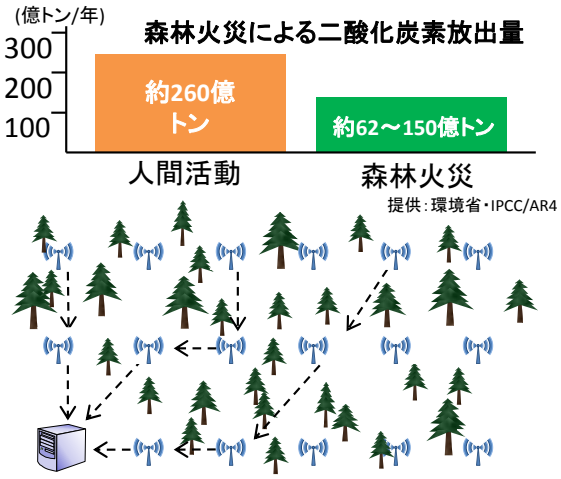
ワイヤレスセンサネットワーク

火災検知データの優先度を考慮した森林火災監視システム

情報工学科 笹瀬研究室 古閑　卓磨(koga@sasase.ics.keio.ac.jp)

研究背景

地球温暖化の一因である森林火災の無線センサ端末による検知が期待されています．また，消火の際は，火災検知だけでなく森林火災の広がりを把握することも重要となっています．

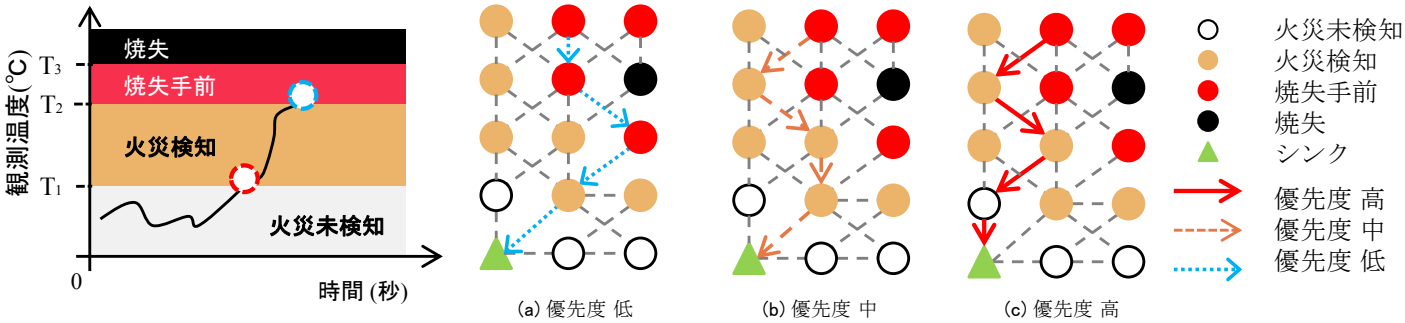


従来方式

焼失しないセンサ端末の代わりに，火災を検知したセンサ端末が焼失前に，データを中継することで，より長く森林火災の様子を把握することが出来ます．しかし，**火災発生後は複数のノードが火災を検知しデータ数が急増するため，新たに火災を検知した情報がデータ衝突により損失してしまい，森林火災の様子把握が困難です．**

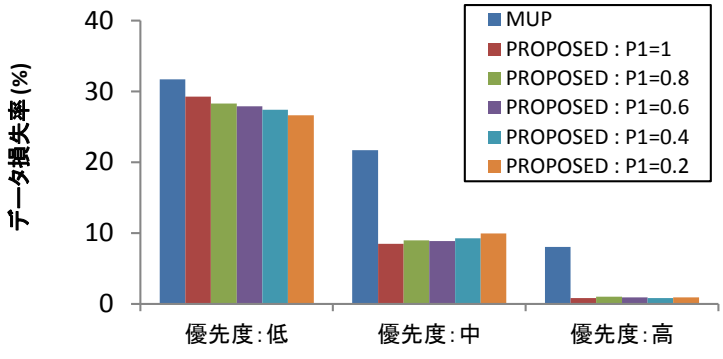
提案方式　森林火災の様子把握に必要なデータの到着率向上

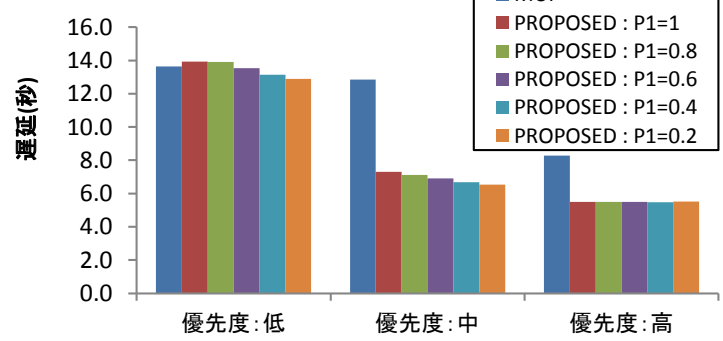
火災検知直後および焼失直前のデータを高優先度に指定．
また各端末では，高優先度のデータを他のデータより先に送信し，焼失する可能性の低い端末を中継．



特性評価

提案方式が，森林火災の様子把握に必要なデータの損失率および遅延を評価しました．





結論

本研究では，森林火災検知データに優先度を不可し，優先度に応じたセンサを中継する方式を提案しました．

本シミュレーション環境において，火災の様子把握に必要なデータを低損失率かつ低遅延で収集可能であることを示しました．

本研究に関する業績

[1] 古閑卓磨，原進一郎，豊田健太郎，笹瀬巌，“火災検知データの優先度を考慮した経路選択を用いた無線センサ森林火災監視システム，”電子情報通信学会通信方式研究会，信学技報，vol. 113，no. 295，CS2013-58，pp. 105-110，2013年11月．

[2] Takuma Koga, Shinichiro Hara, Kentaroh Toyoda and Iwao Sasase, “Priority Based Routing for Forest Fire Monitoring in Wireless Sensor Network,” in Proceeding of International Conference on IEICE Information and Communication Technology Forum, Poznan, Poland, May 2014.

[3] Takuma Koga, Kentaroh Toyoda and Iwao Sasase, “Priority Based Routing for Forest Fire Monitoring in Wireless Sensor Network,” Journal of Telecommunications and Information Technology, No.3, pp.90-97, Sept. 2014.

プライバシー保護

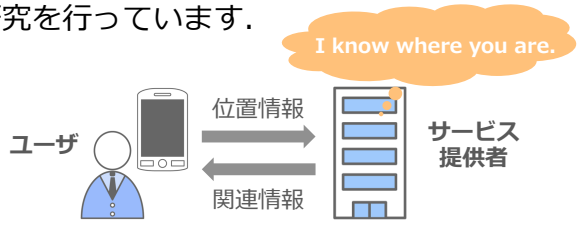
準同型暗号を用いた低コストな秘匿型位置情報検索

情報工学科 笹瀬研究室 宇都宮 靖人

研究背景

モバイル端末の普及により，位置情報検索サービスが活発に利用されています．しかし，ユーザの位置情報はセンシティブな情報であり，適切なプライバシ保護技術が必要となります．

そこで笹瀬研究室では，ユーザのプライバシを侵害しない，安心できる位置情報検索方式についての研究を行っています．



従来研究

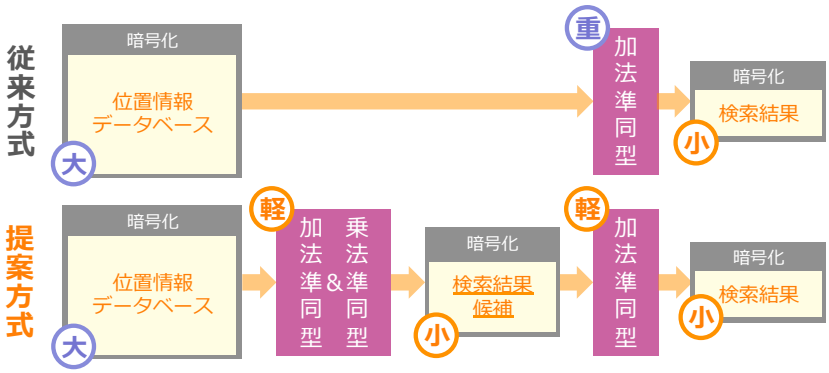
加法準同型性を有する暗号を用いることで，ユーザの現在地をサーバに直接伝えることなく，近隣の位置情報を検索できる方式が提案されています．しかし，この方式はサーバ上での**計算コストが高い**ため，モバイル端末向けのサービスとしては，リアルタイム性に欠けます．

Tip: 加法準同型性と乗法準同型性

暗号化されたデータを復号することなく，演算にそのまま利用できる特性を準同型性といいます．暗号化したまま加算できることを加法準同型性，乗算できることを乗法準同型性といい，両方の特性を持つ暗号は特に完全準同型暗号と呼ばれます．

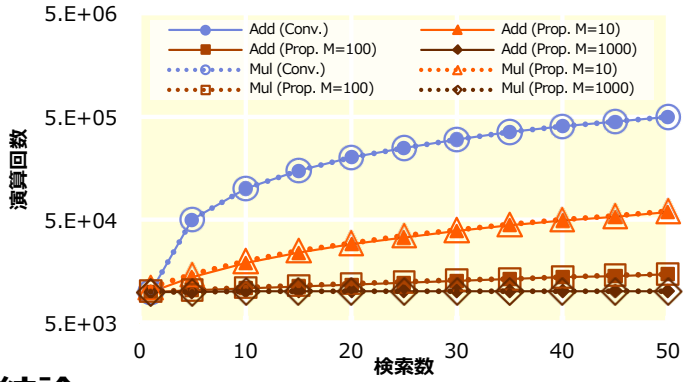
提案方式

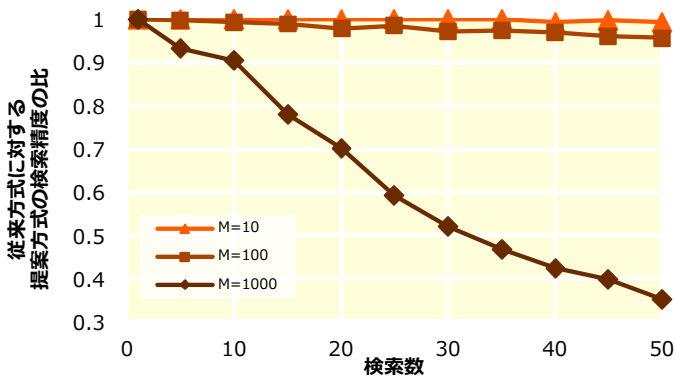
サーバのデータベース上にある，検索に不要な情報を除去する処理を事前に行うことで，従来方式における余分な計算をカットします．この処理を実現するために，加法準同型性の他に，乗法準同型性を有する暗号方式を使用しています．具体的には，位置情報をいくつかのグループに分け，検索結果の候補となるグループ以外を暗号化したまま削除します．



特性評価

実世界にある10,000拠点の位置情報データを用いて，提案方式の計算量と検索精度を評価しました．





結論

加法準同型性に加えて乗法準同型性を用いることで，サーバ側の計算コストを低減する秘匿型位置情報検索方式を提案しました．シミュレーション評価により，従来方式の**検索精度が5%低下**することを許容することで，**計算コストを97%削減**できることを示しました．

本研究に関する業績

[1] 宇都宮靖人, 豊田健太郎, 笹瀬巌, “近傍ロケーションテーブルの分割によりサーバ側の計算量を低減するプライバシ保護k-Points-of-Interest検索手法,” コンピュータセキュリティシンポジウム2014論文集, Vol. 2014, No. 2, pp. 1057-1064, 2014年10月.

WSANsにおける常時アクタ間接続を保証した移動型ネットワーク再形成手法

Yuya Tamura tamura@sasase.ics.keio.ac.jp

研究背景

センサネットワークにアクタと呼ばれる移動可能な多機能ノードを組み合わせるWSANsが近年注目されています．アクタはお互いにネットワークを形成し，協調して行動を起こします．

あるアクタに障害が発生した場合，他のアクタは移動を行うことによってネットワークを再形成する必要があります．

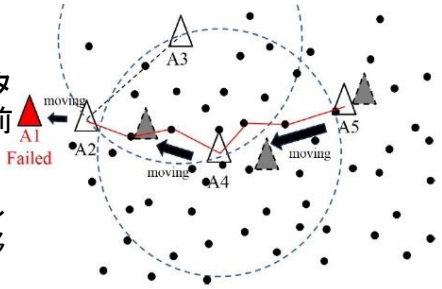
従来方式

アクタが移動する前にパスを形成し，隣人との接続を維持したままネットワークを再形成．しかし，この手法は限られたアクタのみがパスを形成するため，アクタが多い場合，他のアクタはパスを形成しないため隣人と通信不可．

提案方式

・移動する全てのアクタが隣人と再形成開始前にメッセージ交換．

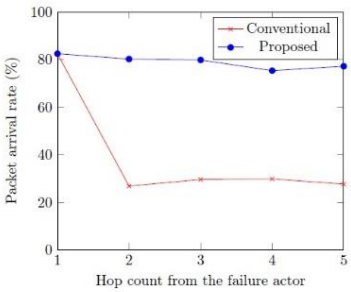
・アクタはパスを形成したのちすぐに自身の移動を開始．

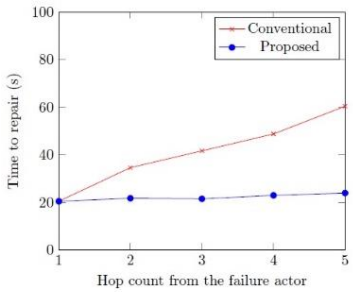


移動する全てのアクタがパス形成しながら移動可能
➡アクタ間接続を維持しつつネットワーク再形成時間を短縮可能

特性評価

移動中のアクタ間のパケット到着率とネットワーク再形成時間を評価しました．





結論

本研究では，アクタ間接続を常時保証するネットワーク再形成手法を提案しました．

本シミュレーション環境において高パケット到着率を達成し，短時間で再形成を完了することを示しました．

本研究に関する業績

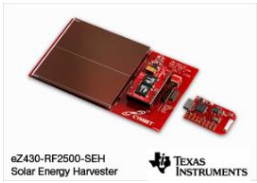
[1] Yuya T, Takuma K, Shinichiro H, Kentaroh T and Iwao S, ˋ Concurrent Moving-based Connection Restoration Scheme between Actors to Ensure the Continuous Connectivity in WSANs,” HPCC2014, Paris, France, August 20-22, 2014.

EHを用いたWSNsにおいて中継ノード選択時の計算量を低減するグリッドルーチング

Ryota Negishi negishi@sasase.ics.keio.ac.jp

研究背景

近年,WSNsを支える技術として環境エネルギーを電力に変換するEHが着目されています.しかし発電量が環境に依存し動作が不安定になるため,従来のルーチングプロトコルが適用できなという問題があります．



http://www.tij.co.jp/tool/jp/ez430-rf2500-seh

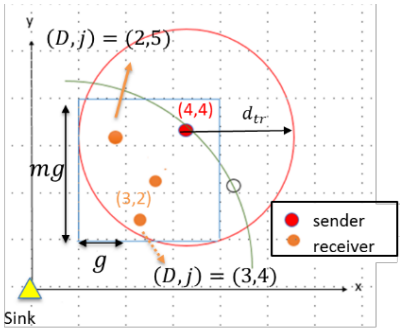
提案方式及び関連研究

従来では,制御パケット,電力モデルの変更や地理的情報を用いたルーチングが提案されてきましたが,オーバーヘッドや計算量の増加が問題となっていました.そこで計算量を低減するルーチングを提案します．

グリッドによってノードに番地を付与．

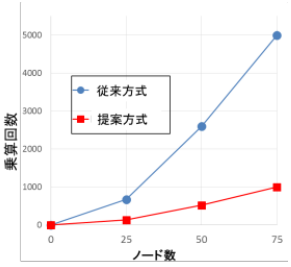
中継ノードはソースノードと番地比較のみで中継スロットを決定．

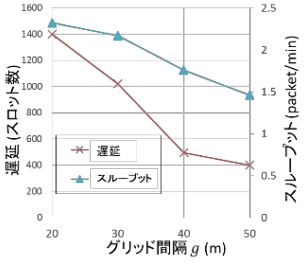
番地差が等しいノード間での衝突を低減するため確率による中継制御．

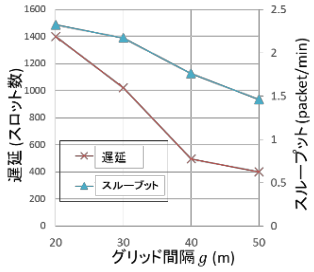


特性評価

乗算回数,グリッド間隔によるトレードオフおよびスループットを評価しました．







結論

本研究では,EH-WSNsにおける中継ノード決定時の計算量を低減するルーチングプロトコルを提案しました．

シミュレーションによってスループットを従来方式と同程度に維持した上で計算量を低減することを示しました．

本研究に関する業績

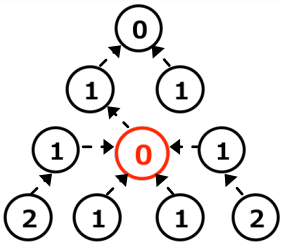
[1] Negishi Ryota, Kentaroh Toyoda and Iwao Sasase, ˋOpportunistic Routing Protocol with Grid-based Relay Slot Selection in Energy Harvesting WSNs ,” APCC2014, Pattaya, Thailand, October 1-3, 2014.

誤検知率の低減を図るRPL監視システム

笹瀬研究室　松永 匠

研究背景

IoTを実現するプロトコルであり，ランク値に基いてルート構築を行うRPL
→ ランク値の偽造を行い多くのパケットを集める攻撃者の検知が必要



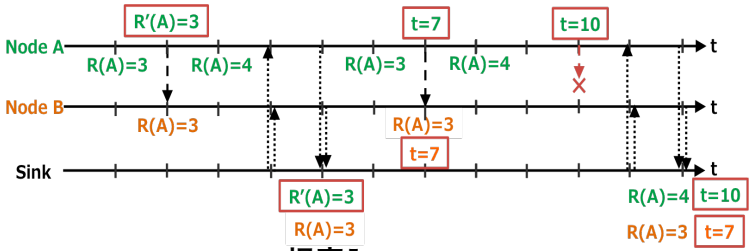
数字: ランク値
赤ノード: 攻撃者

従来方式

シンクが各ノードの近隣ノードの情報を収集し整合性を分析することで攻撃者を検知
→ 情報収集のタイミングやパケットロスにより異なる時刻の情報を用いて整合性を確認することで誤検知が発生する問題

提案方式

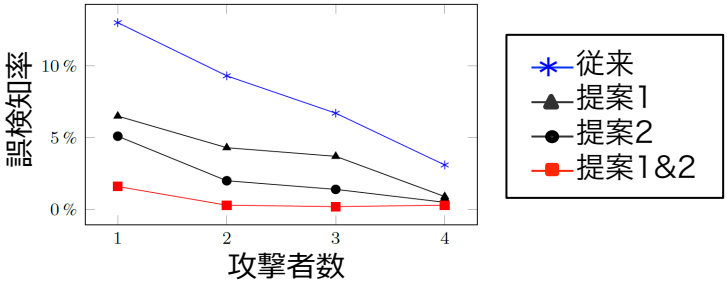
1. **同時刻におけるランク値の利用**
   → 情報収集のタイミングが異なることを考慮
2. **タイムスタンプの利用**
   → パケットロスを考慮して整合性を確認



提案1　　提案2

特性評価

攻撃者数に対する誤検知率の変化を評価
→ 提案方式は従来方式と比較して誤検知率を低減



本研究に関する業績

[1] Takumi Matsunaga, Kentaroh Toyoda and Iwao Sasase, "Low False Alarm Rate RPL Network Monitoring System by Considering Timing Inconstancy between the Rank Measurements," The Eleventh International Symposium on Wireless Communication Systems (ISWCS'2014), Barcelona, Spain, August 25-29, 2014.

RFID物流管理システムにおける決定的 Blocker Tag 検知手法

笹瀬研究室　服部 亮

研究背景

店内や倉庫の在庫管理を容易にする技術であるRFID(Radio Frequency Identification)のタグのプライバシを保護するBlocker Tag(BT)がRFID在庫管理システムを妨害するという問題があります．
そこで笹瀬研究室では，BTを高速かつ正確に検知する方式の研究を行っています．

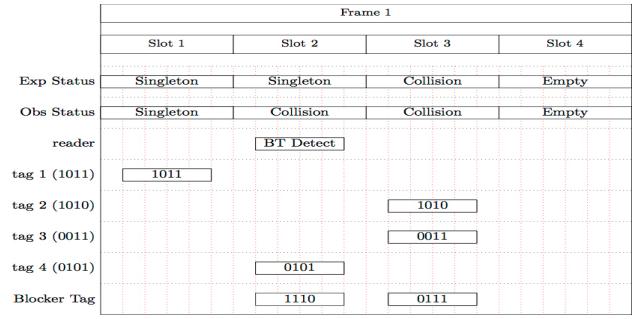
Image taken from silencenet.com

提案方式

リーダは既知の各タグのIDを利用し，応答スロットSNを決めて各スロットの状態を予想する．予想と実際の状態を比較しBTを検知する手法．

$$SN = (ID + r) \bmod f$$

(r :乱数 f : フレーム数)



特性評価

BTを最初に検知するのにかかった最小スロット数を評価しました．タグの数とBTの参加確率を変化させた場合において評価をとりました．

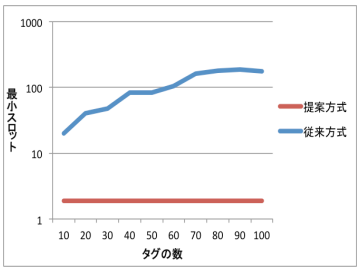


図1. タグ数の変化における BT検知スロット数

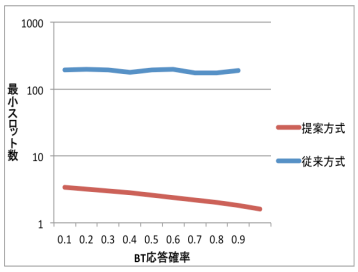


図2. BTの参加確率の変化における BT検知スロット数

本研究に関する業績

[1] Ryo Hattori, Kentaroh Toyoda, Iwao Sasase, "Deterministic Blocker Tag Detection Scheme by Comparing Expected and Observed Slot Status in UHF RFID Inventory Management Systems," The 16th IEEE International Conference on High Performance and Communications(HPCC 2014), Paris, France, August 2014