様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 １７ 日現在

機関番号：２５４０３
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１３００

研究課題名（和文）モバイルアドホックネットワークにおける移動体の経路認証と管理

研究課題名（英文）Path authentication and control of mobile objects in mobile ad hoc networks

研究代表者
双紙　正和（Soshi, Masakazu）

広島市立大学・情報科学研究科・准教授

研究者番号：００２９３１４２

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：近年，IoT（Internet of Things）と呼ばれる環境が普及しつつある．そのような状況では軽量で効率の良い認証手法が求められる．そこで本研究では，我々が提案している，OWCN（One-way Cross Networks）というハッシュ連鎖構成法を応用して，モバイルアドホックネットワークにおける移動体の経路認証および制御のモデルについて研究開発を行う．これにより，モバイルアドホックネットワークにおける軽量で効率のよい認証法の提案のみならず，先進的なユビキタス環境における，認証のフレームワークの確立が期待される．

研究成果の学術的意義や社会的意義
本研究は、ハッシュ連鎖の柔軟な構成法を利用した、認証フレームワークとして期待できる。本研究の手法は、特に、VANET（Vehicular Ad-hoc Networks)や IoT 等における移動体の経路認証および管理に応用できる。具体的には、以下の2点にまとめることができる。(i) 現在（あるいは未来）の経路の認証．たとえば，車の進行方向を認証できるだけでも，衝突回避や渋滞の管理などが可能になる．(ii) 過去の経路の認証．たとえば，工場の自動移動ロボットが，過去のチェックポイントを定められた順番で通過してきたか，あるいは，スタンプラリーなどのエンターテインメントに応用できる．

研究成果の概要（英文）：In recent years, the Internet of Things (IoT) environment is becoming more and more popular. In such an environment, what we need in particular is lightweight and efficient authentication. In this research, we apply our proposed hash chain construction method, OWCN (One-way Cross Networks) and develop a new model for path authentication and control in mobile ad hoc networks. In this work, we propose a lightweight and efficient authentication method for mobile ad hoc networks, and also establish a framework for authentication in advanced ubiquitous environments.

研究分野：セキュリティ

キーワード：セキュリティ　認証　ハッシュ関数　モバイル　アドホックネットワーク　ネットワーク　ハッシュ連鎖　経路認証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１。研究開始当初の背景

近年、移動体間で構築されるネットワークは特に、 MANET (Mobile Ad-hoc NETwork) と呼ばれ、注目されている。 MANET は運用の特性上、送信者から送られてきたデータの信頼性が重要となる。また、アドホックネットワークの一種である MANET は、移動体間の通信を中継することも考えられることから、中継者によるデータの改ざんや送信者へのなりすまし攻撃が考えられる。そうした攻撃に対するセキュリティの確保は、ディジタル署名の利用が有効である。しかし、ディジタル署名は署名の生成、検証の計算に時間がかかり、多数の移動体が往来する場合において一つの移動体に多数の署名が集中する状況では、認証に遅延が発生する。 MANET において，認証の遅延は位置情報などの計算に影響し、致命的な事故に発展する可能性があると考えられる。

ここで、本研究の要素技術として用いられる、ハッシュ関数について述べる。ハッシュ関数とは、(i) 一方向性（ハッシュ関数の値から、入力値を計算することが困難）、および、(ii) 衝突困難性（同じハッシュ値となる二つの異なる入力値を求めることが困難）、を持つような暗号プリミティブである。ハッシュ関数は、量子計算機によっても解読が困難といわれており、いわゆる post-quantum security を確保するための重要な暗号プリミティブの一つとされている。また、ハッシュ関数は、軽量実装が可能であり、かつ、数論をベースにした暗号プリミティブより、はるかに高速に計算できる。さらに、このようなハッシュ関数を応用した技術として、ハッシュ連鎖がある。ハッシュ連鎖とは、ある乱数を初期値とし（以降では「種」と呼ぶ）、ハッシュ関数を繰り返し適用したものである。ハッシュ連鎖は、効率よく一定数の認証値を計算できることから、特に、モバイル端末やセンサー等、計算能力の高くない機器における軽量認証技術として、最も重要なものの一つとなっている。

残念ながら、ハッシュ連鎖を利用した認証法は、ハッシュ値を順に公開（あるいは利用）するといった単純なものがほとんどである。上で述べたように、ハッシュ関数は、次世代環境の VANET や IoT にまさに適した暗号プリミティブであるのに、ハッシュ連鎖を単純に使うだけでは、そのポテンシャルが十分に生かされているか、大きな疑問が残る。

２。研究の目的

こうした観点から、研究代表者の双紙は、ハッシュ連鎖の柔軟な構成法およびそれを応用した認証法について研究開発を行ってきた。本研究は、その認証法をさらに発展・深化させ、モバイルアドホックネットワークにおける移動体の経路手法および管理について、研究開発を行うものである。このために我々は、OWCN (One-way Cross Networks) という、ハッシュ連鎖の柔軟な構成法を提案する。なお、本研究におけるモバイルアドホックネットワークは、各ノードとして、いわゆる携帯端末のみならず、より一般的に、移動可能で無線通信可能な移動体（車など）を対象とする。本研究で提案する手法は、VANET や IoT 等の先進的なユビキタス環境に適用でき、そこでの認証のフレームワークを確立することが期待できる。

３。研究の方法

本研究で提案する経路認証は、センサーなどの安全な位置認証（secure localization や secure positioning と呼ばれる）をより一般的に発展させたものと考えることができる。すなわち、点の認証から、線の認証への拡張と考えられる。

経路認証は、単純に言えば、移動体が進んでいく経路を認証するものである。経路認証には、さまざまな応用が考えられるが、それらは大きく二通りの分類が可能である： (i) 現在（あるいは未来）の経路の認証。たとえば、車の進行方向を認証できるだけでも、衝突回避や渋滞の管理などが可能になる。(ii) 過去の経路の認証。たとえば、工場の自動移動ロボットが、過去のチェックポイントを定められた順番で通過してきたか、あるいは、スタンプラリーなどのエンターテインメントに応用できる。以上、単純に考えただけでも、経路認証の応用分野は広大であることが分かる。しかし、VANET や IoT などの環境に適した、軽量で効率のよい経路認証法については、単純な手法を除いて、十分な研究がなされていない。

そこで我々は、OWCN (One-way Cross Networks) という、ハッシュ連鎖の柔軟な構成法による経路認証法を提案している。OWCN では、経路の方向に対応する複数の種が用意され、それぞれにハッシュ関数を適用した、ハッシュ連鎖によるネットワークが構成される（図 1 参照)。たとえば、図 1 (a) における OWCN は、二つのある種 (s1, s2 とする) に、二つのハッシュ関数(h1, h2 とする) を適用して構成されている。この図で、頂点はハッシュ関数の指数の組を表し、たとえば頂点(1, 1) から (1, 2) への辺によって、$(h1^1(s1), h2^1(s2))$ から $(h1^1(s1), h2^2(s2))$ が構成されることを意味する。そして、移動体は、この OWCN の構成に従って進行方向ごとのハッシュ値を提示し、ハッシュ関数の一方向性を利用することで、経路を認証していく。さらに我々は、OWCN の双対の関係にある、デュアル OWCN なる構成も、同時に提案している。たとえば、図 1 (b)が、図 1 (a)の OWCN に対する、デュアル OWCN である。すなわち、図 1 (a) における頂点 (i, j) について、$(h1^{2-i}(s1), h2^{2-j}(s2))$ なるハッシュ値（認証値）の組を対応させて構成されるハッシュ連鎖のネットワークである。

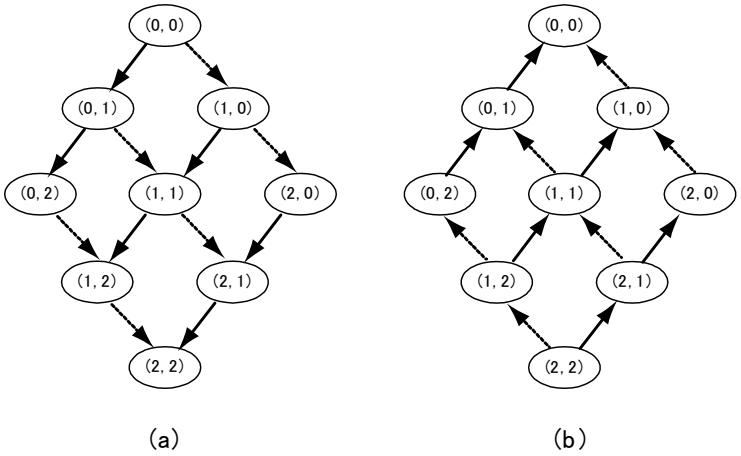

図 1. One-way Cross Networks

４。研究成果

以上の議論から分かるように、OWCN は、種とハッシュ関数の数を任意にして多次元的なネットワークを構成でき、ハッシュ連鎖の真に一般的な構成法になる可能性をもっている。ここで、種を複数使うアイディアは Joye らによって提案されているが、我々の OWCN は、ユビキタス環境に応用可能な一般的なハッシュ連鎖であり、また、図 1(b)のようなデュアル構成が考案されている等、理論応用の面から独創的でかつ重要である。

OWCN による経路認証は、本研究代表者において発表されたが、本研究においてはさらに発展され、デュアル OWCN によるセキュリティの向上や、可能過去経路集合、可能未来経路集合などの新たな概念の提案、さらに、それらによる、より洗練された経路認証が研究された。

本研究の成果の概略は、以下のとおりである。

(1) OWCN を用いた基本的な経路認証方式

一つの移動体について、OWCN を用いた経路認証方式の基本を研究開発した。この方式については、可能過去経路集合、可能未来経路集合などの新しい概念の形式化、デュアル OWCN による経路情報改ざん検知とそのセキュリティや性能について、研究開発を行った。

(2) OWCN を用いた移動体の経路認証及び管理

研究課題 (1) は、OWCN を用いた基本的な経路認証方式の基本的な方式や概念に関する研究開発であった。そこで、それだけの内容では、たとえば実装に至るまでの具体的な処理は難しい。そのため研究課題 (2) では、OWCN を用いた移動体の経路認証及び管理について、より具体的な方式を研究開発した。

ここでまずまず考える必要があるのは、OWCN とデュアル OWCN の違いについてである。移動体の経路認証において、OWCN の初期設定は、一回だけで済む (one-time password の状況を考えると分かりやすい)。一方で、デュアル OWCN については、移動体の進行方向とハッシュ値の増加方向が一致するために、いったんノードを公開すると、それ以降のノードは公開しても意味がない。そこで、原則としては、ノードを公開するごとに、独立したデュアル OWCN を構築する必要が生じる。

デュアル OWCN については、任意の個数のデュアル OWCN を構成できる理想的な状況であれば、可能過去経路集合、可能未来経路集合を適切に組み合わせることで、ハッシュ連鎖によって、任意の経路を表現することができる。しかしながら、公開するノードごとにデュアル OWCN を構築することは、コストが大きい。そこで現実的には、限定された個数のデュアル OWCN を構築することが必要になってくる。しかしそこでは、上で述べたように、移動体の経路を正確に表現することができない。

そこで本研究課題では、このような状況において、OWCN を用いて経路認証を行い手法を研究

開発した。その概要は、以下のとおりである。

まず、移動体の経路 P をハッシュ連鎖で表現する。具体的には、P を、直線経路 L と、経路範囲 A の組み合わせで表現する。いずれも、可能過去経路集合、可能未来経路集合の適切な組み合わせで表現できる。このような経路を、OWCN 経路と呼ぶ。OWCN 経路においては、その差や、攻撃者による改ざん可能経路数などを評価できる。

デュアル OWCN の公開ノードが n 個 (n ≧ 1)の場合の、認証方法の概要を説明する。

1. 移動経路サイズ (M,M) と公開ノードの制限数 n を決定する。
2. 経路をデュアル OWCN の制限数で分割する。
3. 分割された地点まで認証者が進んだとき、認証者が位置するノードを OWCN で公開する。さらに、分割された地点までの経路の中でノードを一点選択する。選択したノードをデュアル OWCN で公開した場合の L, A を計算する。計算した A の値が最も小さいノードをデュアル OWCN で公開する。また、A が同じ値になる場合は、L を比較、L がより大きい方のノードをデュアル OWCN で公開する。
4. 認証者が分割されたノードまで進む度に、3 を繰り返し、OWCN とデュアル OWCN を組み合わせて公開する。
5. 移動経路サイズ (M,M) に到達するまで 3,4, を実行し、終了する。

今後の研究課題としては、複数の移動体の経路認証及び位置などの管理を行う手法を研究開発などが考えられる。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　0件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 平井晨太，双紙正和	４．巻 vol. 119, no. 437, ICSS2019-97
２．論文標題 ハッシュチェーンアグリゲーションを用いた認証方式の拡張	５．発行年 2020年
３．雑誌名 信学技報	６．最初と最後の頁 213-218
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 平井晨太，双紙正和	４．巻 -
２．論文標題 ハッシュチェーン計算によるモデル化	５．発行年 2019年
３．雑誌名 コンピュータセキュリティシンポジウム2019論文集（CSS 2019）	６．最初と最後の頁 1231-1235
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 平井晨太、双紙正和
２．発表標題 IoT認証のためのハッシュチェーンアグリゲーションの改良
３．学会等名 SCIS2019
４．発表年 2018年～2019年

１．発表者名 双紙正和
２．発表標題 ホワイトボックス暗号の改良について
３．学会等名 ICSS2019-3
４．発表年 2018年～2019年

１．発表者名 平井晨太、双紙正和
２．発表標題 ハッシュチェーン計算モデルによる認証
３．学会等名 ICSS2019-3
４．発表年 2018年～2019年

１．発表者名 石橋康介、双紙正和
２．発表標題 One-way cross networksを用いた経路認証フレームワーク
３．学会等名 ICSS2020-33
４．発表年 2020年～2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関