アドホックネットワーク上のTop-k検索における端末のグルーピングを用いたデータ差替え攻撃端末の特定手法

津田　琢士† 　駒井　友香† 　佐々木勇和† 　原　隆浩† 　西尾章治郎†

† 大阪大学大学院　〒 565–0871 大阪府吹田市山田丘 1-5

E-mail: †{tsuda.takuji,komai.yuka,sasaki.yuya,hara,nishio}@ist.osaka-u.ac.jp

あらまし　アドホックネットワークにおいて，Top-k 検索は有効な検索であるが，ネットワーク内に攻撃端末が存在する場合，検索精度が低下してしまう．筆者らはこれまでに，検索結果に入る必要なデータを不要なデータと差し替えるデータ差替え攻撃を提唱し，この攻撃による検索精度の低下を防ぐ Top-k 検索手法および攻撃端末特定手法を提案した．しかし，これらの手法は基本的に攻撃端末が 1 台と想定しており，さらに攻撃端末が複数存在する場合，攻撃端末の特定に長い時間かかってしまう．そこで，本研究では，ネットワーク内の端末が特定した攻撃端末の情報を共有し，効率的に攻撃端末を特定する手法を提案する．この手法では，共有した情報の類似度に基づいて端末をグルーピングし，攻撃端末と通常端末を分類することにより，特定した攻撃端末の情報が端末間で大きく異なる場合や誤った情報を流布する端末が存在する場合でも，精度よく攻撃端末を特定できる．

キーワード　アドホックネットワーク，Top-k 検索，データ差替え攻撃，グルーピング

1. はじめに

近年，無線通信端末のみで構成された一時的なネットワークであるアドホックネットワークへの関心が高まっている．アドホックネットワークでは通信基盤が必要でないため，災害地域などでの応用が期待されている．特に，通信帯域が限られているアドホックネットワークでは，膨大なデータの中から必要なデータのみを効率的に検索するため，何らかの値（スコア）によって順位づけられたデータの上位 k 個のものを検索する Top-k 検索が有効と考えられる．しかし，ネットワーク内の端末が外部からの攻撃により攻撃端末となり，ブラックホール攻撃やジャミング攻撃などの DoS 攻撃 [9] を行うと，重要な情報の欠落など重大な損害が発生する可能性がある．そのため，このような攻撃に耐えうるアドホックネットワーク上の Top-k 検索手法が必要である．

筆者らはこれまでに，他の端末から受信したデータを自身が保有するスコアの低いデータに差し替えて返信する攻撃（データ差替え攻撃とよぶ）を提唱した [8]．攻撃端末がデータ差替え攻撃を行った場合，クエリ発行端末は正しい検索結果を取得できない可能性がある．さらに，スコア上位 k 個のデータは中継端末で置き換えられ，その状況をクエリ発行端末が把握できないため，攻撃を受けたかどうか判断することができない．そのため，アドホックネットワークにおける Top-k 検索に対して，データ差替え攻撃は強力な攻撃である．

そこで，筆者らは，アドホックネットワークにおけるデータ差替え攻撃を考慮した Top-k 検索手法および攻撃端末特定手法 [8] を提案した．この Top-k 検索手法では，2 本の経路によるデータ返信により検索結果の取得精度を維持しつつ，攻撃の検知が可能である．さらに，クエリ発行端末が攻撃を検知した後，攻撃端末の候補を絞り込む．その後，攻撃端末特定手法では，攻撃端末の候補が送信したクエリ応答を確認することで，攻撃端末を特定する．これらの手法を用いることで，取得精度を維持しつつ，攻撃の検出および，攻撃端末の特定を行うことができる．

しかし，この方法では，基本的に攻撃端末が 1 台と想定している．さらに，クエリ発行端末から遠い位置に存在する攻撃端末の特定は困難な場合が多いため，攻撃端末が複数存在する環境では，攻撃端末の特定に長い時間がかかってしまう可能性が高い．したがって，複数台の攻撃端末が存在する環境でも攻撃端末を早急に特定し，ネットワークから排除する必要がある．そのための効果的なアプローチとして，各端末が攻撃端末を特定した後，特定した攻撃端末の情報をネットワーク内の他端末に送信して情報を共有することで，より多くの攻撃端末を早急に排除できると考えられる．しかし，攻撃端末は自身が特定されないように通常端末のことを攻撃端末と偽って情報を送信することが考えられ，各端末は受信した情報を単純に信頼することは出来ない．一方，上述のように位置的な条件により特定しにくい攻撃端末が存在するため，受信した情報を基に多数決のような単純な手法で攻撃端末を決定すると，通常端末を攻撃端末と判定してしまう可能性が高くなる．

そこで，本稿では，アドホックネットワーク上の Top-k 検索における端末のグルーピングを用いたデータ差替え攻撃端末の特定手法を提案する．提案手法では，ネットワーク内で攻撃端末に関する情報を共有するために，攻撃端末を特定した端末は，攻撃端末の情報を他端末に送信する．ここで，ネットワーク内の端末は，自身と隣接する攻撃端末を特定しやすく，自身から遠い位置に存在する攻撃端末はほとんど特定できないという傾向があるため，隣接する通常端末同士は同じ端末を特定する場合が多くなる．そのため，攻撃端末が通常端末を攻撃端末であると偽ると，隣接する通常端末が特定した攻撃端末に関す

る情報とは異なる場合が多くなる．そこで，提案手法では，共有した攻撃端末の情報の類以度に基づいてネットワーク内の端末をグルーピングし，各グループ内で攻撃端末候補を通常端末と攻撃端末に分類する．さらに，各グループの判定結果に基いて，最終的な攻撃端末の判定を行う．提案手法では，攻撃端末が通常端末のことを攻撃端末と偽って通知メッセージを送信する攻撃（虚偽通知攻撃）を行なっても，通常端末との情報の類似度の差が明確となり，容易にその攻撃を検出できる．さらに，攻撃端末が通常端末との類似度を高くするように，通常端末が特定した攻撃端末に加えて，他の通常端末を攻撃端末と偽ってネットワーク内に通知したとしても，グループ内の他の通常端末は攻撃端末のみを特定しているため，虚偽通知攻撃を検出できる場合が多く，その影響を小さく出来る．

以下では，2. で関連研究を紹介し，3. で先行研究について説明する．その後，4. で想定環境について，5. で提案手法についてそれぞれ説明する．6. でシミュレーション実験により提案手法の有効性を示す．最後に，7. で本稿のまとめと今後の予定について述べる．

2. 関 連 研 究

分散システムにおいて悪意を持ったユーザや故障端末が存在する場合に，その端末の行動を評価し，ネットワークから排除するシステムとしてレピュテーションシステムが挙げられる．本研究では，アドホックネットワーク内に存在する攻撃端末について，各端末が互いの情報を共有して攻撃端末を排除することを考えているため，レピュテーションシステムを利用できると考えられる．そこで本章では，分散システムにおけるレピュテーションシステムに関する従来研究について紹介する．さらに，本研究と従来研究を比較し，本研究との相違点を述べる．

非構造 P2P ネットワークやセンサネットワーク，アドホックネットワークでは，ネットワーク内の端末の信頼度を考えたレピュテーションシステムに関する研究が行われている．文献 [5] では，非構造 P2P ネットワークにおいて，ネットワーク内の端末が，他の端末から受信したファイルの正誤から自身以外の端末のローカルの評価値を計算し，計算したローカルの評価値をネットワーク内の端末にフラッディングする．各端末は，他の端末から受信した評価値と自身が計算したローカルの評価値から，各端末のグローバルな評価値を計算することで，悪意のある端末を特定する．文献 [6] では，アドホックネットワークにおいて，ネットワーク全体の端末による評価を統合管理するための評価者端末を複数台用意し，各端末の評価値をハッシュ関数を用いて管理するレピュテーション管理システムを提案している．これより，ネットワーク内のある 1 台の評価者端末が攻撃端末となった場合に，誤った評価が行われることを防ぐことができる．しかし，これらの研究は，各端末の評価値は信頼できることを想定しており，嘘の評価値を送信するなど不正評価について考慮していない．

文献 [2], [3] では，レピュテーションシステムにおいて嘘の評価値を送信する不正評価に関する研究が行われている．文献 [2] では，アドホックネットワークにおけるレピュテーションの際に，評価者端末が，評価対象の端末から受信した評価値があらかじめ指定されたしきい値以内か，制限時間以内に評価対象から評価値を受信しているか，評価対象から受信した評価値と自身が記録していた過去の評価値との差分がしきい値以内かの三点を確認することで，不正な評価値を除く方法を提案している．この方法では，攻撃端末が常に攻撃を行うことを想定しており，本研究の想定とは異なる．文献 [3] の手法では，非構造 P2P ネットワークにおいて，各端末は，事前に送信先の端末と暗号鍵を交換しておき，送信先の端末に対し，自身の識別子と送信先の端末の現在および過去の評価値を暗号化して送信する．送信先の端末は，受信した評価値を解読し，確認することで不正な評価値を除外する．この研究では，ネットワーク全体で攻撃端末の情報を共有せず，各端末が対象の端末から受信した情報のみから対象の端末の評価値を算出しているため，本研究の想定とは異なる．

3. 先 行 研 究

本章では，先行研究 [8] で提案した，Top-k 検索手法および攻撃端末特定手法について簡単に説明する．

3.1 Top-k 検索手法

クエリ発行端末は，初めにネットワーク全体に検索条件や要求データ数 k を添付した検索クエリをネットワーク全体にフラッディングする．検索クエリを受信した端末は，自身からクエリ発行端末までの複数の経路を把握する．クエリ応答送信時に，各端末は，攻撃端末を経由しないようにデータを送信するために，隣接する端末のうち 2 台の端末にクエリ応答を送信する．これにより，1 つの経路上に攻撃端末が存在したとしても取得精度を維持することが可能となる．また，送信先の端末においてデータの送信経路を把握するために，クエリ応答にメッセージの送信元および送信先端末の情報を格納したクエリ応答の転送経路を添付して送信する．クエリ発行端末では，隣接する端末から受信したデータとデータに添付されたクエリ応答の転送経路を用いて，攻撃の検知を行う．この時，隣接端末から受信したクエリ応答に添付されたクエリ応答の転送経路に検索結果のデータを所有する端末が含まれているのに，そのクエリ応答に含まれるデータに検索結果のデータが含まれていない場合，攻撃があったと判断する．

3.2 攻撃端末特定手法

クエリ発行端末は，攻撃の検知後，攻撃端末の特定を行う．クエリ発行端末は，クエリ応答に含まれているべき検索結果のデータを保有する端末から自身までのクエリ応答の転送経路を求める．差し替えられたデータが含まれるクエリ応答の経路上に存在する全ての端末は，攻撃の機会があると考えられる．この手法では基本的に攻撃端末を 1 台と想定しているため，差し替えられたデータが含まれる経路上の端末のうち全ての経路に含まれる端末を攻撃端末の候補とする．攻撃端末の候補を絞り込んだ後，攻撃端末の候補の送信したクエリ応答を問い合わせ，どのようなデータを送信したかを確認する．この際，攻撃端末の候補に直接問い合わせてしまうと，その端末が実際に攻撃端末であった場合，問合せを無視されたり嘘の情報を返信されて

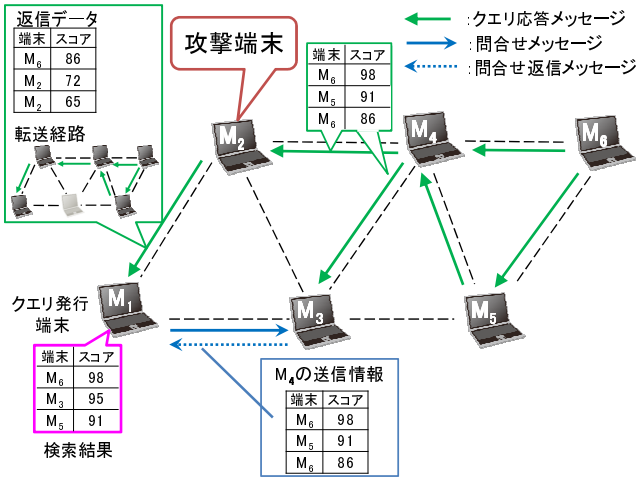


図 1　攻撃端末の特定

Fig. 1　Identification of the malicious node

しまうことが考えられる．そのため，攻撃端末の候補がクエリ応答を送信した際の送信先端末に，攻撃端末の候補が送信したデータの情報を問い合わせる．これにより，通常端末を誤って攻撃端末と特定することなく，攻撃端末を特定する．

攻撃端末を特定する動作について図 1 を用いて説明する．クエリ発行端末 M_1 は，M_2 から受信したクエリ応答の転送経路より，検索結果に入るデータの所有端末 M_5 および M_6 が送信元端末に含まれていることがわかる(注1)．しかし，M_2 からの返信データには M_5 および M_6 が所有する検索結果に入るデータ（スコア：98，91）が含まれていないため，クエリ発行端末はこのメッセージの返信データが差し替えられた（攻撃を受けた）ことを検知できる．次に，検索結果に入るデータを所有する M_5 および M_6 から，M_2 を経由してクエリ発行端末 M_1 までクエリ応答が送信された経路をそれぞれ算出する．全ての経路の共通部分は M_2 および M_4 であるため，これらの端末を攻撃端末の候補とする．クエリ発行端末 M_1 は，攻撃端末の候補である端末 M_4 のクエリ応答の送信先であり，攻撃端末の候補ではない端末 M_3 に問合せメッセージを送信する（M_2 は，ホップ数が 1 なので，問合せを行わない）．問合せメッセージを受信した M_3 は，攻撃端末の候補 M_4 からの返信データのスコア情報（スコア：98，91，86）を M_1 に返信する．M_3 から問合せ返信メッセージを受信した M_1 は，受信したスコア情報（スコア：98，91，86）より，M_4 は検索結果に含まれる正しいデータを返信していることを確認する．これにより，M_4 は正しく返信しているが，M_2 より受信したクエリ応答に必要なデータが含まれなかったため，M_2 を攻撃端末であると特定する．

この研究では，検索結果の取得精度を維持しつつ，攻撃端末を特定できる．しかし，基本的に攻撃端末が 1 台と想定している．さらに，クエリ発行端末から遠い位置に存在する攻撃端末の特定は困難な場合が多い．そのため，攻撃端末が複数台存在する場合，すべての攻撃端末を特定するのに長い時間がかかってしまう．

(注1)：このとき，クエリ発行端末 M_1 は，M_3 から正しい検索結果を受信しているため，M_5 および M_6 がスコアが高いデータを保持していることを把握している．

4.　想 定 環 境

本稿では，アドホックネットワークを構成する各端末が，自身と他の端末が持つデータに対して Top-k 検索を行う環境を想定する．さらに，各端末は攻撃端末を特定した後，ネットワーク内で攻撃端末に関する情報を共有するためにメッセージを送信する．システムモデルおよび攻撃モデルについて詳細を以下に示す．

4.1　システムモデル

ネットワーク内には，同等の性能を持つ n 台の端末（識別子：M_1，M_2，...，M_n）が存在し，各々が自由に移動する．また，ネットワーク内の端末は，自身の通信範囲およびネットワークの領域サイズを把握しているものとする．本研究では，テロ災害地域での救急活動などで，救急隊員の所有している通信端末を用いてアドホックネットワークを構築し，救急隊員が被災者情報を交換する環境を想定しており，セキュアな通信やデータの保護が重要である．そのため，ネットワーク内の端末は，公開鍵と秘密鍵を所有しており，データ（クエリ応答）を送信する際，送信先以外の端末にデータを解読されないように，送信先の端末の公開鍵を用いて暗号化し，クエリ応答を送信する．一方，検索クエリを送信する際は，隣接端末を事前に把握していないため，暗号化を行わず，メッセージをブロードキャストする．

データのスコアは，検索条件から何らかのスコアリング関数を用いて算出されるものとする．また，各端末の所有するデータは，救急隊員の所有する通信端末とは異なる医療機器（通信端末とは OS やアプリケーションが全く異なる機器）などで計測され，事前に暗号化されており，クエリ発行端末のみ解読することが可能であるものとする．そのため，攻撃端末が新たにデータを作成したり，データを偽装できないものとする．ただし，データのスコアは応答メッセージに添付されるため，把握することができるものとする．

4.2　攻撃モデル

本稿では，ネットワーク内に攻撃端末が m 台存在することを想定する．攻撃端末は，クエリ発行端末に，攻撃されていることを検知，および自身が攻撃端末であることを特定されないように攻撃を行うものとする．データに添付されているスコアを改ざんした場合，クエリ発行端末で受信したデータと添付されているデータのスコアとの整合性を確認することにより，攻撃端末の存在が検知されてしまうため，スコアの改ざんは行わない．攻撃端末は，隣接端末から受信したクエリ応答に含まれるデータおよび自身の所有するデータの上位 k 個のうち，$\lceil h \cdot k \rceil$ 個（h：データ差替え割合）のデータを自身の所有する別のデータに差し替えて送信する．

さらに，攻撃端末に関する情報をネットワーク内の端末間で共有するため，各端末は攻撃端末を特定した後，その情報を全端末に送信する．この際，攻撃端末は，通常端末による攻撃端末の特定を遅らせるために，通常端末を攻撃端末であると偽って通知する虚偽通知攻撃を行う．この際，闇雲に通常端末のみを攻撃端末であると偽ると，虚偽通知攻撃が容易に判明してし

まうため，攻撃端末は，他の通常端末が特定した情報に便乗して，同じ端末を攻撃端末とする通知メッセージを送信する．これに加えて，通常端末を攻撃端末として偽って送信する．これにより，通常端末による攻撃端末の判定に大きな影響を与えることができる．

以上のように，攻撃端末は，2 種類の攻撃を行うものと想定する．ただし，攻撃端末は常に 2 種類の攻撃を行うのではなく，一方の攻撃のみを行うものや，攻撃を適時切り替えるものも存在する．

5. 提 案 手 法

5.1 手 法 概 要

提案手法では，Top-k 検索を実行する中で攻撃端末を早急に特定するために，各端末が先行研究 [8] を用いて特定した攻撃端末の情報を端末間で共有し，効率的に攻撃端末を判定する．先行研究 [8] の攻撃端末特定手法では，ネットワーク内の各端末は，自身に隣接する攻撃端末を特定する場合が多く，自身に遠い位置に存在する攻撃端末は特定するのが困難な場合が多い．そこで，ネットワーク内で攻撃端末に関する情報を共有するために，攻撃端末を特定した端末は，攻撃端末に関する情報をネットワーク内の他の端末へ送信する．各端末は，一定数の検索クエリを受信後，共有した攻撃端末に関する情報の類似度に基づいてネットワーク内の端末をグルーピングし，各グループ内で攻撃端末候補を通常端末と攻撃端末に分類する．さらに，各グループの判定結果に基いて，最終的な攻撃端末の判定を行う．

5.2 通知メッセージの送信

ネットワーク内の端末が，先行研究 [8] を用いて，クエリを発行し攻撃端末を特定した場合，ネットワーク内の端末に特定した攻撃端末に関する情報をフラッディングする．これにより，端末間で攻撃端末の情報を共有する．以下に，その方法の詳細を示す.

（1） 攻撃端末を特定した端末 M_p は，通知メッセージを全ての隣接端末に送信する．このメッセージには，クエリ識別子 Q_{Num}，自身の識別子 M_p および特定した攻撃端末の識別子リスト $\mathbf{BL_p}$ が添付されている．

（2） 通知メッセージを初めて受信した端末 M_q は，受信した通知メッセージを記録する．さらに，受信したメッセージをコピーし，自身の隣接する全ての端末に送信する．

（3） 再度同じ通知メッセージを受信した端末 M_r は，受信したメッセージを無視する．

5.3 端末のグルーピング

ネットワーク内の端末は，自身に隣接する攻撃端末を特定する場合が多く，自身から遠い位置に存在する攻撃端末を特定するのは困難な場合が多い．そのため，隣接する通常端末同士は同じ端末を攻撃端末として特定する場合が多くなり，攻撃端末が通常端末のことを攻撃端末と偽ると，隣接する通常端末が特定した攻撃端末に関する情報とは異なる可能性が高い．そこで，共有した攻撃端末に関する情報の類似度を基にネットワーク内の端末をグルーピングすることにより，虚偽の情報を効率的に分離して，攻撃端末と通常端末を正確に分類できる可能性がある．この際，各端末が特定した攻撃端末数による影響をなくすため，コサイン類以度を用いて，類以度を計算する．

さらに，グルーピングの結果，通常端末と攻撃端末が混在するグループが存在する可能性があるため，グループ内でクリーニングを行う．具体的には，まず，同じグループに属する端末を攻撃端末と特定している端末が存在する場合，特定された端末をグループから除去する．ここで，攻撃端末が虚偽通知の際に，通常端末との情報の類似度を高くするように，通常端末が特定した攻撃端末に関する情報も $\mathbf{BL}$ に加えた場合，この攻撃端末は通常端末と同じグループに分類される可能性が高い．このような虚偽通知攻撃を行う攻撃端末の影響を小さくするため，グループ内の端末のうち一定数以下の端末からしか特定されていない攻撃端末を特定した端末は，グループから除去する．

以下に，ネットワーク内の端末をグルーピングする方法の詳細を示す.

（1） 端末 M_s は，検索クエリを Num_{Query} 回受信後，ネットワーク内の端末のグルーピングを開始する．M_s は，受信した通知メッセージを攻撃端末を特定した端末（クエリ発行端末）ごとにまとめ，端末ごとの評価値 $\boldsymbol{R_i}(i = 1, 2, ..., n)$ を求める．ここで，評価値 $\boldsymbol{R_i}$ は，端末 M_i が特定した攻撃端末を表し，2 値の n 次元ベクトルで表される．$\boldsymbol{R_i}$ の $j(j = 1, 2, ..., n)$ 成分は，端末 M_i が端末 M_j のことを攻撃端末と特定した場合は 1，特定していない場合は 0 で表される．

（2） 端末 M_s は，特定した攻撃端末に関する情報の類以度を，各端末間に対して求める．端末 M_a と端末 M_b の類以度 $sim(a, b)$ は，評価値 $\boldsymbol{R_i}$ を用いて以下の式で表される．

$$sim(a, b) = \cos(\boldsymbol{a}, \boldsymbol{b}) = \frac{\boldsymbol{R_a} \cdot \boldsymbol{R_b}}{\|\boldsymbol{R_a}\|\|\boldsymbol{R_b}\|} \tag{1}$$

（3） 端末 M_s は，類以度 $sim(a, b)$ が，$sim(a, b) \geqq \theta$ となる場合（しきい値 θ は，システムパラメータ），端末 M_a と M_b を同じグループ G_u とする．このとき，グループ G_u に含まれる全端末を，$\mathbf{M_{G_u}} = \{\mathbf{M_a}, \mathbf{M_b}\}$ とする．一方，複数の端末間の類似度において，$\{\forall a \in G | \ \forall b \in G, sim(a, b) \geqq \theta\}$ かつ $\{\forall x \in N - G | \ \forall a \in G + x, \forall b \in G + x, \exists sim(a, b) < \theta\}$（$N$ はネットワーク内の端末を表す）を満たす場合，G に属する端末を同じグループとする．

（4） 端末 M_s は，端末のグルーピング後，グループ内の攻撃端末をクリーニングする．各グループ G_u（$u = 1, 2, ..., g$, g はグループの総数）において，グループ内の端末 $\mathbf{M_{G_u}}$ が特定したすべての攻撃端末からなる集合 BL_{G_u} にグループ内の端末が含まれる場合，特定した方の端末が虚偽通知攻撃を行った攻撃端末である可能性があるため，その端末をグループから除去する．さらに，$\mathbf{BL_{G_u}}$ 内の各攻撃端末が，それぞれグループ内の端末 $\mathbf{M_{G_u}}$ のうち何台に特定されたかをカウントする．そのカウント数がしきい値 $\rho(= |\mathbf{M_{G_u}}| \cdot \alpha)$（$0 \leqq \alpha \leqq 1$）以下となる端末を攻撃端末と特定した端末 M_t は，グループ G_u から除去する．

端末間の類以度 $sim(a, b)$ を用いたネットワーク内の端末のグルーピングの例を表 1 に示す．表の 1 列目は，クエリを

表 1　各端末が受信した通知メッセージの例
Table 1　Example of notification messages received by each node

クエリ発行端末	特定した攻撃端末
M_1	M_2, M_5
M_2	M_1, M_4
M_4	M_2, M_5
M_6	M_5
M_5	M_1, M_4
M_3	M_5
M_8	M_1, M_2, M_5
M_7	M_5
M_9	M_5, M_8
M_{10}	M_5

表 2　各端末間の特定した攻撃端末の情報の類似度
Table 2　Similarity of the information on identified malicious nodes between each pair of nodes

	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}
M_1	-	0	0.71	1	0	0.71	0.71	0.82	0.5	0.71
M_2	0	-	0	0	1	0	0	0	0	0
M_3	0.71	0	-	0.71	0	1	1	0.58	0.71	1
M_4	1	0	0.71	-	0	0.71	0.71	0.82	0.5	0.71
M_5	0	1	0	0	-	0	0	0	0	0
M_6	0.71	0	1	0.71	0	-	1	0.58	0.71	1
M_7	0.71	0	1	0.71	0	1	-	0.58	0.71	1
M_8	0.5	0	0.71	0.5	0	0.71	0.71	-	0.5	0.71
M_9	0.5	0	0.71	0.5	0	0.71	0.71	0.41	-	0.71
M_{10}	0.71	0	1	0.71	0	1	1	0.82	0.71	-

表 3　攻撃端末の判定の例
Table 3　Example of identified malicious nodes

グループ	グループ内の端末	$\mathbf{Mal_u}$
G_1	$M_1, M_3, M_4, M_6, M_7, M_{10}$	M_5
G_2	M_1, M_4	M_2, M_5
G_3	M_2, M_5	M_1, M_4
G_4	M_3, M_6, M_7, M_{10}	M_5

発行し，通知メッセージを送信した端末 $M_1 \sim M_{10}$ を表し，2 列目は，1 列目のクエリ発行端末が特定した攻撃端末を表す．端末間の類似度を表 2 に示す．この例では，攻撃端末を M_2, M_5, M_8 としている．表 1 および表 2 より，全く同じ端末を特定している端末同士の類以度は 1 となる．しきい値 $\theta = 0.7$ の場合，グループ $G_1 = \{M_1, M_3, M_4, M_6, M_7, M_{10}\}$ とグループ $G_2 = \{M_1, M_4, M_8\}$，グループ $G_3 = \{M_2, M_5\}$，グループ $G_4 = \{M_3, M_6, M_7, M_9, M_{10}\}$ にグルーピングされる．ここで，グループ G_2 内の端末のうち，M_8 は M_1 を攻撃端末と特定しているので，グループ内から M_8 を除外し，$G_2 = \{M_1, M_4\}$ となる．また，$\alpha = 0.2$ の場合，グループ G_4 ではしきい値 $\rho = 1.0$ となり，グループ G_4 内の端末のうち M_9 のみが M_8 を攻撃端末と特定しているため，グループ G_4 から M_9 を除外し，$G_4 = \{M_3, M_6, M_7, M_{10}\}$ となる．

5.4　攻撃端末の判定

ネットワーク内の端末をグルーピングした後，各グループ内の端末が特定している攻撃端末の情報を基に攻撃端末の判定を行う．グループには，(i) 通常端末のみのグループ，(ii) 攻撃端末のみのグループ，(iii) 通常端末と攻撃端末が混在するグループが存在する．通常端末は，通常端末を攻撃端末と特定することはないため，(i) 通常端末のみのグループおよび (iii) 通常端末と攻撃端末が混在するグループでは，グループ内のすべての端末が特定した攻撃端末は攻撃端末であると判断できる．また，(ii) 攻撃端末のみのグループが存在することを考慮し，ある端末を攻撃端末と判定したグループ数がしきい値以下の場合，最終的にその端末を攻撃端末と判断しない．

以下に，ネットワーク内の攻撃端末 $Malicious$ の判定方法の詳細を示す．

（1） 端末のグルーピングを行った端末 M_s は，各グループ G_u（$u = 1, 2, ..., g$）内の全ての端末が攻撃端末と特定した端末を $\mathbf{Mal_u}$ とする．

（2） グループ内の全ての端末が端末 $M_{\mathrm{x}} (M_{\mathrm{x}} \in \mathbf{Mal_u})$ を攻撃端末と特定したグループ数が，しきい値 $\phi (= g \cdot \beta)$ $(0 \leqq \beta \leqq 1)$ 以上の場合，M_{x} を攻撃端末と判定し，$Malicious$ に追加する．さらに，M_x が所属するグループにおいて，グループから M_x を除去する．

（3） 手順（1）および（2）の操作を，新たに $Malicious$ に加わる端末がいなくなるまで繰り返す．

（4） $Malicious$ の端末を最終的な攻撃端末と判定する．

表 3 を用いて，攻撃端末を判定する処理の例を説明する．表の 1 列目はグループ名，2 列目は各グループに含まれるクエリ発行端末を，3 列目は $\mathbf{Mal_u}$ をそれぞれ表す．$\beta = 0.3$ とした場合，しきい値 $\phi = 1.2$ となるため，$\mathbf{Mal_u}$ 内のある端末が 2 グループ以上に含まれ場合，その端末を攻撃端末と判定する．表 3 より，端末 M_5 は $\mathrm{Mal}_1, \mathrm{Mal}_2, \mathrm{Mal}_3$ の 3 グループに含まれており，攻撃端末と判定される．また，G_3 は，攻撃端末と判定された端末 M_5 が G_3 に所属しているため，M_5 を G_3 から除去する．$M_1, M_2, , M_5$ は，それぞれ $\mathrm{Mal}_3, \mathrm{Mal}_2, \mathrm{Mal}_3$ の 1 グループのみに含まれており，攻撃端末と判定されないため，攻撃端末の判定を終了する．

提案手法では，各端末が特定した攻撃端末に関する情報の類以度を基に端末をグルーピングするため，攻撃端末が通常端末を攻撃端末であると偽る虚偽通知攻撃を行なうと，通常端末と攻撃端末が異なるグループとなることが多い．そのため，通常端末の数が攻撃端末の数よりも大幅に大きい一般的な環境では，通常端末のグループ数は攻撃端末のグループ数よりも大幅に大きくなる，その結果，最終的な判定において攻撃端末を含むグループ数が ϕ を超えないため，虚偽通知攻撃の影響を受けない．また，攻撃端末が通常端末との情報の類以度を高くするように，通常端末が特定した攻撃端末に加えて，他の通常端末を攻撃端末と偽ってネットワーク内に通知したとしても，グループ内の他の通常端末は攻撃端末のみを特定しているため，グループ内のすべての端末が特定した端末を攻撃端末と判断する本手法では，その影響を小さく出来る．その結果，攻撃端末を早く特定できる．

6.　シミュレーション評価

本章では，提案手法の性能評価のために行ったシミュレーショ

ン実験の結果を示す．本実験では，ネットワークシミュレータ Qualnet5.2(注1) を用いた．

6.1 シミュレーション環境

500[m]×500[m] の 2 次元平面状の領域に 50 台の端末（M_1,M_2, …,M_{50}）が存在する．各端末はランダムウェイポイント [1] に従い，0.5[m/秒] の速度で移動し，停止時間は 30[秒] とした．各端末は，IEEE802.11b を使用し，伝送速度 11[Mbps]，通信伝搬距離が 100[m] 程度となる送信電力で通信パケットを送信する．各端末は，128[B] のサイズのデータを 50 個もち，ネットワーク内には総数 2,500 個のデータが存在するものとした．30[秒] ごとに，ネットワーク内の端末のうち 1 台がランダムに選ばれ，Top-k 検索クエリを発行する．その際，要求データ数は k とした．ネットワーク内には，データ差替え攻撃と虚偽通知攻撃の両方を行う攻撃端末（MN と表す）および虚偽通知攻撃のみを行う虚偽端末（LN と表す）が，それぞれ m 台および l 台存在するものとする．データ差替え攻撃では，受信したデータのうち $\lceil 0.5k \rceil$ 個のデータを任意に選んで，自身の所有するデータに差し替える．虚偽通知攻撃では，自身が発行する通知メッセージ内の攻撃端末に関する情報を，自身が初めて受信した通知メッセージ内の攻撃端末に関する情報にそのメッセージの発行者を加えたものとする．つまり，基本的に全ての攻撃端末および虚偽端末は，同じ通常端末を攻撃端末として通知メッセージを送信するが，自身は攻撃端末情報に含めない．

比較手法として，端末のグルーピングを行わず多数決を用いる手法を用いる．この手法では，最も多くの端末から特定された攻撃端末を攻撃端末と判定し，この端末が特定した攻撃端末の情報を破棄する．その後，判定した攻撃端末以外の端末の中で，最も多くの端末から特定された攻撃端末を攻撃端末と判定するという操作を，しきい値 $\lambda(= IM_{rec} \cdot \gamma)$ 台（IM_{rec} は通知メッセージを送信した端末数，γ はシステムパラメータ）以上の端末がなくなるまで攻撃端末の判定を繰り返す．

表 4 に，各手法におけるしきい値に関するシステムパラメータを示す．また，表 5 に本実験で用いたパラメータを示す．各パラメータは基本的に定数値をとるが，そのパラメータの影響を調査する際には括弧内の範囲で値を変化させた．

以上のシミュレーション環境において，各端末の初期位置をランダムに決定して配置し，ネットワーク内の端末が Num_{Query} 回のクエリを発行した後，各端末が攻撃端末を判定する試行を 100 回繰り返した際の，以下の評価値を調べる．

- 攻撃端末の特定台数 : 100 回の試行において，ネットワーク内で特定された攻撃端末の平均台数．
- 攻撃端末の誤特定割合 : 100 回の試行において，ネットワーク内で攻撃端末と特定された端末に通常端末が含まれていた割合．

6.2 クエリ発行回数の影響

クエリ発行回数 Num_{Query} を変化させたときの結果を図 2 に示す．この図において，横軸はクエリ発行回数 Num_{Query} を表し，縦軸は，図 2(a) は攻撃端末の特定台数および図 2(b) は攻撃端末の誤特定割合を表す．図 2 中の凡例では，MN - 5 は，MN がネットワーク内に 5 台存在している場合を表しており，MN - 5 + LN - 5 は，MN および LN がそれぞれ 5 台存在することを表す．

図 2(a) の結果より，どちらの手法においてもクエリ発行回数が大きくなるにつれて，攻撃端末の特定台数が増加している．これは，クエリ発行回数が大きくなると，各端末が特定した攻撃端末台数が増加するためである．提案手法では，多数決手法よりも少ないクエリ発行回数で攻撃端末を多く特定できている．提案手法では各端末が特定した攻撃端末に関する情報の類似度を基に端末をグルーピングすることで，攻撃端末が同一のグループに，通常端末は特定した攻撃端末の組合せごとにグループに分類される．その結果，通常端末のグループ数が攻撃端末のグループ数よりも多くなり，通常端末のグループが特定した攻撃端末のみを最終的に攻撃端末と判断できるためである．したがって，提案手法では，攻撃端末に対する特定情報が少ない段階でも多くの攻撃端末を特定できる．また，どちらの手法も，虚偽端末 LN が増加した場合でも攻撃端末の特定台数を維持できている．これは，LN が増加しても，多数決手法では，しきい値台数以上の端末から特定されたもののみを攻撃端末と判断しているためである．また，虚偽端末および攻撃端末は同じ端末を攻撃端末として通知するため，提案手法における特定した攻撃端末に関する情報を基にしたグルーピングでは，攻撃端末および虚偽端末は同じグループに分類される．そのため，LN が増加しても，通常端末のグループの数の方が多くなり，正しく攻撃端末を特定できる．

図 2(b) の結果より，どちらの手法もクエリ発行回数が大きくなるにつれて，誤特定割合が減少している．これは，多数決手法では，多くの端末が攻撃端末を特定することにより，攻撃端末の虚偽通知攻撃の影響が減少したためである．また，提案手法では，各端末が多くの攻撃端末を特定することにより，通常端末のグループ数が増加していき攻撃端末のグループの影響が減少したためである．一方，クエリ発行回数が小さいとき，提案手法では多数決手法よりも誤特定割合が小さい．これは，提案手法では，端末のグルーピングにより，攻撃端末が同一の

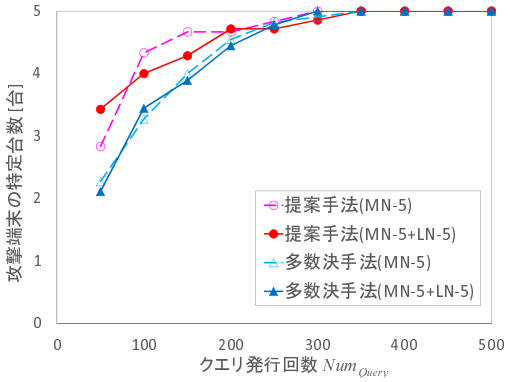
表 4　しきい値に関するシステムパラメータ
Table 4　System parameters regarding thresholds

手法	パラメータ	値
提案手法	θ	0.7
	α	0.2
	β	0.1
多数決手法	γ	0.2

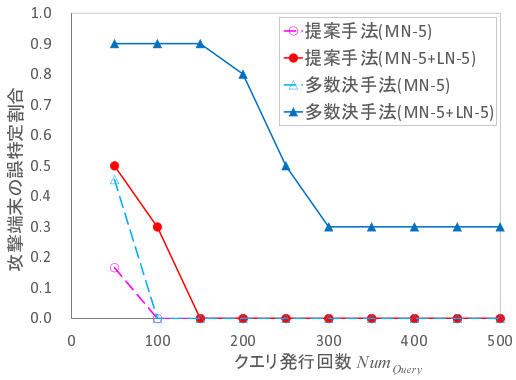
表 5　パラメータ設定
Table 5　Parameter Configuration

パラメータ	意味	値
Num_{Query}	クエリ発行回数	150 (50〜500)
m	攻撃端末台数	5 (1〜10)
k	要求データ数	30（5〜50）

(注1) : Scalable Network Technologies: Creators of Qualnet Network Simulator Software,
< http://www.scalable-networks.com >



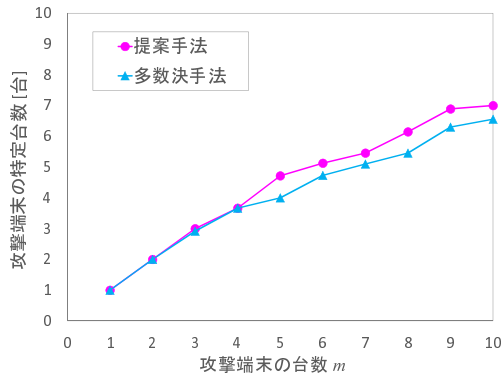
(a) 攻撃端末の特定台数



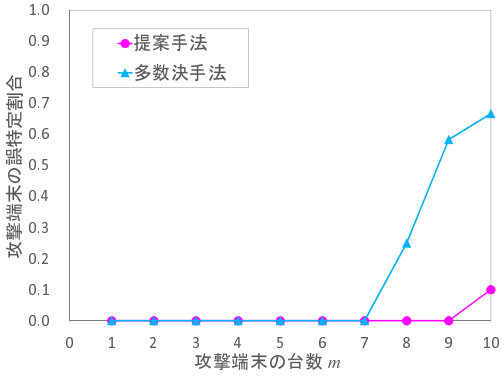
(b) 攻撃端末の誤特定割合

図 2　クエリ発行回数 Num_{Query} の影響

Fig. 2　Effect of Num_{Query}



(a) 攻撃端末の特定台数



(b) 攻撃端末の誤特定割合

図 3　攻撃端末の台数 m の影響

Fig. 3　Effect of m

グループに分類され，虚偽通知攻撃の影響が小さくなり，誤特定割合も小さくなるためである．また，提案手法では，多数決手法と比べて，虚偽端末 LN が増加した場合，攻撃端末の誤特定割合の増加量が小さい．これは，多数決手法では，虚偽通知攻撃を行う端末が 2 倍にると，しきい値台数以上の攻撃端末から特定された通常端末が存在する割合が大きくなる．一方，提案手法では，虚偽端末が増加しても，攻撃端末および虚偽端末が同一のグループに分類されるため，虚偽通知攻撃の影響が小さくなり，攻撃端末の誤特定割合が小さくなる．

6.3　攻撃端末の台数の影響

攻撃端末の台数 m を変化させたときの結果を図 3 に示す．本実験では，虚偽端末は 0 台とした．この図において，横軸は攻撃端末の台数 m を表し，縦軸は，図 3(a) は攻撃端末の特定台数および図 3(b) は攻撃端末の誤特定割合を表す．

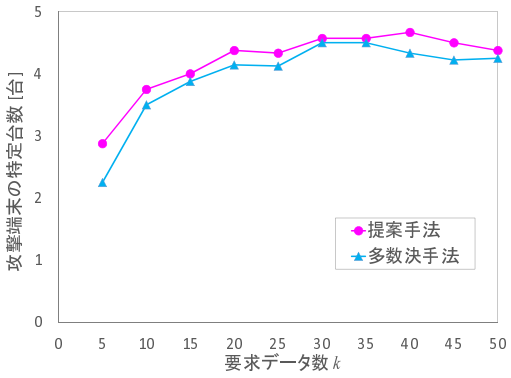
図 3(a) の結果より，提案手法は，攻撃端末の台数が多くなると，多数決手法と比べて，攻撃端末の特定台数も多くなる．提案手法では，攻撃端末の台数が増加すると，通常端末の特定した攻撃端末数が多くなり，通常端末間の情報の類以度が大きくなり，通常端末のグループ数が大きくなる．そのため，提案手法では，攻撃端末をより多く特定できる．

図 3(b) の結果より，多数決手法では攻撃端末の台数が 8 台以上に，提案手法では攻撃端末の台数が 10 台になると，攻撃端末の誤特定割合が増加している．これは，攻撃端末が増加することで，虚偽通知攻撃を受ける機会が増加し，通常端末を誤って攻撃端末と判断してしまう機会が増加するためである．提案手法では，多数決手法に比べて，攻撃端末数が増加しても攻撃端末の誤特定割合が小さい．多数決手法は，各端末が特定した攻撃端末に関する情報を基に，しきい値台数以上の端末が特定した攻撃端末を攻撃端末と判断する．一方，提案手法では，ネットワーク内の端末のグルーピングを行うことで，攻撃端末が同一のグループに含まれる場合が多く，通常端末のグループ数のほうが多くなるため，虚偽通知攻撃の影響が小さくなる．そのため，特定した攻撃端末に通常端末が含まれる機会が小さくなる．

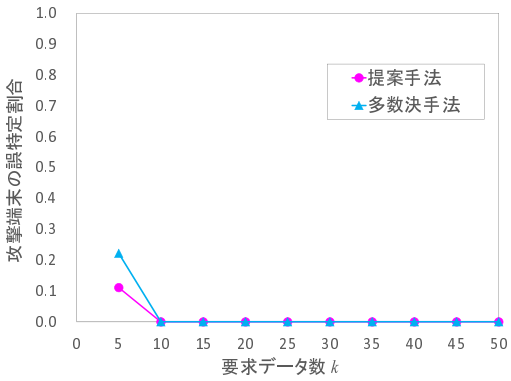
6.4　要求データ数の影響

要求データ数 k を変化させたときの結果を図 4 に示す．本実験では，虚偽端末は 0 台とした．この図において，横軸は要求データ数 k を表し，縦軸は，図 4(a) は攻撃端末の特定台数および図 4(b) は攻撃端末の誤特定割合を表す．

図 4(a) の結果より，どちらの手法においても要求データ数が小さい時に攻撃端末の特定台数が小さくなる．これは，要求データ数が小さいとき，各端末が返信するデータ数が小さく，攻撃端末を判定するのに十分に情報を受信できないため，クエリ発行端末が攻撃端末を特定できる割合が小さくなるからである．また，要求データ数 k が 50 のとき，どちらの手法においても攻撃端末の特定台数が低下している．これは，各端末が返信するデータ数が大きくなり，パケットロスが頻繁に発生するため，クエリ発行端末が攻撃端末を特定できる割合が小さくなり，攻撃端末をを特定するのに十分な情報を受信できないから



(a) 攻撃端末の特定台数



(b) 攻撃端末の誤特定割合

図 4　要求データ数 k の影響

Fig. 4　Effect of k

である．

図 4(b) の結果より，どちらの手法も要求データ数 k が 5 のとき，攻撃端末の誤特定が生じている．要求データ数が小さいとき，クエリ発行端末が攻撃端末を特定できる割合が小さくなり，攻撃端末を判定するのに十分に情報が受信できていない．そのため，虚偽通知攻撃の影響が大きくなり，通常端末を誤って攻撃端末と判定してしまう．ここで，提案手法は，多数決手法に比べて，攻撃端末の誤特定割合が小さくなっている．多数決手法は，各端末の特定した攻撃端末に関する情報を基にしきい値台数以上の端末が特定した攻撃端末を攻撃端末と判断するが，提案手法では，ネットワーク内の端末のグルーピングを行うことで，攻撃端末が同一のグループに分類されるため，攻撃端末の虚偽通知攻撃の影響を小さくできるためである．

7. まとめと今後の課題

本稿では，アドホックネットワーク上の Top-k 検索を対象とし，端末のグルーピングを用いたデータ差替え攻撃端末の特定手法を提案した．提案手法では，ネットワーク内で攻撃端末の情報を共有するために，攻撃端末を特定した端末は，攻撃端末に関する情報を他端末に送信する．共有した攻撃端末に関する情報の類以度に基づいてネットワーク内の端末をグルーピングし，各グループ内で攻撃端末候補を通常端末と攻撃端末に分類する．さらに，各グループの判定結果に基いて，最終的な攻撃端末の判定を行う．提案手法では，攻撃端末が通常端末のことを攻撃端末であると偽って通知メッセージを送信する攻撃（虚偽通知攻撃）を行なっても，通常端末と攻撃端末との間で情報の類似度の差が明確となるため，その攻撃を検出できる場合が多い．さらに，攻撃端末が通常端末との情報の類似度を高くするように，他の通常端末が特定した攻撃端末に関する情報を自身が特定したものと偽って，虚偽の情報と共に通知メッセージに加えたとしても，グループ内の他の通常端末は攻撃端末のみを特定しているため，虚偽通知攻撃を検出できる場合が多い．そのため，虚偽通知攻撃の影響を小さく出き，多くの攻撃端末をより早く特定できる．

本稿の実験では各端末がランダムに動くことを想定しているが，攻撃端末が偏って存在している場合では，提案手法を用いても，攻撃端末を特定するまでに時間がかかってしまうことが考えられる．そのため，今後は，攻撃端末の攻撃頻度や地理的分布に影響を受けにくい攻撃端末特定手法について検討する予定である．さらに，提案手法では，虚偽端末は特定できないため，今後は虚偽端末を特定する手法について検討する予定である．

謝　　辞

本研究の一部は，文部科学省研究費補助金・基盤研究 S(21220002)，および基盤研究 B（24300037）の研究助成によるものである．ここに記して謝意を表す．

文　　献

[1] T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research,” Wireless Communications and Mobile Computing, vol.2, no.5, pp.483–502, 2002.

[2] S. Chen, Y. Zhang, Q. Liu, and J. Feng, “Dealing with Dishonest Recommendation: The Trials in Reputation Management Court,” Ad Hoc Networks, vol.10, no.8, pp.1603–1618, 2012.

[3] P. Dewan and P. Dasgupta,“P2P Reputation Management Using Distributed Identities and Decentralized Recommendation Chains,” IEEE Trans. on Knowledge and Data Engineering, vol. 22, no.7, pp.1000–1013, 2010.

[4] R. Guha, R. Kumar, P. Raghaven, and A. Tomkins, “Propagation of Trust and Dsitrust,” Proc. Int’l Conf. on World Wide Web, pp.403–412, 2004.

[5] S.D. Kamvar, D. Sepander, M.T. Schlosser, and H. Garcia-Molina,“The EigenTrust Algorithm for Reputation Management in P2P Networks,” Proc. Int’l Conf. on World Wide Web, pp.640–651, 2003.

[6] Z. Li and H. Shen,“A Hierarchical Account-aided Reputation Management System for Large-Scale MANETs,” Proc. IEEE Int’l Conf. on Computer Communications, pp.909–917, 2011

[7] M. Srivatsa, L. Xiong, and L. Liu, “TrustGuard: Countering Vulnerabilities in Reputation Management for Decentralized Overlay Networks,” Proc. Int’l Conf. on World Wide Web, pp.422–431, 2005.

[8] 津田琢士, 駒井友香, 佐々木勇和, 原 隆浩, 西尾章治郎,“アドホックネットワークにおけるデータ差替え攻撃を考慮した Top-k 検索手法および攻撃端末特定手法,” マルチメディア，分散，協調とモバイル（DICOMO2013）シンポジウム論文集, pp.569–576, 2013.

[9] A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” IEEE Computer, vol.35, no.20, pp.54–62, 2002.