様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 １８ 日現在

機関番号：１４４０１
研究種目：挑戦的萌芽研究
研究期間：2014～2015
課題番号：２６５４００３５

研究課題名（和文）アドホックネットワークにおける情報検索のためのセキュリティ技術

研究課題名（英文）Security Techniques for Information Retrieval in Ad Hoc Networks

研究代表者
原　隆浩（Hara, Takahiro）

大阪大学・情報科学研究科・教授

研究者番号：２０２９４０４３

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：Top-k検索は、検索条件から計算されるスコアに対して上位k個のデータを収集する検索であり、一般にアドホックネットワークでは検索条件をネットワーク全体に配布し、データを所持する端末が自身が持つ上位k個のデータを返信することで実現される。この際に、ネットワーク内に複数の攻撃端末が存在し、それらが検索結果に入るべきデータを別のデータ（自身がもつスコアの低いデータ）に差し替えると、検索精度が低下してしまう。そのため、本研究ではこのような攻撃により検索程度が低下する問題を抑止するとともに、攻撃者を効率的に同定することを目的として研究開発を実施した。

研究成果の概要（英文）：Top-k search is a typical information retrieval technique, which retrieves data items with k highest scores calculated by s query specified condition. In mobile ad hoc networks (MANETs), top-k search is basically processed as follows: a query issuer floods the entire network with a query with the query condition, and then every mobile node receiving this query sends back data items with k highest scores among its own and received data items. During this process, if multiple malicious nodes exist and these nodes replace received data items which are included in the final search result as its own data items with low scores, the accuracy of the top-k search decreases. To tackle this problem, in this project, we have proposed some approaches for improving the search accuracy against this kind of attacks and also detecting the malicious nodes.

研究分野：データ工学

キーワード：モバイルネットワーク　アドホックネットワーク　情報検索　セキュリティ

## １．研究開始当初の背景

モバイル端末などによって一時的に構築されるアドホックネットワークは、災害時の救助活動などの重要な応用が期待されているが、端末自体が通信パケットを中継するという性質上、悪意のあるユーザからの様々な攻撃にさらされる可能性がある。そのため、国内外の研究コミュニティでは、悪意のあるユーザ（攻撃端末）による通信妨害（パケット廃棄や改ざん）に対抗するための様々なセキュリティ手法が考案されてきた。しかし、実際のアドホックネットワークの応用では、ユーザ同士が単純に通信（音声・ビデオ通話など）を行うことは稀であり、ユーザが所持する情報にアクセスする場合が多い。このような場合、通信自体を攻撃せずに、情報アクセス（検索）の精度を下げる攻撃が可能となり、救助活動などの重要な応用では致命的な問題となる。

そこで研究代表者は、本研究の準備段階として、ユーザが指定した条件に合致する上位 $k$ 個のデータを収集する Top-k 検索を想定し、攻撃端末によるデータ差替え攻撃に対して、検索精度を向上しつつ、攻撃端末を同定する手法を研究してきた。しかし、この先行研究では、簡単化のため、ネットワーク全体で攻撃端末が 1 台のみと想定していた。

## ２．研究の目的

上記の研究背景に基づいて、本研究では、より一般的な環境として、攻撃端末が複数存在する環境を想定し、Top-k 検索などの高度な情報検索に対する攻撃を抑止するとともに、攻撃端末を効率的に同定する機構について研究を推進する。具体的には、複数の経路から返送される検索結果を比較し、攻撃の有無および攻撃者の候補を検出する機構と、他の端末と連係して攻撃者を同定する機構を実現する。特に、ネットワークの構成（トポロジ）や各端末の位置関係に依存して、検出可能な攻撃端末および攻撃端末候補が異なるため、各端末が検出した情報を比較、解析することで、できる限り早急に多数の攻撃端末を発見する機構について研究開発を進める。

## ３．研究の方法

### (1) 複数の攻撃端末によるデータ差替え攻撃に対する Top-k 検索および攻撃端末同定手法

Top-k 検索は、検索条件から計算されるスコアに対して上位 k 個のデータを収集する検索であり、一般にアドホックネットワークでは検索条件をネットワーク全体に配布し、データを所持する端末が自身の持つ上位 $k$ 個のデータを返信することで実現される。この際、返信データを中継した端末は、受信した $k$ 個のデータと自身の持つ上位 $k$ 個のデータの中からスコアが上位の $k$ 個のみを次の端末に返信する。つまり、中継端末において、スコアに基づいたデータの置き換え（フィルタリング）が行われる。攻撃端末は、この検索プロトコルに従わず、スコアに関係なく、自身が所持するデータを検索結果に紛れ込ませる。他の端末は、この攻撃を単純に検出することはできないため、検索要求を発行した端末は、差し替えられたデータを検索結果と判断してしまう。

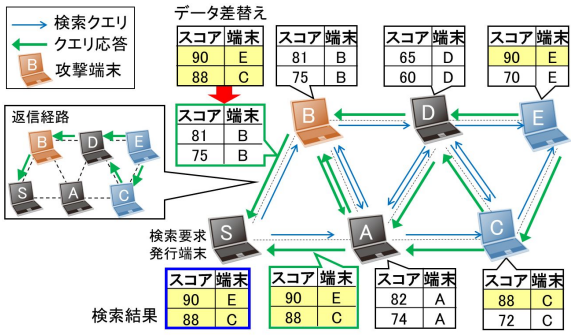



図 1：複数経路を用いた Top-k 検索処理

この攻撃を防ぐために、本研究では、複数の経路を用いて検索結果を返信することを想定する。つまり、攻撃端末によってデータが差し替えられたとしても、他の経路からそのデータが返信されれば、最終的に検索要求を発行した端末で受信可能となる。例え、攻撃端末により差し替えられたデータが発行端末に受信されたとしても、受信データのスコアを比較することにより、正しい検索結果を得ることができる。さらに、返信データに、中継端末の情報を付与することにより、検索結果に入るべきデータを所持する端末を経由しながらも、そのデータが返信されなかった経路（被攻撃経路）を検出でき、その端末を経由した上で正しい検索結果を得られた経路と中継端末の情報を比較することで、攻撃端末（完全に同定できない場合は複数の候補端末）を同定できる。例えば、図 1 では、端末 S は、2 本の経路によって、最もスコアが高い上位 2 個のデータを取得できる。さらに、B からの返信経路に E および C（上位 2 個のデータ保有端末）が含まれているにも関わらず、上位 2 個のデータが含まれていないため攻撃を検知できる。

ここで、検索結果の精度を保証し、攻撃端末を同定するためには、攻撃端末数に対して十分な数の複数経路で検索結果を返信する必要がある。そのため、まず本研究では、攻撃端末数と返信経路数に対する、検索精度および攻撃端末同定率の関係を明らかにする。その後、複数の経路を用いた Top-k 検索手法と、攻撃端末同定手法を具体的に設計する。

考案手法の性能を、詳細なシミュレーション実験により評価する。評価結果に基づいて、考案手法の問題点を検出・分析する。

### (2) 協調処理による攻撃端末の同定

Top-k 検索などの高度検索では、ネットワ

ーク構造や各端末の位置関係に依存して、メッセージを送受信できる相手端末や、中継する検索結果のデータ、攻撃端末との位置関係が大きく異なるため、各端末が検出可能な攻撃端末・候補端末が大きく異なってくる。

そこで本研究では、検出した攻撃端末・候補端末の情報をネットワーク内の端末間で交換し、収集した情報を統合的に判断することで、迅速かつ広範囲に攻撃端末を同定する手法を検討する。この際、複数の攻撃端末が協調して、(潔白な)他端末を攻撃者とする虚偽の情報を流布したとしても正しく攻撃端末を同定できるように、収集した情報間の類似性比較や、クラスタリングなど様々な解析技法を取り入れる。

(3) 認証子を用いたメッセージングによるセキュリティレベルの向上

各モバイル端末が検索処理時に交換するメッセージのセキュリティをさらに強固にし、根本的に攻撃を受けにくくするために認証子を用いた検索手法などを検討する。

## ４．研究成果

(1) 複数の攻撃端末によるデータ差替え攻撃に対する Top-k 検索および攻撃端末同定手法

まず、研究代表者らの先行研究を拡張し、任意の台数(a 台)の隣接端末に Top-k 検索の返信メッセージを送信する手法を考案した。さらに、その性能をシミュレーション実験により検証した。

実験結果から、返信先を 2 台以上にした場合、ネットワークの端末密度が低いときに、検索結果の取得精度を向上できる場合はあるが、特に端末密度が高いときに、通信量の増加に伴うパケットロスなどにより、逆に精度が低下する場合が多いことを確認した。そのため、単純に返信先の端末数を増加することが性能向上につながらないため、精度と通信量のバランスを考慮して、2 台への返信が適切であるとの結論に達した。

(2) 協調処理による攻撃端末の同定

研究項目(1)の成果から Top-k 検索の返信メッセージは 2 台の端末に対して行うことを前提に、複数の端末の協調処理により、より早く攻撃端末を同定する手法を考案した。

① 考案手法の概要

考案手法では、クエリ発行端末が攻撃端末を特定した場合、特定した攻撃端末情報を添付した通知メッセージをネットワーク内にフラッディングし、全端末で共有する。一定数の通知メッセージを受信後、ネットワーク内の各端末は受信した通知メッセージより、ネットワーク内の端末を特定した攻撃端末情報の類以度よりグルーピングし、攻撃端末を判定する。

② 攻撃端末に関する情報の共有

攻撃端末を特定した端末は、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、自身の識別子および特定した攻撃端末の識別子リストが添付される。通知メッセージを初めて受信した端末は、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。これにより、端末間で攻撃端末の情報を共有する。

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する。

④ 最終的な攻撃端末の判定

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。(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。

(3) 認証子を用いたメッセージングによるセキュリティレベルの向上

データ差替え攻撃を根本的に防ぐために、Top-k 検索の返信メッセージに認証子を付与して攻撃端末を特定する手法を考案した。この研究では、各端末は公開鍵と秘密鍵を保有しているものとする。

① 考案手法の概要

考案手法では、各端末が Top-k 検索時に、自身の送信データの情報を認証子として暗号化して添付する。これにより、クエリ発行端末はネットワーク内の端末が送信したデータの情報を把握できる。クエリ発行端末は、受信したクエリ応答中の認証子を確認することで、データ差替え攻撃の検知および攻撃端末の特定が可能である。攻撃端末を特定後、クエリ発行端末は特定した攻撃端末および収集した認証子を添付した通知メッセージをネットワーク内にフラッディングする。通知メッセージを受信した端末は、受信した認証子より、通知された攻撃端末が実際にデータ差替え攻撃を行っていたかを確認する。これにより、通知メッセージが偽造されていないことを保証できるため、虚偽の通知による特定誤りを防ぎつつ、攻撃端末の情報を効果的に共有することができる。

② クエリ応答メッセージの送信

考案手法では、クエリ発行端末が検索クエリをフラッディングした後、ネットワーク内の端末がクエリ応答を開始する。各端末は、受信したデータおよび自身の所有するデータのうちスコアの高い上位 $k$ 個のデータ、応答転送経路、および認証子を添付したクエリ応答を隣接する 2 台の端末に送信する。これにより、攻撃端末を経由しないでデータを送信する機会を増やし、取得精度の維持を図る。送信する認証子には他の端末から受信したクエリ応答中の認証子に加えて、自身の認証子として以下の情報を記録する（図 2）。

- 自身の所有するデータのうち返信データに含まれるデータのスコアと自身の識別子の組。
- 他の端末から受信したデータのうちスコアが上位 $k$ 個であるが、返信データには含まれないデータ（自身が持つデータによって $k$ 位外になったデータ）のスコアとそのデータを保有している端末の識別子の組。
- クエリ応答の送信元（自身）と送信先端末の識別子の組。

このとき、送信する認証子のうち自身の認証子は、自身の秘密鍵で暗号化を行う。これにより、攻撃端末は、他の端末の認証子を復号することは可能であるが、再暗号化できないため、正式な認証子を偽造することはできない。そのため、仮に認証子を偽造しても簡単に検知される。

③ 攻撃端末の特定

クエリ発行端末は全てのクエリ応答を受信後、受信したクエリ応答中の認証子より、攻撃端末によって検索結果に入るデータが差し替えられていないかを確認し、攻撃の検知および攻撃端末の特定を行う。クエリ発行端末が攻撃端末を特定した場合、特定した攻撃端末情報を共有するため、特定した攻撃端末と収集した認証子を添付した通知メッセージをフラッディングする。通知メッセージを受信した端末は、受信した通知メッセージ

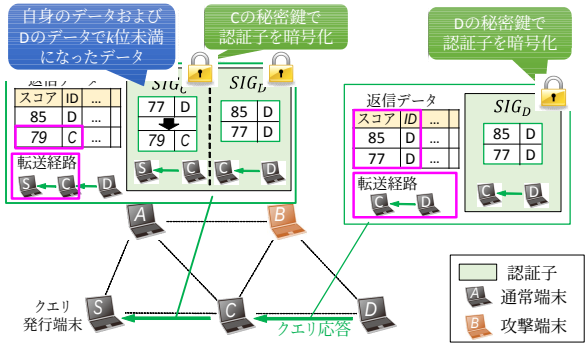



図 2：認証子の作成例

中の認証子を復号し、通知された攻撃端末が実際にデータ差替え攻撃を行っていたかを確認する。

(4) 考案手法の性能評価

考案手法の性能を評価するため、シミュレーション実験を行った。実験では、500[m]×500[m]の領域に 50 台の端末が存在し、そのうち 5 台を攻撃端末とした。研究項目(2)の考案手法では、認証子を付けずにクエリ応答をマルチパスで送信し、端末間の情報共有と端末のグルーピングにより攻撃端末を特定する。この際、クエリ 10 回毎に共有情報に基づいて攻撃端末を決定する。この手法を「比較手法」と表記する。研究項目(3)の考案手法を「提案手法」と表記する。

要求データ数 $k$ を変化させた場合の、全ての攻撃端末を特定するのに要するクエリ発行回数、取得精度（取得すべき上位 $k$ 個のデータのうち実際に取得できた割合）、およびトラヒック（検索処理に要した総バイト数の 1 クエリ当たりの平均）を図 3 に示す。研究項目(3)の考案手法は認証子をクエリ応答に添付しているため、研究項目(2)の考案手法に比べてトラヒックが大きくなるが、取得精度を維持しつつ攻撃端末を早く特定できている。

(5) 研究成果の学術的重要性・インパクト

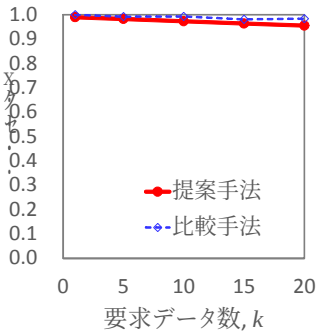
上記で示した本研究の一連の考案手法は、アドホックネットワーク上の Top-k 検索において重大な脅威となるデータ差替え攻撃に対する効果的かつ実用的なアプローチであり、国内外で学術的に高い評価を得ている。

本研究の成果は 5 に示すように、国際論文誌に 1 編、国際会議に 2 編、国内学会に 1 編の論文として公表している。これらの中には、IEEE の著名な論文誌や、分散システムの信頼性分野およびモバイルデータ管理分野で世界的に権威のある国際会議である SRDS と MDM も含まれており、本研究成果の学術的重要性の高さを表している。

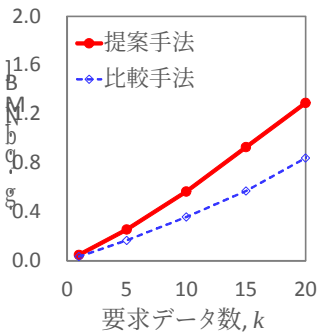
本研究成果は、災害時など通信インフラが破たんしている状況での救助活動などにおいて、情報共有の信頼性および効率を大幅に向上するものであり、社会的な重要性が非常

| | $k = 10$ | $k = 20$ |
|---|---|---|
| 提案手法 | 5.6回 | 6.8回 |
| 比較手法 | 120回 | 130回 |

(a) クエリ発行回数




(b) 取得精度




(c) トラヒック

図 3：考案手法の性能評価

に高い。

以上のように、本研究成果は学術的および社会的にインパクトが大きく、挑戦的萌芽研究として、当初の目的以上の成果を達成したものと考える。

## 5．主な発表論文等

〔雑誌論文〕（計１件）


① Takuji Tsuda, Yuka Komai, Takahiro Hara, Shojiro Nishio, Top-k Query Processing and Malicious Node Identification Based on Node Grouping in MANETs, IEEE Access, Vol.4, pages 993-1007, Mar. 2016. DOI: 10.1109/ACCESS.2016.2541864


〔学会発表〕（計３件）


① Takuji Tsuda 他，Signature-Based Top-K Query Processing Against Data Replacement Attacks in Manets, IEEE International Symposium on Reliable Distributed Systems (IEEE SRDS 2015), pages 130-139, 9 月 30 日，McGill Conference Center (Montreal, QC, Canada).

② 津田 琢士他，アドホックネットワーク上の Top-k 検索における攻撃端末検出のための認証子付き通知メッセージ作成手法，データ工学と情報マネジメントに関するフォーラム，2015 年 3 月 2 日，磐梯熱海ホテル華の湯（福島県郡山市）.

③ Takuji Tsuda 他, Top-k Query Processing and Malicious Node Identification against Data Replacement Attack in MANETs, IEEE International Conference on Mobile Data Management (IEEE MDM 2014), 2014 年 7 月 17 日, The University of Queensland's St. Lucia Campus (Brisbane, Australia).


## 6．研究組織

(1)研究代表者


原　隆浩（HARA, Takahiro）
大阪大学・大学院情報科学研究科・教授
研究者番号：20294043