論文の内容の要旨

論文題目
DETECTION OF COMMUNICATION DISTURBANCES
IN WIRELESS SENSOR NETWORKS
(無線センサーネットワークにおける
メッセージ通信妨害攻撃の検知)

氏名　清　　雄　一

無線センサーネットワークは，多数のセンサーノードから構成され，環境情報を取得することができる.ネットワーク管理者は興味のあるイベントを登録し,そのイベントを検知したノードは,無線を通じてユーザまでマルチホップで通知を行う.無線センサーネットワークは森林火災検知や侵入者検知等に用いることができる．無線センサーネットワークの形態として，信頼できるベースステーション（中央サーバ）を設置する形態と設置しない形態の2 種類がある．信頼できるベースステーションを設置するほうが，より高度な処理を行うことができる．だがベースステーションを設置できない環境に無線センサーネットワークを配置することもあるため,どちらの形態についても考慮する必要がある．ベースステーションが利用できるどうかにより，異なる手法を提案することになる．

無線センサーネットワークは，高範囲の領域に設置されることが多い．そのため，無線センサーネットワークにおいては,攻撃者がセンサーを物理的に取得し,不正に操作する脅威が存在する．センサーノードは通常低コストで製作されるため，耐タンパハードウェアを装備していない．したがって攻撃者は,取得したセンサーノードから,鍵等の情報を全て抜き出すことが可能である．抜き出した情報を用いて，攻撃者はネットワークに対し様々な攻撃を行うことができる．無線センサーネットワークの目的が侵入者検知の場合，攻撃者は，検知されたイベントがユーザまで届かないようにするための攻撃を行うことが考えられる．

本論文は，検知されたイベントが確実にユーザまで届くようにするため，それを阻害する攻撃を検知することを目的とする．攻撃を，物理層・リンク層・ネットワーク層・メッセージング層に分類し，本論文ではメッセージング層における攻撃の検知を行う．メッセージング層の攻撃とし

て，1．メッセージの改ざん，2．メッセージの破棄，3．メッセージ送信によるDoS 攻撃が挙げられる．また，これらの攻撃力を増大させる攻撃として，4．複製ノード攻撃が挙げられる．複製ノード攻撃とは，不正取得したノードを大量に複製してネットワークにばら撒くことにより，ネットワークに多大な影響を与える攻撃である．
また，センサーノードの大きな特徴として故障しやすいことが挙げられる．また，バッテリ駆動であるため，できるだけエネルギー消費を抑える必要がある．従って，無線センサーネットワークにおけるセキュリティ手法を提案する場合には要件として，i.不正取得に対して耐性があり，ii．故障に対して耐性があり，iii．できるだけ省エネルギーな手法であることが求められる．省エネルギーな手法とは，計算量やトラフィック量が少ない手法ということである．
上記1-4 の攻撃を検知する既存研究を調査し，セキュリティ手法の要件i-iii を満たしているかどうかを確認する．満たされていない部分について，本論文において新しい手法を提案する．具体的な貢献は次の通りである．

・メッセージ改ざんノードの検知
信頼できるベースステーションが設置されている状況を想定する．ベースステーションにおいて，メッセージが改ざんされていることを検知すると同時に，メッセージを改ざんしたノードを特定する．既存研究では，メッセージを発生させたノードからベースステーションまでのルーティングパスが固定されている状況にのみ対応している．だが，ノードの故障を考慮すると，無線センサーネットワークではルーティングパスが頻繁に変更されることが予想される．したがって我々はルーティングパスの変更に対応した手法を提案する．また提案手法を用いることにより，ルーティングパスが変更しない状況においても，既存研究よりも早く，メッセージを改ざんしたノードを特定することができる．
・ メッセージ送信によるDoS 攻撃の検知（不正メッセージの検知）
メッセージ送信によるDoS 攻撃として，正しいメッセージを何度も送信する攻撃と，不正メッセージを何度も繰り返し作成し送信する攻撃が考えられる．同じメッセージを何度も送信する攻撃は検知が容易であるため，ここでは，不正メッセージの検知を目的とする．既存研究では，ノード不正取得への耐性とノード故障への耐性を同時に実現する手法が存在しない．したがって我々はこの2 つの要件を同時に満たす手法を提案する．
・ 複製ノードの検知
信頼できるベースステーションが設置されていない状況を想定する．このとき，ノード不正取得攻撃への耐性とノード故障への耐性を同時に実現する既存手法が存在するが，この手法を用いるためには大量のトラフィック量が発生してしまう．したがって我々はこの2 つの要件を同時に満たしつつ，トラフィック量の削減を行う．本手法を用いることで，ベースステーションを利用できる環境と同程度の検知率・トラフィック量で，複製ノードの検知が可能である．