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　元 年　 ６ 月 ２７ 日現在

機関番号：３２６５７
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１４０

研究課題名（和文）故障・攻撃・盗聴に対する耐性を備えた移動無線センサネットワーク構成手法の研究

研究課題名（英文）Wireless Sensor Networks Tolerating Faults, Attacks and Eavesdropping

研究代表者
桧垣　博章（HIGAKI, Hiroaki）

東京電機大学・未来科学部・教授

研究者番号：７０２８７４３１

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：無線センサーノードによる無線マルチホップ配送により観測データを収集する無線センサネットワークでは、中継無線センサノードの故障や悪意のある無線ノードによる攻撃、盗聴に対して耐性を持つことが求められる。本研究課題では、無線マルチホップ配送経路の検出と観測データメッセージ配送の両フェーズにおいて、無線ノードの故障や悪意のある動作によって、不適切な配送経路を検出すること、観測データを破棄、改竄すること、中継無線センサノードの故障を誤って通知することを検出、通知する手法を考案し実装した。さらに、近隣無線センサノードが協調的に観測データを送信することで盗聴を困難にする手法を考案し実装した。

研究成果の学術的意義や社会的意義
多数のセンサが取得する観測データを簡易に収集可能とする無線センサネットワークへの需要は拡大することが予想されるが、多数の無線センサノードで構成されることから故障への耐性は必須である。また、悪意のある無線ノードにより、観測データが破棄、改竄されたり、正常無線センサノードを故障と偽って通知されることで、無線センサネットワークの機能が損なわれることも回避しなければならない。本研究課題の成果は、これらの問題を近隣の無線センサノード間の協調によって解決する新しい手法を考案した点にある。ここでは、特別なハードウェアを付加することなく、制御メッセージの適切な交換のみによって問題解決している点で優れている。

研究成果の概要（英文）：In wireless sensor networks where observation data messages are transmitted along a wireless multi hop transmission route consisting of multiple intermediate wireless sensor nodes, it is required to tolerate faults of intermediate wireless sensor nodes, various attacks and eavesdropping by malicious wireless nodes. Hence, methods for detections of configuration of inadequate wireless multi-hop transmission routes, losses and falsifications of observation data messages, and fake notifications of faults of intermediate wireless sensor nodes are proposed and implemented. In addition, methods for avoidance of eavesdropping by overhearing malicious neighbor wireless nodes by concurrent observation data message transmissions by neighbor sensor nodes are also proposed and implemented.

研究分野：コンピュータネットワーク

キーワード：無線センサネットワーク　耐故障　耐攻撃　耐盗聴　無線マルチホップ通信　プロトコル　協調検出

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

1. 研究開始当初の背景

固定基地局との通信に依存せず、隣接移動無線ノード間の通信を活用することで柔軟で高性能な無線アドホックネットワークを実現する技術が検討、提案、実現されてきた。各移動無線ノードは、消費電力低減の必要性から定められた電力消費で通信可能な隣接移動無線ノードとの通信のみが可能であることを前提とし、移動無線ノードによる中継により送信元移動無線ノードから送信先移動無線ノードへのデータメッセージ配送を実現する。携帯、車載、散布される移動無線ノードを活用できる柔軟性から、構成移動無線ノードの増減や経時的位置変化を前提とする車輌ネットワーク、災害救済ネットワーク、防災/減災ネットワーク、防衛ネットワーク、センサネットワークへの応用が期待されている。

無線アドホックネットワークでは、隣接無線ノード間のデータメッセージ転送が無線通信によって実現されることから、無線信号の衝突、衝突回避のための競合による通信性能低下 (配送遅延の延長、配送成功率の低下) の改善、プロードキャスト送信される無線信号の傍受が容易である一方で計算性能が限られることによる安全性と適用性のトレードオフを考慮した暗号通信手法の検討、中継移動無線ノードの移動による経路の不安定性の問題を改善する多様なルーティング手法、無線通信に要する消費電力の低減手法などが必要となる。しかし、本研究課題で問題にしている耐故障、耐攻撃、耐盗聴性能を備えた移動無線センサネットワークの実現には、従来手法では解決できない多様な問題を含んでいる一方、各移動無線センサノードによる通信が無線信号のブロードキャストを基礎としていることにより解決の可能性を含むものがある。

従来研究では、故障/攻撃移動無線ノードは停止故障モデルに従い、すべての通信を停止することを前提としているが、悪意のある誤メッセージの送信や送信電力を変更することによるデータメッセージの破棄や改竄データメッセージ送信の隠蔽などのより一般的な異常動作への耐性を備えることが求められている。一方、メッセージの送受信を停止した寡黙な盗聴移動無線ノードがデータメッセージ群を取得することを回避する手法が求められている。これまでに暗号化による盗聴防止が主として検討されてきたが、コンピュータの計算能力の向上により傍受されたデータメッセージ群の盗聴可能性が高まってきている問題がある。移動無線センサノードの備える計算性能は限られることから、強力な暗号通信手法の導入は困難である。さらに、多数のセンサノードの保持する内部時計に誤差が含まれるために、各センサノードによる観測データとデータ取得時の内部時計の値の対からなる集合と実際に環境で発生している事象とが整合しない問題など、移動無線センサネットワークにおける広義の故障への耐性も求められている。

2. 研究の目的

移動機能と無線通信機能を備えた多数の移動無線センサノードから構成される移動無線センサネットワークにおいては、移動無線センサノードの故障、悪意ある移動無線ノードによる攻撃、盗聴に対して耐性を持つことが求められる。本研究課題では、従来手法で実現されていた移動無線センサノードの機能停止故障への対処のみならず、意図的なものを含む誤メッセージの送信、送信電力の意図的な操作による攻撃に対して、故障/攻撃移動無線ノードを特定し、除去する手法を実現する。また、寡黙移動無線ノードによる盗聴に対して、複数配送経路の選択による消極的手法、ノイズ信号送出による積極的手法により、センサネットワークアプリケーションを安全に実行する環境を提供する。これらの手法を移動に電力消費を伴わない落下型/漂流型の移動無線センサノードから構成される移動無線センサネットワークに適用する。ここでは、提案手法をより柔軟に実現するために落下/漂流速度を自律的に修正することでネットワークトポロジの変更が可能な移動無線センサノードを開発し、実機への適用によって提案手法の有効性を示す。

3. 研究の方法

研究期間の前半においては、理論的検討を中心としつつ、実機検証のための落下型/漂流型移動無線センサノードの移動速度調節機構の試作と開発を行なう。また、研究期間の後半においては、実証的、実践的検討を中心とする。

理論的検討では、誤データメッセージと誤制御メッセージ (故障通知メッセージ) の送信をともなうビザンチン故障した移動無線センサノードの検出と故障通知手法を検討し、これを実現するための無線マルチホップ配送経路探索 (ルーティング) プロトコルとデータメッセージ配送プロトコルを設計する。また、単一の寡黙盗聴移動無線ノードによるデータメッセージ群の取得を困難とする無線マルチホップ配送経路の構築手法、データメッセージ配送タイミングに合わせて中継無線センサノードの近隣無線センサノードがノイズ無線信号を送信する手法を検討する。誤差を含む時計を搭載した移動無線センサノードからの観測データに対して整合性のある観測時刻を付与する問題については、隣接無線センサノードが共通に観測した事象の観測データを活用する方法を検討する。実証的、実践的検討では、ネットワークシミュレータを用いたシミュレーション実験による性能評価と実機による有効性検証を行なう。

４．研究成果

本研究課題の主な研究成果は、以下の 8 項目である。

(1) 無線マルチホップ配送経路探索における故障/攻撃への耐性

無線センサネットワークを含む無線マルチホップネットワークにおいては、データメッセージの配送経路を決定するルーティングプロトコルの動作において、故障/攻撃無線ノードによる不適切な経路検出への耐性をそなえることが必要である。本研究課題では、隣接無線ノード位置情報からデータメッセージの転送先を決定する GEDIR ルーティングプロトコルを対象として、位置情報を誤/偽広報によるデータメッセージの収集 (ブラックホールノード問題) を解決する手法を考案した. 隣接無線ノードからのデータメッセージ転送を故障/攻撃無線ノードが自身に誘導する誤/偽位置情報を広告しても、各無線ノードがあらかじめ自身の隣接無線ノードが広告した位置情報の集合を広告しておくことにより、誤った/偽った位置情報に従ってデータメッセージが転送されることがほとんど発生しないことを明らかにした。

(2) 無線マルチホップ配送経路の中継無線ノードによる送信電力変更をともなうデータメッセージの破棄と改竄データメッセージ配送への耐性

無線マルチホップ配送経路の中継無線ノードの故障/攻撃によってデータメッセージが破棄、改竄されることを検出する手法としてウォッチドッグ手法が提案されているが、このとき中継無線ノードがデータメッセージの送信電力を変更している場合には検出できない問題がある。本研究課題では、送信電力の変更を加えた場合でも検出可能な協調ウォッチドッグ手法を考案した。ここでは、中継無線ノードが送信電力を変更してデータメッセージの破棄や改竄の隠蔽を試みてもそれを検出可能な近隣無線ノードによる監視を行う。またこのような協調監視無線ノードを各中継無線ノードに対して配置可能な無線マルチホップ配送経路を検出するルーティングプロトコルを考案し実装した。

(3) 無線マルチホップ配送経路の中継無線ノードによる誤/偽故障通知制御メッセージ送信への耐性

無線マルチホップ通信において、データメッセージの破棄や改竄を行う中継無線ノードが検出されたならば、その旨を送信元無線ノードに通知してこの故障/攻撃無線ノードを含まない新たな無線マルチホップ配送経路を検出、構築する。このとき新たな故障/攻撃の問題として、故障/攻撃中継無線ノードが他の正常な中継無線ノードを誤って/偽って故障であると通知することが考えられる。そこで、本研究課題では、同時に複数の中継無線ノードが故障/攻撃しないことを前提として、この誤った/偽った検出通知を行う故障/攻撃中継無線ノードを特定し、このノードによる故障/攻撃の検出を通知する手法を考案した。ここでは(2)と同様に無線マルチホップ配送経路には含まれない近隣無線ノードが協調する拡張協調ウォッチドッグ手法を考案、実装している。

(4) 隣接独立な複数経路を用いた寡黙盗聴移動無線ノードによるデータメッセージ群取得への耐性

無線マルチホップ配送経路の中継無線ノードの無線信号到達範囲へと移動し、これが転送するデータメッセージを傍受する盗聴無線ノードは、この無線ノード自身が無線信号を創出することがない限り検出することができず、配送されるすべてのデータメッセージを取得することが可能である。このような寡黙な盗聴移動無線ノードへの耐性を備えるひとつの手法として、データメッセージ群を分割して複数の経路を用いて配送することが考えられる。本研究課題では、異なる配送経路に含まれる中継無線ノードの無線信号到達範囲が互いに重複しない隣接独立な複数配送経路を検出する経路探索 (ルーティング) プロトコルを考案、実装した。これによって、単一の寡黙盗聴移動無線ノードは高々1 経路を配送するデータメッセージ群しか傍受できないことを保証し、秘密分散通信技術と組み合わせることによって安全性を向上したデータメッセージ群配送を実現した。

(5) ノイズ無線信号の協調的送信によるアドホックネットワークにおける寡黙盗聴移動無線ノードによる盗聴への耐性

(4)のデータメッセージ群配送手法によって、配送するデータメッセージ群の一部のみしか取得されないことが保証されるものの、単一経路を配送されるデータメッセージ群は無防備なまま傍受されることとなる。この問題を解決するために、位置を特定できない寡黙盗聴移動無線ノードによる傍受をより困難とするために、中継無線ノードが次ホップの中継無線ノードにデータメッセージを転送するタイミングに合わせて、送信する中継無線ノードの 1-および 2-ホップ隣接無線ノードの一部がノイズ無線信号を送出することでデータメッセージの傍受を妨害する手法を考案した。ここでは、次ホップ中継無線ノードが転送されるデータメッセージを正しく受信するために、その 1-ホップ隣接無線ノードはノイズ無線信号を送信することはない。無線マルチホップ配送経路の各中継無線ノードに対して、そのデータメッセージ送信時にノイズ無線信号を送出する近隣無線ノードを特定する手法

と、ノイズ無線信号送出タイミングを通知する手法とを考案し実装した。

(6) 協調的観測データ転送による無線センサネットワークにおける寡黙盗聴無線ノードによる盗聴への耐性

(5)により寡黙盗聴移動無線ノードによるデータメッセージの傍受を妨害することが可能になるが、データメッセージを送信する中継無線ノードの近隣でノイズ無線信号を送出する無線ノードには追加の電力消費を要求することとなり、さらに、その隣接無線ノードによるデータメッセージ転送を抑制することとなり、無線マルチホップネットワーク全体のスループットが低下する。また、データメッセージの送信とノイズ無線信号の送信との同期に要するオーバヘッドも必要となる。そこで、無線センサネットワークを対象として、近隣の無線センサノードが送信するデータメッセージが互いに寡黙盗聴移動無線ノードに対してはノイズとして作用する、すなわち、データメッセージ同士の衝突によって傍受を妨害するように各無線センサノードの観測データメッセージ送信タイミングを調整する手法を考案した。多くの無線センサネットワークでは TDMA 方式が用いられ、各無線センサノードは与えられた時間スロットに観測データメッセージを送信することから、時間スロット割り当てを適切に行うことで、所望の衝突を発生させることが可能となる。

(7) 内部時計誤差による環境情報の誤認識を回避するための無線センサネットワークにおける内部時計誤差推定手法

無線センサネットワークでは、各無線センサノードが取得した観測データとその観測時刻をデータメッセージとしてシンクノードへ配送する。観測時刻は各無線センサノードが備える内部時計によって得られるため、これらを同期させることが必要であるが、無線ネットワークでは配送遅延のゆらぎが大きいために内部時計の値を相互に交換する従来手法では高精度の同期が困難である。そこで、複数の共通のイベントを観測した複数の無線センサノードの観測時刻における内部時計の値を比較することで内部時計の差異を検出する手法を考案した。ただし、いずれのイベントが共通に観測したものであるかを確実に特定する方法が存在しないことから、これを推定するヒューリスティックを導入し、その有効性を実験により検証した。

(8) 遠隔測定誤差への耐性を備えた移動センサノード相対位置取得手法

時刻情報に加えて位置情報の不確定さを解消することは、無線センサネットワークにおいて重要な課題であるが、受信電波強度 (RSSI) や伝達遅延など遠隔で測定されるデータに基づいて位置を推定する方法の多くが生じる誤差に十分な耐性を備えないことが指摘されている。本研究課題では、遠隔であっても比較的小さな誤差で抑えることができる角度の測定と直接測定可能な自身の移動距離の計測のみで移動センサノードの相対位置を得ることができる手法を考案した。実験により十分小さな誤差で位置情報を取得できることが確認された。

５．主な発表論文等

〔雑誌論文〕（計 1 件）

1．金持，桧垣，“ 秘密分散通信のための無線マルチホップ配送手法，” 情報処理学会論文誌，vol.57，pp.1554-1564，2016，査読有．

〔学会発表〕（計 7 件）

1. Arao, A. and Higaki, H., “Local Clock Synchronization without Transmission Delay Estimation of Control Messages in Wireless Sensor Networks,” Procedings of the 15th International Conference on Information Technology: New Generation, Springer, pp.175-183, 2018, 査読有.

2. Arao, A. and Higaki, H., “Local Clock Offset and Drift Estimation between Neighbor Wireless Sensor Nodes,” Proceedings of the 18th International Conference on Computational Science and its Applications, Springer, Lecture Notes of Computer Science, vol.20962, pp.163-176, 2018, 査読有.

3. Okuri, M. and Higaki, H., “Concurrent Data Message Transmissions for Interference of Illegal Overhearing in Wireless Sensor Networks,” Proceedings of the 22nd International Conference on Circuits, Systems, Communications and Computers, pp.1-8, 2018, 査読有.

4. Okuri, M. and Higaki, H., “Intentional Collisions for Preventing Illegal Overhearing by

Eavesdropper Node in Wireless Sensor Networks," Proceedings of the 26th International Conference on Software, Telecommunications and Computer Networks, 2018, **査読有**.

5. Higaki, H., "Neighbor-Disjoint Wireless Multihop Transmission Routes for Secret Sharing Communication," Proceedings of the 5th International Conference on Computer Science and Computational Intelligence, 2018, **査読有**.

6. Shimada, I. and Higaki, H., "Secure Wireless Multihop Transmissions by Intentional Collisions with Noise Wireless Signals," Proceedings of the 15th International Conference on Wireless Networks, pp.51-56, 2016, **査読有**.

7. Sota, N. and Higaki, H., "Cooperative Watchdog for Mallicious Failure Notification in Wireless Ad-Hoc Networks," Proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security, pp.1-4, 2016, **査読有**.