科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１０　日現在

機関番号：　３２６１２
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５６０４６５

研究課題名（和文）高効率セキュアモバイルアドホックネットワークに関する研究

研究課題名（英文）Research on High Efficient Secure Mobile Ad-Hoc Networks

研究代表者
笹瀬　巌（SASASE, IWAO）

慶應義塾大学・理工学部・教授

研究者番号：００１８７１３９

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：　モバイルアドホック・センサネットワークでは，マルチホップ通信を行う必要があり，セキュアなルーチングが求められる．また，省電力，リアルタイム性，高信頼性，高スループットが求められる.さらに，センサ位置の推定精度を向上させることも重要である．本研究では，セキュアなモバイルアドホック・センサーネットワークにおけるルーチングとメディアアクセス制御方式について検討を行ない、優れた方式を提案した.

研究成果の概要（英文）：　Since it is necessary to relay a node by using multi-hop communications in mobile ad-hoc and wireless sensor networks, secure routing is required to prevent the effect malicious node which may exist. Moreover, power saving, real-time communication, high reliability, and high throughput are required. Furthermore, it is also important to raise accuracy of the sensor position. We carried out the research on high efficient secure mobile ad-hoc and wireless sensor networks, and proposed some routing and media access control schemes to achieve better performance.

研究分野：　工学

科研費の分科・細目：　電気電子工学　通信・ネットワーク工学

キーワード：　アドホックネットワーク　センサネットワーク　経路選択　クラスタ　セキュアネットワーク　メディアアクセス制御

１．研究開始当初の背景

近年，ユビキタス社会を支える技術として，環境計測，物流管理，構造物監視，健康管理支援などのアプリケーションでは，セキュアなルーングができるモバイルアドホックネットワーク(Mobile Ad-Hoc Network: MAMET)・無線センサネットワーク(Wireless Sensor Network: WSN)が注目されている.MANETやWSNでは，省電力，リアルタイム性，高信頼性，高スループットが求められる.また,セキュリティの確保も重要な課題である．よって，セキュアなMANET・WSNにおける，省電力，リアルタイム性，高信頼性，および，高スループットを満たすルーチングとメディアアクセス制御(Media Access Control: MAC)方式の検討が必須である.

２．研究の目的

本研究では，セキュアなMANET・WSNにおける，省電力，リアルタイム性，高信頼性，および，高スループットを満たすルーチングとMAC方式について検討を行う．本研究における課題と目的を以下に示す.

(1) MANETにおいて，各ノードがいかに正しく振る舞うかを示す指標として信頼度を導入し,その信頼度をもとに通信経路を評価することで悪意あるノードを回避するセキュアルーチング方式が提案されている．しかし,ノード信頼度の値の改ざんやノードのなりすまし問題，また信頼度を他のノードに通知する方式におけるノードの負担や信頼度利用の非効率等の問題がある． そこで本研究では,ネットワークの規模に応じた証明書の発行・失効管理と，MANETにおけるデータ･制御パケットの転送回数を考慮した信頼度および経路信頼度の算出方法について検討を行う.

(2) リアルタイム性を実現するために,位置情報を用いたルーチング方式として，Cluster Based Routing Protocol for Supporting Mobile Sinks (CBRPM)が注目されている．CBRPMは，ネットワークエリアを格子状に区切り,フラッディングの範囲を制限することで,モバイルシンクを発見するための制御パケット数やパケットの送信遅延を低減し，さらに，アクティブ状態のノードをセル内に一つだけ選出し,他ノードをスリープ状態にすることで電力消費効率を高めている．しかしながら，CBRPMでは，送信可能範囲内のすべてのアクティブノードにパケットを送信できないため,ネットワークの両端からシンクまでの送信パケットのリレーノード数やvoid cellを迂回する際のリレーノード数が増大し，パケット到達遅延や消費電力量が増大するという問題がある.そこで本研究では,セルローテーションを導入することにより格子を広い間隔で区切り，さらに，格子の斜め方向にパケットを送信させることによりリレーノード数を低減し，パケット到達遅延および電力消費効率を改善する方式を検討する.

(3) 非同期の受信者始動型 WSN において，ビーコン型の制御パケットを用いて，送受信が行われていないときは端末をスリープ状態に移行させることで省電力化を図る Receiver-Initiated MAC Protocol (RI-MAC)が提案されている．しかし,スリープ時間が固定であるため,トラヒックの変動に対して柔軟性に乏しく，トラフィックが増加した場合,パケットの送受信に時間がかかるという問題がある.そこで，スリープ時間をトラヒックに適応させ柔軟に変化させることにより，遅延特性やスループット特性の改善を図りつつ，低消費電力を維持できる可変Duty-Cycle MACプロトコルを検討する.

３．研究の方法

セキュアなMANET・WSNにおいて，遅延・消費電力・スループット特性の改善を図ることができるルーチング方式とMAC方式を検討し，理論解析および計算機シミュレーションにより，提案方式の有効性を明らかにする.

４．研究成果

(1) Mobile IPv6においてDoS攻撃を考慮した効率的なIPアドレス保持証明
(雑誌論文(1)，学会発表(8))

Voice over IP(VoIP)やストリーミングメディアの普及に伴い,ネット ワークを移動してもセッションを維持できるMobile IPv6(MIPv6)が注目されている．しかし，MIPv6 に対応した移動端末は容易に IP アドレスを偽ることができるため，悪意のある端末が通信を乗っ取る，宛先の存在しないアドレスにパケットを転送する，あるいは通信に関係のない端末にパケットを転送させることができるという問題があった．これまで，ゼロ知識対話証明の 1 つである FFS (Feige-Fiat-Shamir)認証を用いることによって,正当な端末のみが自身のIPアドレスを生成できることを証明する方式が提案されている．この方式では,通信相手が,移動端末が正しく IP アドレスを生成したかを検証するための問題の出題を行い,移動端末はその問題に解答し，通信相手はその解答の正当性を検証している．しかし，この方式では通信相手が正当性の検証を行うため，通信相手の計算資源を浪費させることを目的とした Denial of Service attack (DoS)攻撃に弱いという課題がある．そこで本論文では，検証を合格するのに必要な問題を 2 問にし，1 問目と 2 問目で検証に必要な演算量を変化させることで，1 問目で効率的に DoS

攻撃を行う端末を排除し，正当な端末以外の 検証にかかる計算量を低減する方式を提案した．そして，計算機シミュレーションにより，DoS 攻撃時および正常な端末の検証に必要な乗算剰余演算回数，検証に必要なメモリ量を評価し，提案方式の有効性を示した．

(2) WSN において階段状スリープを用いた非同期受信者始動型 MAC プロトコル
(雑誌論文(2)，学会発表(9))

バッテリ駆動型の WSN において，省電力を達成する非同期受信者始動型 MAC プロトコルでは，複数ノードが同時にパケットを保持した場合のアイドルリスニング時間の増加による，パケット到達率，遅延時間，および，電力効率の劣化が問題になる．本研究では，前ホップのノードよりもスリープ時間を等比級数的に一定割合で短縮していく階段状スリープを用いることで，各ノードのアイドルリスニング時間を低減し，特性向上を図る MAC プロトコルを提案した．提案方式では，スリープ時間が等比級数で与えられるため，各ノードのアイドルリスニング時間の上限を定式化できる．また，シンクはソースからのホップ数を取得できるため，ホップ数の変更にあわせて効率的にスリープ時間を更新できる．計算機シミュレーションを用いた特性評価により，提案方式は，従来方式の RI-MAC と比較して，パケット到達率，遅延時間，および電力効率の特性を改善できることを示した．

(3) WSN におけるセルローテーションを用いたグリッドルーチングプロトコル
(雑誌論文(3)，学会発表(7))

WSN におけるグリッドルーチングプロトコルは，ネット ワークエリアを格子状のセルに区切ることで，動き回るシンクに即座にデータを届ける必要のあるアプリケーションにおいて，パケット到達遅延と制御パケット数を低減することができる．なかでも，Cluster-Based Routing Protocol for supporting Mobile sinks (CBRPM)は，セル内でアクティブ状態となるノードを選択することで，経路選択の効率を高め消費電力量を低減する．しかし，この方式はセルを細かく区切るため，シンクまでのリレーノード数が増大し遅延が大きくなる問題がある，本研究では，セルを複数のサブセルに分割することで，アクティブ状態となるノードの存在範囲を限定し，アクティブ状態のノードを巡回させるセルローテーションを導入することにより，セルをより広い間隔で区切ることが可能となる方式を提案した．提案方式では，セルを２分割，４分割，６分割した場合のセル間隔の拡大を試みた．セル間隔の拡大により，アクティブノードを各セルに配置した状態でパケット送信におけるリレーノード数が低減し，パケット到達遅延および電力消費効率が改善できる．計算機シミュレーションによる特性評価を行い，各提案方式が CBRPM よりも，パケット到達遅延と消費電力量を低減できることを示した．

(4) ノードにおける複数の QoS パラメータに基づいたゲートウェイ発見アルゴリズム
(雑誌論文(4),学会発表(5))

MANET および既存のネットワークを相互接続するために，残存電力，速度，ノードのホップ数などの複数のサービス品質(Quality of Service: QoS)メトリックを考慮した最適ゲートウェイ選択法を提案した．提案方式では，最適なゲートウェイノードを選択するために，Simple Additive Weighting(SAW)を用いて複数メトリックを考慮した各ノードの重みを算出し，各ノードのうち最大の重みを持つノードを最適ゲートウェイとする．計算機シミュレーションによって特性評価を行った結果，提案方式は，ネットワーク全体のスループット特性を改善できることを示した．また，MANET におけるノードが移動した場合，地面に近い場合，到来角度が変化した場合などの受信電界強度などの受信変動の影響を，実験により測定しデータ解析を行った．

(5) コグニティブ無線環境下の MANET におけるホップ数最小化マルチホップ協調ルーチング
(雑誌論文(5)，学会発表(2),(12))

ノードがクラスタ化された MANET において，１次利用者と２次利用者が同じ周波数を利用するコグニティブ無線環境下において，ホップ距離の X 軸投影の距離を拡張し，ホップ数を最小化するマルチホップルートを検索するマルチホップ協調ルーチングを提案した．最後のホップを除いて，各ホップのコグニティブリレーとコグニティブ受信機は，次の手順で選択される．まず，コグニティブ送信機から最寄りのコグニティブノードをコグニティブリレーとして選択し，コグニティブ宛先ノードをコグニティブ受信機として設定する．そして，もしこの選択されたコグニティブリレーを用いることが QoS 要求を満たさなければ，QoS 要求を満たすコグニティブ受信機候補から，コグニティブリレーのＸ座標の差が最大となるコグニティブノードをコグニティブ受信機として選択する．最後のホップでは，コグニティブリレーが使用可能な場合は協調通信が行われ，使用不可能な場合は直接通信が行われる．計算機シミュレーションにより，提案方式は，従来方式と比較して，平均ホップ数を削減し，平均エンドツーエンドの信頼性，平均エンドツーエンドのスループットおよび所要平均送信電力特性が，優れていることを示した．

(6) DDoS 攻撃に対して排他的論理和と確率的

Marking 方式を用いてルータへの負荷分散を実現する IP Traceback
(雑誌論文(6),学会発表(11))

DoS 攻撃や Distributed DoS(DDoS)攻撃に対し，その発信元を特定する IP トレースバックは重要な技術である．これまで，マーキング方式やロギング方式が個別に提案されてきた．しかし，マーキング方式ではトレースバックのために大量の攻撃パケットの回収が必要であるという課題があり，またロギング方式では全ての通過パケットのハッシュ値を保持するためルータへの負荷が増大するという課題がある．また，マーキングとロギングを交互に行うことでロギング回数を従来と比較し半分に低減できる HIT(Hybrid IP Traceback) 方式が提案されているが，全ての通過パケットに対して処理が必要，DDoS 攻撃において被害ホスト近傍のルータへ大きな負荷が大きいといった課題がある．そこで本論文では，DDoS 攻撃に対するトレースバックにおいて，95% 以上の高いトレースバック成功率を達成しつつルータへの負荷を低減・分散するために，排他的論理和と確率的パケットマーキングを用いたトレースバック方式を提案した．提案方式では，排他的論理和を用いることで 2 つのルータの ID を 1 つにまとめることができ，ロギングの回数を低減することが可能となる．また， DDoS 攻撃において攻撃パケットは大量に送信されてくるという特徴と被害ホスト近傍に攻撃パケットが集中するということを考慮して，全ての通過パケットではなく確率的に選択したパケットに対して 1 度のみ処理を行う．これにより，ルータへの負荷を低減することが可能となる．計算機シミュレーションにより各方式におけるトレースバック成功率とパケット処理率，またパケット処理回数の評価を行い，高いトレースバック成功率を達成しつつルータへの負荷を低減・分散可能な提案方式の有効性を示した．

(7) 教師無し Random Forests を用いた迷惑電話発信者判別法 (学会発表(1))

IP 電話の普及に伴い，販売促進および宣伝といった迷惑電話の出現が問題視されている．着信側は電話に応答して初めてその電話が迷惑電話であるかを判定できるため，迷惑電話を着信前に判定することは，事前に内容を確認できる E メールのスパム判定より困難である．これまで，通話頻度，平均通話時間などの特徴量を用いて，迷惑電話を発信するアカウントを判別する方式が検討されてきた．しかしながら，迷惑電話発信者は複数アカウントを用いることにより，これらの判定方式を用いた場合の判定精度を低減できる．これは，従来手法では，いずれも単一の特徴量毎に判定を行っているため，各特徴量の閾値の設定が困難になるからである．そこで本論文では，多くのユーザが 1 つの Session Initiation Protocol (SIP)サーバを利用することに着目し，教師なし Random Forests に複数の特徴量を入力し，各ユーザの通話の特徴に関する類似度を基に迷惑電話を発信するアカウントを分類する方式を提案した．提案方法では，教師なし Random Forests を用い，複数の特徴量を用いて各ユーザ間の類似度から分類を行うことで，発信の特性が異なる迷惑電話発信者を，事前学習なしで分類することが可能となる．また，迷惑電話発信者が発信する相手は通話毎に異なり，その通話先から電話が掛け返される割合が低いことに着目し，これらの割合を顕著に表す特徴量を 2 つ提案する．実際の通話記録およびコンピュータによって生成された通話データを用い，提案方式の有効性を示した．

(8) クラスタリングを用いた WSN における中継機能分離方式 (学会発表(3))

クラスタリングを用いた WSN では，ネットワーク全体をクラスタに分割し，各クラスタの代表(Cluster Head: CH) が他クラスタにデータを中継することにより衝突確率を低減する．本論文では，CH はデータ収集だけでなく，中継でも多くの電力を消費していることに着目し，中継を行う CH がルータノード(R ノード) を選出し，R ノードが中継を行う方式を提案した．この方式では，中継を行う CH の消費電力を低減できるため，データ収集期間中に CH の電力が尽きる回数を低減でき，データ受信成功率が低下する時間を延長できる．計算機シミュレーションにより，提案方式は，ある時間までの生存ノード数，およびシンクのデータ受信成功率を向上できることを示した．

(9) WSN における冗長な位置推定パケットを低減する省電力位置推定
(学会発表(4))

WSN において，隣接センサノード間の距離，およびセンサノードの位置推定誤差を考慮することで位置推定誤差を従来と同程度に保ちつつ，冗長な位置推定パケット数を低減する省電力位置推定法を提案した．提案方式では，面積重複率に基づいた閾値を設定し，各センサノードは自身との距離が閾値以下の隣接センサノードが先に位置推定パケットを送信した場合に，位置推定パケットの送信を抑制することにより，類似した位置推定パケットの送信数を低減する．さらに，各センサノードに最大位置推定誤差に比例したバックオフを割り当てることで，最大位置推定誤差が大きいセンサノードは，自身よりも最大位置推定誤差の小さい隣接ノードが近くに存在する場合に位置推定パケットの送信を抑制することにより，

位置推定パケットの送信数を低減する．計算機シミュレーションにより，従来方式，および提案方式における位置推定パケットの送信数，位置推定誤差，および消費電力を評価し，提案方式は，従来方式と比較して，位置推定誤差を同程度に低く保ちつつ，冗長な位置推定パケット数を低減し，消費電力を低減できることを示した．

(10) 協調通信を用いたMANETにおけるリレー選択およびMAC方式 (学会発表(6))

協調通信を用いたMANETにおいて，リレー候補ノードをグループ化して時間的に分散し，リレー選択に参加できる確率と再参加率を変化させることにより，高いパケット到達率と短競合時間が達成できるリレー選択およびMAC方式を提案した．提案方式では，受信失敗率の値をもとにリレーノード候補を複数のグループに分割し，グループごとに割り当てられたスロット内で競争を行い，さらに受信失敗率が低いノードの競争への再参加を可能にすることで，応答パケット数の低減と受信失敗率が低いリレーノードの選択を可能にし，空白スロットの有効利用を図る．特性評価により，提案方式は，従来方式と比較して，受信失敗率が低いリレーノードをより選択可能であることを示した．

(11) WSNにおいてホップ数を低減することで省電力化を図るDuty Cycle MACプロトコル
(学会発表(10))

Light Weight energy efficiency Media Access Control (LWMAC)は，WSNにおいて，データを送信する際に次ホップノードをあらかじめ指定せず，最も早くアクティブになるノードを次ホップノードとすることで，送受信タイミングを合わせるプリアンブルを短縮し，消費電力を低減することができる非同期型のduty cycle MACプロトコルである．しかし，LWMACでは次ホップノードまでの距離を考慮していないため，送信ノードがすぐ近くのノードを次ホップ先に選択し，ホップ数が増加してしまう可能性があり，消費電力を低減することができない．本論文では，LWMACのプリアンブルの長さを変えずに，プリアンブル送信中に次ホップノードの候補となるノードが2個以上アクティブになる場合に，シンクノードに近いノードを次ホップノードとして選択することで，シンクノードまでの平均ホップ数を低減し，省電力化を図るMACプロトコルを提案した．計算機シミュレーションにより，提案方式は，従来方式と比較して，シンクノードまでの平均ホップ数を低減し，ノードの消費電力を低減できることを示した．また，P-MACのduty cycle中に予約フレームを導入するプロトコルを提案し，フレームの予約により，Request-to-Send/Clear-to-Send (RTS/CTS)の送信回数およびアイドルリスニングの時間と平均消費電力を低減できることを．計算機シミュレーションにより示した．

５．主な発表論文等

(研究代表者には下線)

〔雑誌論文〕(計 6件)「すべて査読有」

(1) 豊田健太郎, 笹瀬巌, ″FFS認証においてチャレンジの分割により検証に必要な乗算回数を低減する手法の検討,″ 情報処理学会論文誌, Vol.55, No.5, pp.1518-1529, 2014年5月.

(2) Takahiro Wada, I-Te Lin and Iwao Sasase, “Asynchronous receiver - initiated MAC protocol exploiting stair-like sleep in wireless sensor networks,” IEICE Transactions on Communications, Vol.E96-B, No.1, pp.119-126, January 2013.

(3) Hidetoshi Kajikawa, I-Te Lin and Iwao Sasase, “Grid-based routing protocol with cell division and rotation in wireless sensor networks,” IEICE Communications Express (ComEX), Vol.1, No.1, pp.1-6, September 2012.

(4) Safdar H.Bouk, Iwao Sasase, Syed Hassan Ahmad and Nadeen Javaid, “Gateway discovery algorithm based on multiple QoS path parameters between mobile node and gateway node,” Journal of Communications and Networks, KICS, Vol.14, No.4, pp.434-442, August 2012.

(5) I-Te Lin and Iwao Sasase, “Primary traffic based cooperative multihop relaying with preliminary farthest relay selection in cognitive radio ad hoc networks,” IEICE Transactions on Communications, Vol.E95-B, No.8, pp.2586-2599, August 2012.

(6) 井上慎一郎, 石井方邦, 笹瀬巌, “DDoS攻撃に対し排他的論理和と確率的Marking方式を用いることでルータへの負荷分散を実現するIP Traceback,” 情報処理学会論文誌, Vol.53, No.2, pp.795-804, 2012年2月.

〔学会発表〕(計 32件)

(1) Kentaroh Toyoda and Iwao Sasase, “SPIT callers detection with unsupervised random forests classifier,” 2013 IEEE International Conference on Communications - Communication and Information Systems Security Symposium (ICC'13 CISS), June 11th, 2013, Budapest, Hungary.

(2) I-Te Lin, Mio Sekiya and Iwao Sasase, “Cooperative MAC protocol with

distributed relay selection using group - based probabilistic contention," 18th Asia - Pacific Conference on Communications (APCC'12), October 16th, 2012, Jeju Island, Korea.

(3) Shinichiro Hara, Tatsuya Koizumi and Iwao Sasase, "Load balanced cluster - based WSNs by separating relay function from cluster heads," 2012 Triangle Symposium on Advanced ICT (TriSAI' 12), September 19th, 2012, Tokyo, Japan.

(4) Shinji Kano, Tatsuya Koizumi and Iwao Sasase, "Power saving localization by considering node's distance and localization error for reducing redundant packets in mobile WSNs," 2012 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'12), September 10th, 2012, Sydney, Australia.

(5) Nadeem Javaid, Ayesha Bibi, Akmal Javaid, Safdar H. Bouk and Iwao Sasase, "Modeling enhancements in DSR, FSR, OLSR under mobility and scalability constraints in VANETs," 3rd IEEE International Workshop on Smart Communications in Network Technologies, 2012 IEEE International Conference on Communications (ICC'12), June 11th, 2012, Ottawa, Canada.

(6) I-Te Lin and Iwao Sasase, "A primary traffic based multihop routing algorithm using cooperative transmission in cognitive radio ad hoc networks," 2nd International Workshop on Densely Connected Networks, IEEE 6th Consumer Communications and Networking Conference (CCNC'2012), January 14th, 2012, Las Vegas, USA.

(7) Hidetoshi Kajikawa, I-Te Lin and Iwao Sasase, "Grid-based routing protocol using cell rotation to reduce packets latency and energy consumption in wireless sensor networks," 3rd International Research Student Workshop, IEEE 6th Consumer Communications and Networking Conference (CCNC'2012), January 14th, 2012, Las Vegas, USA.

(8) Kentaroh Toyoda, Yuta Kamiguchi, Shinichiro Inoue and Iwao Sasase, "Efficient solution to decrease the effect of DoS attack against IP address ownership proof in mobile IPv6," 2011 IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'11), September 14th, 2011, Toronto, Canada.

(9) Takahiro Wada I-Te Lin and Iwao Sasase, "Asynchronous receiver - initiated MAC protocol with the stair-like sleep in wireless sensor networks," 2011 IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'11), September 13th, 2011, Toronto, Canada.

(10) Tatsuya Koizumi, Shinji Kano and Iwao Sasase, "A duty cycle MAC protocol with energy consumption reduction by decreasing the number of hops in wireless sensor networks," 8th IEEE Asia Pacific Wireless Communication Symposium, August 23th, 2011, Singapore.

(11) Shinichiro Inoue, Shinji Kano, Masakuni Ishii and Iwao Sasase, "A load-distributed IP traceback by using exclusive-OR and probabilistic packet marking for DDoS attacks," 8th IEEE Asia Pacific Wireless Communication Symposium, August 24th, 2011, Singapore.

(12) I-Te Lin and Iwao Sasase, "A multihop cooperative routing algorithm for minimizing the number of hops in spectrum sharing networks," 6th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom' 11), June 3rd, 2011, Osaka, Japan,

その他 20 件

〔図書〕(計 0 件)
〔産業財産権〕
○出願状況 (計 0 件)
○取得状況 (計 0 件)
〔その他〕
笹瀬研究室ホームページ
http://www.sasase.ics.keio.ac.jp

６．研究組織

(1)研究代表者
笹瀬 巌 (SASASE IWAO)
慶應義塾大学・理工学部・教授
研究者番号：00187139

(2)研究分担者 なし
(3)連携研究者 なし