスオネストなノードには，以下のノードが含まれる．

- **正規ノード**　正しい位置と隣接関係を申告する．
- **攻撃ノード**　正しい位置を申告するが，偽装ノードを作成し，架空の隣接関係を申告する．
- **偽装ノード**　攻撃ノードに架空のノードとして作成された実際に存在しないノードであり，申告する位置と隣接関係は，偽装されている．

なお，正規ノードは，正しい位置と隣接関係を申告するものの，LVS からは攻撃，および偽装ノードと区別がつかないという点で，ディスオネストなノードに分類される．

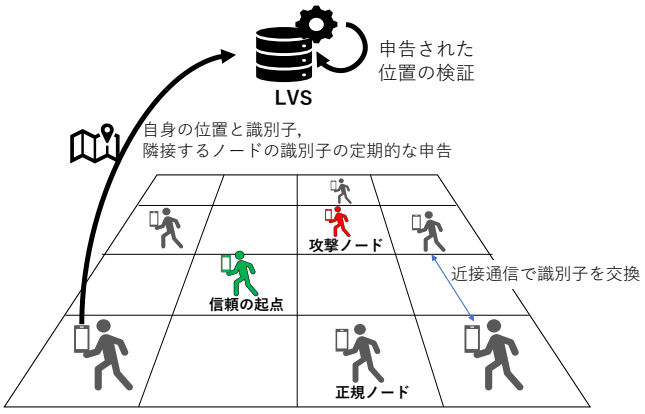

図 1　申告と位置検証のシナリオ

2.2 位置検証に対する脅威

ノードが証明書などを用いた検証可能な識別子を持つことを仮定すると，登録にかかる手間や心理的な障壁のため，位置ベースサービスに参加するノードが少なくなる可能性がある．このため，ソーシャルネットワークサービスのように，ノードは匿名の識別子を使用することとする．匿名な識別子の採用により，悪意のあるノード（攻撃ノード）は，複数の識別子を作成することで，複数の偽装ノードを作成することが可能になる．TrustRnak を用いた位置検証の目的は，攻撃ノードが作成した偽装ノードが申告する偽装された位置を検出することである．

3. 隣接関係を用いた偽装位置の検出

3.1 概要

本研究では，Wi-Fi や Bluetooth などの近接無線通信によって隣接ノードの識別子を交換することを隣接関係を有すると定義し，隣接関係を用いて各ノードが申告した位置を検証する手法 [4] を考える．

この手法では，各ノードは，自身の位置の申告と同時に，近接無線通信によって交換した隣接ノードの識別子を LVS に申告する．LVS では，ノードを頂点，申告された隣接関係を辺とするグラフを構成し，そのグラフ上で各頂点の信頼性を計算することで，位置の偽装を検出する．以降，このグラフを位置ベースグラフと呼ぶ．

各頂点の信頼性を検出する方法として，Web で信頼性の低いページを検出する技術である TrustRank [5] を用いる．TrustRank は，Web ページを頂点，ページ間のハイパーリンクを辺とするグラフを形成し，信頼できることが確認された Web ページに対応する頂点からのグラフの接続関係に基づいて各頂点に信頼性のスコアを計算する．以降，TrustRank によって算出される信頼性のスコアを，単にスコアと呼称する．位置ベースグラフを用いた位置検証では，位置と隣接関係の申告が必ず正しいと保証される信頼

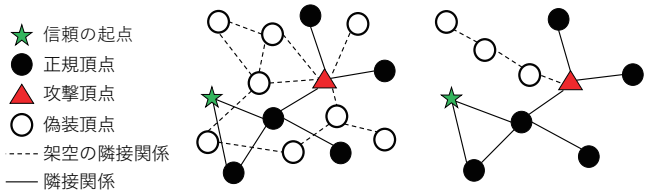

図 2 架空の隣接関係を含む位置ベースグラフ

の起点を用意し，TrustRank を用いて各頂点のスコアを計算する．

次章では，隣接関係を用いた位置ベースグラフの生成方法と TrustRank による位置の信頼性の計算方法を説明する．

3.2 位置ベースのグラフ

各ノードは，自身の識別子，位置，および，近接無線通信により確認できた隣接ノードの識別子を LVS にアップロードする．LVS は，各ノードを頂点，正しい隣接関係を辺とするグラフを形成する．正しい隣接関係を抽出するため，LVS では，2 つのノードが申告する位置から 2 点間の距離を求め，その距離が近接無線通信の範囲内に収まらない場合に矛盾が生じているとみなし，矛盾の発生している隣接関係を却下する．つまり，2 つのノードが十分に離れているにもかかわらず互いの識別子を隣接関係として申告したとしても，その隣接関係を棄却する．

2 章で議論したノードに対応する位置ベースグラフ上の頂点を，次の通りに定義する．

- **信頼の起点**　信頼の起点に対応する頂点を指す．TrustRank における信頼の起点に相当する頂点であるため，本稿では頂点ではなく，位置ベースグラフ上でも信頼の起点と呼称する．
- **正規頂点**　正規ノードに対応する頂点を指す．
- **攻撃頂点**　攻撃ノードに対応する頂点を指す．
- **偽装頂点**　偽装ノードに対応する頂点を指す．

これらの頂点によって構成される位置ベースのグラフの例を図 2 に示す．ある攻撃ノードが偽装ノードを配置して位置の偽装をしようとした場合，その偽装ノードは，現実には申告した偽装位置には存在しないため，その場の正規ノードとは隣接関係を構築することはできない．すなわち，位置ベースグラフに接続されない状態であるため，容易に偽装ノードが検出できる．これに対して，攻撃ノードが，隣接関係に基づいたグラフが構成されることを知っているものとすると，攻撃ノードは，自身は申告した位置に存在し，周囲の正規ノードとの隣接関係を形成しつつ，複数の偽装ノードを生成し，偽装ノードとの間に架空の隣接関係を申告する．最終的に，それらの偽装ノードから偽装した位置を申告する．具体的な偽装頂点の配置方法については，4 章で説明する．

3.3 TrustRank

TrustRank [5] は，Web 上のスパムページを検出することを目的としたアルゴリズムである．Web ページを頂点，ハイパーリンクを有効辺とするグラフの固有ベクトル中心性を利用した Web ページのランキングアルゴリズムである PageRank [6] をベースにしたアルゴリズムであり，人によって信頼できることが確認された小数のページを信頼の起点とし，その他の Web ページにスコアを算出することができる．

TrustRank は，信頼できる Web ページからハイパーリンクが設定されている Web ページは信頼できるという仮定のもと，ユーザのページ閲覧をある種のランダムウォークで表現し，グラフ上で信頼の起点からランダムウォークを開始して十分な時間が経過した後の各頂点におけるユーザが存在する確率を頂点のスコアとするアルゴリズムである．TrustRank におけるランダムウォークは，各頂点から，一定の確率でいずれかの信頼の起点を一様ランダムに選択してジャンプする，あるいは，出辺から一様にランダムで 1 つ選択して移動する．

スコアは，式 (1) を繰り返し計算することで導出する．

$$\boldsymbol{r} \leftarrow \alpha \boldsymbol{T} \boldsymbol{r} + (1-\alpha)\boldsymbol{d} \tag{1}$$

$\boldsymbol{r}$ はスコアを表すベクトルであり，各要素は各頂点のスコアに対応する．第一項は，隣接する頂点への遷移，第二項は離れた頂点へのジャンプを表す．α は，ランダムウォークにおいて有向出辺を辿る確率であり，つまり，確率 $(1-\alpha)$ で信頼の起点へとジャンプすることを意味する．行列 $\boldsymbol{T}$ の各要素 $\boldsymbol{T}(p,q)$ は，頂点 p から頂点 q に遷移する率であり，次式で定義する．

$$\boldsymbol{T}(p,q) = \begin{cases} 1/\omega(q) & \text{if } q \to p \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

ここで，$q \to p$ は，頂点 q から p への有効辺が存在することを表し，$\omega(q)$ を頂点 q の出次数とする．つまり，隣接する頂点を一様ランダムに選択し，その頂点に遷移することを意味する．

式 (1) の第二項のベクトル $\boldsymbol{d}$ の各要素 $\boldsymbol{d}(q)$ は，信頼の起点 q への遷移率を表し，以下の式で定義する．

$$\boldsymbol{d}(p) = \begin{cases} 1/|\mathcal{A}| & \text{if } p \in \mathcal{A} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

ここで，$\mathcal{A}$ は信頼の起点の集合，$|\mathcal{A}|$ を $\mathcal{A}$ の要素数である．これは，信頼の起点を一様ランダムに選択し，選択した信頼の起点に遷移することを意味する．

3.4 信頼の起点からの隣接関係を用いた偽装位置の検出

ViewMap [4] では，位置ベースグラフ上の各頂点のスコ

アに基づいて，申告位置の検証をする．具体的には，位置ベースのグラフでは，攻撃ノードは，実際に存在する位置においてのみ正規ノードとの隣接関係を申告できるという制限があるため，信頼の起点から偽装頂点までのグラフにおける距離は大きくなる傾向にあり，それに伴いスコアも小さくなると想定できる．この仮説に基づいて，スコアの低い頂点の位置は偽装されているとしている．

ViewMap [4] では，攻撃ノードの特定の攻撃を想定しており，スコアを意図的に向上させるような攻撃を想定していなかった．本研究では，4 章で位置検証に対する攻撃を定義し，5 章で，それらの攻撃が適用されたときのスコアを評価する．

4. 隣接関係を用いた偽装位置検出への攻撃

隣接関係を用いた偽装位置検出では，攻撃ノードは，攻撃頂点と偽装頂点間の隣接関係を自由に設定することができ，これを応用して，攻撃ノードが少数の偽装頂点を配置して高いスコアを得ることができる．本章では，攻撃ノードによる位置検証への攻撃の方法を議論する．

4.1 想定する位置ベースサービス

3 章で議論した位置検証方法には，想定する位置ベースサービスの種類に応じた攻撃が想定できる．本研究では，1) サービス側が位置を指定する場合と，2) ノードが位置を指定する場合の 2 つのサービスを検討する．前者のサービスとしては，ViewMap [4] が想定するような交通事故の動画収集など，ある位置をサービスが指定し，その位置に応じた情報を収集する位置ベースクラウドソーシングサービスがある．一方，後者については，ノードが主体となってある位置の情報を提供するクラウドソーシングサービスがある．例えば，オンライン地図におけるクラウドソーシング型の交通情報の取得や，クラウドソーシング型の天気実況中継サービスなどがある．

4.2 攻撃ノードの能力

攻撃ノードの能力として，次の条件を仮定する．まず，攻撃ノードは，信頼の起点および正規頂点を操作することはできない．また，攻撃ノードは，信頼の起点の位置を知らないものとする．これら 2 点の条件より，攻撃ノードが偽装頂点のスコアを上げるためには，偽装頂点の配置と攻撃頂点と偽装頂点間の隣接関係を調整するしか方法がない．最後に，1) の位置ベースサービスを検討した場合には，攻撃ノードは，位置ベースサービスが指定する位置に対する事前知識を持たないものとする．

4.3 位置検証への攻撃方法

1) の位置ベースサービスを想定した場合，攻撃ノードは，どの位置が指定されるか事前に知ることはできないため，偽装申告した位置に対応する偽装頂点が位置ベースサービスから選択される可能性を上げるためには，多くの偽装頂点を配置する必要がある．さらに，攻撃ノードは，位置ベースサービスが指定する位置に関する知識を保有しないため，結果的には，図 2(a) に示すように，多数の偽装頂点をランダムに配置する必要がある．

この場合，3 章で議論した通り，偽装頂点と正規頂点や信頼の起点からなる位置ベースグラフとの接点は，攻撃頂点のみである．したがって，TrustRank のランダムウォークにおいて，偽装頂点に到達するためには攻撃頂点を経由する必要がある．したがって，大量に偽装頂点を配備する必要がある場合は，信頼の起点から偽装頂点までのホップ数が長くなる傾向にあると同時に，大量の偽装頂点間でスコアが分散するため，偽装頂点のスコアは低くなる傾向にある．ViewMap では，この特徴を応用して偽装した位置申告を検出している．

一方で，2) の位置ベースサービスを想定した場合，攻撃ノードは任意の位置を指定できるため，位置ベースグラフ上の TrustRank の特徴を鑑みて，スコアが高くなるように偽装頂点を配置することが可能である．図 2(b) のように，嘘の位置を申告する偽装頂点までのホップ数が最小，かつ，各偽装頂点の出次数が最小になるように偽装頂点を配置することで，偽装頂点のスコアを高く維持することが可能である．この場合，偽装頂点のスコアが正規頂点のスコアに対して相対的に低くならずに偽装頂点の検出ができない可能性が危惧される．

次章では，シミュレーションにより，これらの 2 つの攻撃を想定し，偽装頂点のスコアを評価する．

5. 偽装位置の検出評価

4 章で議論した 2 種類の偽装頂点の配置に対して，Trust Runk が偽装頂点を検知できるかどうかを，シミュレーションにより評価する．本章では，ノードと頂点を同じ意味で用いることとし，ノードとしての動作を説明する場合も，グラフ上での隣接関係を説明する場合も頂点を用いて説明する．

5.1 シミュレーション条件

シミュレーションでは，2 km 四方の正方形に頂点を配置し，近接無線の通信範囲を 0.1 km とする．通信範囲内にある正規頂点は，双方とも正しく隣接関係を申告する．また，TrustRank のパラメータ $\alpha = 0.8$ とする．

シミュレーションは 10,000 回実施し，シミュレーションごとに，以下の条件の沿って，各頂点を異なる配置に設定した．

- 信頼の起点 1 個を正方形の中心に配置する．
- 正規頂点は，1598 個を正方形内のランダムな位置に配置する．0.1 km の通信範囲に存在する全正規頂点の対

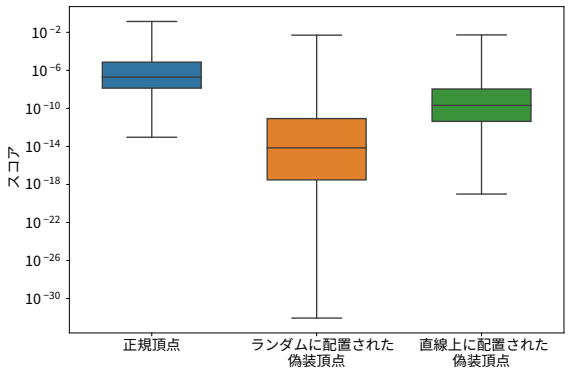

図 3 正規頂点と偽装頂点のスコアの分布

に，隣接関係を設定する．これにより，他の正規頂点との間に隣接関係と持たない孤立した正規頂点が存在しないようにしている．

- 攻撃頂点 1 個を，シミュレーション毎にランダムな位置を選択して配置する．
- 攻撃頂点は，偽装頂点を，以下の 2 通りのパターンで配置する．

(1) ランダムな配置：信頼の起点と正規頂点の合計と同数の 1600 個の偽装頂点を正方形内にランダムに配置する．配置した偽装頂点と攻撃頂点は，0.1km の通信範囲に存在する全ての偽装頂点と隣接関係を設定する．

(2) 直線上の配置：攻撃頂点から，ランダムに選択した方向に向かって，偽装頂点を通信範囲の 0.1km 間隔で直線上に配置する．

5.2 ホップ数とスコア

5.2.1 ホップ数を考慮しないスコアの分布

スコアの大小を用いて偽装頂点と正規頂点を分離可能かを判定するため，10,000 回のシミュレーションに対して，それぞれのスコアの分布を求めた．図 3 に，正規頂点，ランダムに配置された偽装頂点，直線上に配置された偽装頂点のスコアの分布を，それぞれ箱ひげ図で示す．箱ひげ図は，データの分布を表す統計図であり，第一四分位数から第三四分位数までの範囲を箱と呼ぶ長方形，最大と最小値をひげと呼ぶ線で表す．

図 3 から，ランダムに配置した場合のスコアは正規頂点よりも相対的に低いものの，正規頂点と偽装頂点のスコアの分布には重なりが多く，スコアに閾値を設けることでこれらを分離することは困難であることが分かる．

5.2.2 ホップ数を考慮したスコアの分布

Trust Rank では信頼の起点からのホップ数が増加すると，頂点のスコアは減少する．まず，正規頂点をランダム，かつ均等に配置した条件で，信頼の起点からの距離，ホップ数，スコアの関係を解析する．図 4 は，正規頂点に対して，

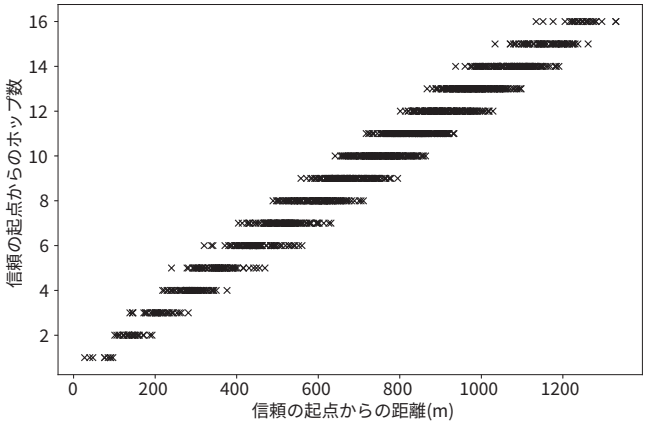

図 4 信頼の起点から正規頂点までの地理的な距離とホップ数の散布図

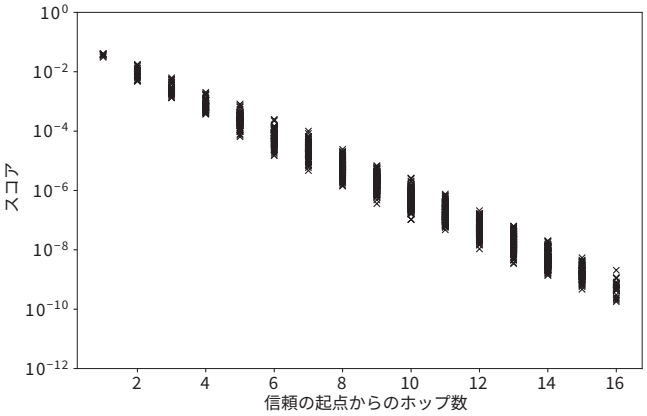

図 5 信頼の起点から正規頂点までのホップ数とスコアの相関

信頼の起点からの距離とホップ数を散布図で示し，図 5 は，正規頂点に対して，信頼の起点からのホップ数とスコアを散布図で示している．図 4 に示すように，信頼の起点からの地理的な距離とホップ数は正の相関があり，正規頂点が信頼の起点から離れるにつれてホップ数は増加する．さらに，図 5 に示すように，ホップ数が増加するにつれて，スコアは減少している．

正規頂点のスコアは，図 5 に示すように，ホップ数の増加に伴い減少する．このため，（1）のように，広い領域，例えば，2 km 四方の正方形にランダムに正規頂点を配置した場合，正規頂点のスコアの分散が大きくなる．この結果，信頼の起点から離れてスコア流入が少ない正規頂点のスコアと，攻撃頂点に近接し，攻撃頂点からのスコア流入の多い偽装頂点のスコアの区別が難しくなっている．

5.2.3 正規頂点と偽装頂点のホップ数

TrustRank は，Web ページのハイパーリンクのように，任意の 2 頂点間にリンクを設定できるグラフを対象としている． つまり，膨大な頂点数に対して，2 頂点間の最短経路の最大値であるグラフの直径が小さいグラフを仮定している [7]．この結果，Web ページにおいては，正規ページは信頼できるページからのホップ数が小さいのに対して，偽装したページは信頼できるページから直接ハイパーリン

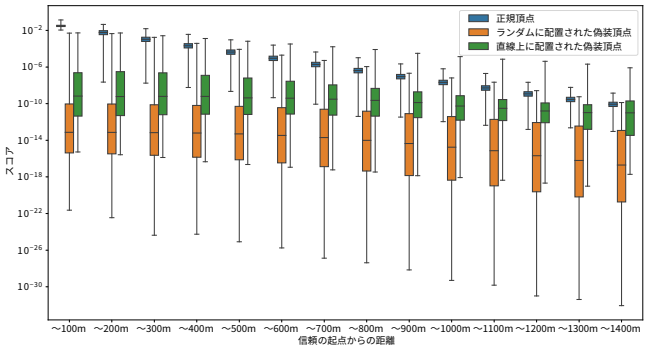

図 6 信頼の起点からの距離毎の正規と偽装頂点のスコアの分布

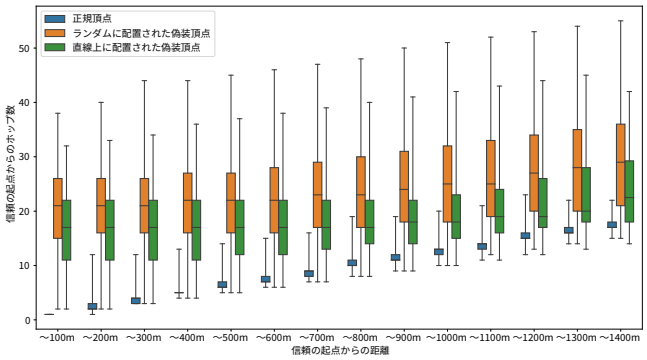

図 7 信頼の起点からの距離と正規と偽装頂点へのホップ数の分布

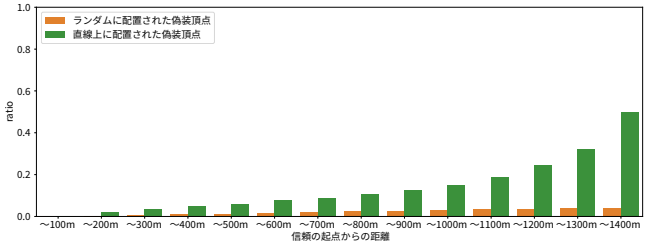

図 8 信頼の起点からの距離に対する，正規頂点の最小スコアを上回る偽装頂点の割合

クを設定することが難しく，信頼できるページからのホップ数が大きくなりやすい．このホップ数の差を利用して，TrustRank は，正規のページと偽装したページを分離している．

一方，位置ベースグラフでは，隣接関係の構築に地理的な制約があり，正規頂点は，信頼の起点に隣接したもの以外は，信頼の起点との直接隣接関係を築くことはできない．このため，5.2.2 章に示したように，信頼の起点から距離的が離れるにつれて，ホップ数は増加し，スコアは減少する．一方，偽装頂点は，必ず攻撃の頂点を経由しないと，スコアが流入しない．このため，信頼の起点から，攻撃頂点を経由した偽装頂点までのホップ数は，同じ距離に位置する正規頂点と比較して長くなることが想定できる．この影響を明らかにするため，以下のステップでスコアの分布を解析する．

まず，信頼の起点からの距離ごとに，正規頂点と偽装頂点のスコアの分布を比較する．図 6 は図 3 の結果に対して，信頼の起点からの距離 100 m 毎に区切った 100 m の幅の帯の中に位置する頂点の集合に対して，四分位数，最大値および最小値を箱ひげ図で示したものである．正規頂点と偽装頂点とも，信頼の起点からの距離が遠くなるにつれ，スコアが減少するが，一方，どの距離においても，正規頂点のスコアは，偽装頂点のスコアと比較して，大きい範囲に分布している．

次に，信頼の起点からの距離とホップ数の関係を，信頼の起点からの 100 m 幅の帯ごとに集計した結果を，図 7 に示す．図から明らかなように，偽装頂点までは攻撃頂点を経由する必要があるため，同じ距離であっても，偽装頂点までのホップ数は正規頂点の値より多くなる．偽装頂点をランダムに配置した場合，距離が遠い帯でも，2 つの分布の差は明確である一方で，偽装頂点を直線上に配置すると，偽装頂点までのホップ数の分布は正規頂点の分布との差が少なくなる．

5.3 TrustRank の脆弱性

文献 [4] の手法に対して，TrustRank のスコアに加えて信頼の起点からの距離やホップ数を用いることで，正規と偽装頂点を正確に分離できる可能性がある．しかしながら，信頼の起点からの距離が遠くなるにつれて，攻撃頂点を経由することで増加するホップ数が，ホップ数全体に占める割合が低くなるため，正規頂点と偽装頂点の分離が難しくなる．

以下では，距離が遠くになるにつれて分離が難しくなることを示すため，信頼の起点からの 100 m 幅の帯の正規頂点と偽装頂点を分離できるかどうかを評価する．具体的には，100 m 幅の帯ごとに，外れ値を除く正規頂点と偽装頂点のスコアの分布を用いて，正規頂点の最小スコアを閾値とした場合に，閾値を上回るスコアを持つ頂点を偽装頂点として判定する．図 8 は，100 m 幅の帯ごとに，誤って正規頂点と判定される偽装頂点の割合を示している．ここで，外れ値は，スコア分布の第一四分位数から四分位範囲の 1.5 倍を引いた値と第三四分位数に四分位範囲の 1.5 倍を加えた値を下限と上限とする範囲外の値としている．

図 8 より，信頼の起点からの距離の増加に伴い，誤って正規頂点と判断される偽装頂点の割合が増加している．また，誤って判断する割合は，ランダムに配置された偽装頂点と比較して，直線上に配置された偽装頂点の方が，距離の増加につれて大きくなっている．このことより，偽装頂点を直線上に配置する攻撃に対して，信頼の起点から距離的に離れた偽装頂点を検出することが難しくなっている．

6. 関連研究

無線アドホックネットワークやセンサーネットワークにおいて，ディスオネストなノードを仮定して，ノードが申告した位置をセキュアに検証する手法は多数提案されてき

た [2]．例えば，Verifiable Multilateration (VM) [8]，Secure Localization [9] など多数の位置検証プロトコルが開発された．これらの手法はいずれも距離の測定をベースとして，Distance-bounding [3] プロトコルを用いている．これらの Distance-bounding プロトコルは検証端末と被検証端末の距離を，電波の往復遅延時間の計測値から推定する．このため，ナノ秒オーダの精度で往復遅延時間を計測するために，高価な専用のハードウェアを搭載する必要がある．これに対して，文献 [10] や [11] では，カーネルあるいはデバイスドライバで往復遅延時間を計測しているが，計測誤差が数ミリ秒であるため，移動速度の速い電波を用いる場合，位置の推定誤差が大きくなる．電波の代わりに移動速度の遅い音波を用いることで [11]，位置の推定誤差を小さくすることは可能である．しかし，これらの手法では多数の信頼できる装置，端末を設置する必要があり，本稿で採用した TrustRank を用いた位置検証手法と比較してコストが高くなる．

一方，端末が申告した，自身の位置と近接する端末の位置から，隣接関係をエッジとする位置ベースグラフを解析することにより，偽装した位置を検出する手法として，TrustRank [5] が有用である．TrustRank を位置検証サービスに適用した研究は，本稿以外に ViewMap [4] がある．ViewMap では，攻撃者が検証対象の位置が知らないことを仮定して，偽装ノードをランダムに配置する攻撃に対する耐性を評価しているだけである．これに対して，本稿では，攻撃者が検証対象の位置を知っていることを仮定して，偽装ノードを配置する攻撃に対する耐性を評価している．この結果，TrustRank の一般的な位置検証サービスで使用するための課題を明らかにしている．

7. おわりに

本稿では，クラウドソーシングベースの位置ベースサービスにおいて，ノードの隣接関係を示すグラフ上で TrustRank を用いてノードが申告した位置を検証する手法に対して，攻撃者が偽装ノードを作成して位置を偽装する攻撃への耐性を評価した．この結果，信頼の起点から偽装ノードまでのホップ数が，攻撃者のノードを経由すること増加することを用いて，TrustRank が偽装ノードを検出することを示した．

謝辞：本研究は NICT 受託研究課題 191 によるものである。

参考文献

[1] Gummidi, S., Xie, X. and Pedersen, T.: A Survey of Spatial Crowdsourcing, *ACM Transactions on Database Systems*, No. 2, pp. 1–46 (2019).

[2] Zeng, Y., J.Cao, Hong, J., Zhang, S. and L.Xie: Secure localization and location verification in wireless sensor networks: a survey, *The Journal of Supercomputing*, No. 3, pp. 685–701 (2013).

[3] Brands, S. and Chaum, D.: Distance-bounding Protocols, *Proceedings of EUROCRYPT*, pp. 344–359 (1994).

[4] Kim, M., Lim, J., Yu, H., Kim, K., Kim, Y. and Lee, S.-B.: ViewMap: Sharing Private In-Vehicle Dashcam Videos, *Proceedings of USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, pp. 163–176 (2017).

[5] Gyöngyi, Z., Garcia-Molina, H. and Pedersen, J.: Combating web spam with TrustRank, *Proceedings of International Conference on Very Large Data Bases (VLDB)*, pp. 576–587 (2004).

[6] Page, L., Brin, S., Motwani, R. and Winograd, T.: The PageRank citation ranking: Bringing order to the web., Technical report, Stanford InfoLab (1999).

[7] Albert, R., Jeong, H. and Barabási, A.: Diameter of the world-wide web, *Nature*, Vol. 401, No. 6749, pp. 130–131 (online), DOI: 10.1038/43601 (1999).

[8] Capkun, S. and Hubaux, J. P.: Secure positioning of wireless devices with application to sensor networks, *Proceedings IEEE CCS*, Vol. 3, pp. 1917–1928 (2005).

[9] Anjum, F., Pandey, S. and Agrawal, P.: Secure localization in sensor networks using transmission range variation, *Proceedings of IEEE MASS.* (2005).

[10] Li, W., Mok, R. K. P., Wu, D. and Chang, R. K. C.: On the accuracy of smartphone-based mobile network measurement, *Proceedings of IEEE INFOCOM* (2015).

[11] Koizumi, Y., Yamamoto, Y. and Hasegawa, T.: Emergency Message Delivery in NDN Networks with Source Location Verification, *Proceedings of IEEE GLOBECOM Workshop* (2019).

ⓒ 2019 Information Processing Society of Japan