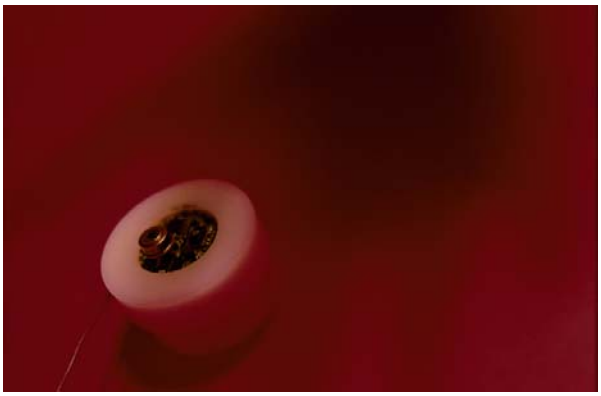
SECURITY IN WIRELESS SENSOR NETWORKS

ワイヤレスセンサネットワークにおけるセキュリティ

Adrian Perrig, John Stankovic, and David Wagner

ワイヤレスセンサネットワークは、ノードキャプチャ、物理的改竄、サービス妨害を含む、さまざまな攻撃の影響を受けやすい．このことが一方で，一連の基礎研究チャンレジへの取り組みを促進している。

ワイヤレスセンサネットワークのアプリケーションには，海洋・野生生物モニタリングや，製造機械の性能モニタリング，建物の安全性と地震モニタリング，及び，多数の軍事応用が含まれる．将来のアプリケーションは，さらに広範囲なスペクトラムになって行くと考えられる．そのようなモニタリングの対象には，高速道路の交通量，公害，森林火災，建物のセキュリティ，水質，さらには人間の心拍数さえも含まれる．これらのシステムの主な利点は，ネットワーク内処理を行うことで生データの大量のストリームを，便利な集約された情報へと還元できることである．それをすべて保護することは極めて重要である．



センサネットワークはユニークなチャレンジを提示するので，伝統的なネットワークで使用されてきた伝統的なセキュリティ技術は直接適用することができない．まず第 1 に，センサネットワークを経済的に実行可能にするためには，センサデバイスは，電力，計算能力，通信能力の点で制限される．第 2 に，伝統的なネットワークとは異なり，センサノードは容易にアクセスできる地域に配備されることが多いので，物理的な攻撃のリスクが増えることになる．第 3 に，センサネットワークは物理的環境や人々と密接に相互作用するので，新しいセキュリティ問題を提示する．結局既存のセキュリティ機構は不十分であり，新しいアイデアが必要になる．幸いこの新しい問題のおかげで，新しい研究が盛んになっており，開始時点からセンサネットワークセキュリティについて話す機会が与えられている．

本稿では，これらのネットワークにおけるセキュリティ問題について概観し，センサネットワークセキュリティの現状を議論し，今後の研究の方向について述べる．我々は，鍵確立（key establishment），秘密厳守（secrecy），認証（authentication），プライバシー，サー

ビス妨害攻撃（denial-of-service）に対する頑健性（robustness），安全なルーティング（secure routing），及びノードキャプチャ（node capture）を含む，いくつかの重要なセキュリティチャレンジについても触れる．また，ワイヤレスセンサネットワークに対して要求されるいくつかの高レベルセキュリティサービスについても触れ，今後の研究チャレンジで本稿を終わる．

安全なシステム

セキュリティはシステムアーキテクチャの独立したコンポーネントとしてみなされることもあり，そのような場合別のモジュールがセキュリティを提供している．しかし，この分離は，通常，ネットワークセキュリティに対する欠陥のあるアプローチである．安全なシステムを完成させるためには，セキュリティを考慮せずに設計されたコンポーネントは，攻撃の対象となりやすいので，セキュリティは各コンポーネントに統合する必要がある．

鍵確立と信用設定

センサネットワークを構築する際，最初に要求されるものの 1 つは，以後に使用する暗号鍵の確立である．研究者は，数十年以上もの間，この十分に研究されてきた問題に対してし，様々な提案してきた．しかし，なぜセンサネットワークでは，同じ鍵確立プロトコルを用いることができないのだろうか？それは，センサネットワーク固有の性質が，以前のプロトコルを非実用的なものにしてしまう．多くの今日のセンサデバイスは計算能力を限定してしまうので，公開鍵暗号基本演算はシステムオーバヘッドの点でコストがあまりにも高くなる．鍵確立技術は，何百何千というノードを持つネットワークの規模拡大が必要となる．さらにセンサネットワークの通信パターンも従来のネットワークとは異なっている：センサノードが鍵確立を行うのは，隣のノードだけでなく，データ集積ノードとも行う必要があろう．

最も単純な鍵確立の手法は，ネットワークワイドの共有鍵をつくることである．残念なことに，ネットワーク中のたった 1 つのノードでもセキュリティ侵害（compromise）を許すと，秘密鍵が明らかになり，すべてのネットワークトラフィックが復号化されてしまう．この考えの 1 変種は，ネットワーク全体でたった 1 つの共有鍵を使用して，通信をするノード 1 組に対して 1 個ずつのリンク鍵の集合を確立し，次にセッション鍵を設定したらネットワークワイドの鍵を消去する方法である．しかし，鍵確立プロセスのこの変種では，初期配備完了後には新しいノードの追加が許されない．

公開鍵暗号系（例えば，Diffie-Hellman 鍵確立法）は，今日のセンサネットワークの能力を上回る別のオプションである．その主な利点は，ノードがネットワーク中の他のいかなるノードとも安全鍵を生成できることである．

さらに別のアプローチとして，あまり深く考えられているわけではないが，各組のノード間にユニークな対称共有鍵を，ネットワークに前もって設定する方法がある．この手法では，n 個のノードを持つセンサネットワークにおいて，各ノードは n-1 個の鍵を保持する必要があるので，ネットワーク内の確立で必要とされる鍵は n(n-1)/2 個となる．

信頼できる基地局を使用して鍵をブートストラッピングするのも別のオプションである．ここでは，各ノードは基地局とたった 1 つの鍵を共有し，基地局を通して他のノードとの鍵を生成する必要がある[6]．この調停において，基地局をたった 1 つの故障点とするが，たった 1 つの基地局しかないので，基地局のみに改ざん防止のパッケージングを組み込めば，物理的攻撃の脅威は改善されよう．

研究者たちは最近，ランダム鍵事前配布（random-key predistribution）プロトコル[3]を開発した：そのプロトコルでは，対称鍵の大きなプールを選択し，そのプールからランダムに選ばれた部分集合を各センサノードへ配布される．お互いに通信をしたい 2 つのノードは，各々のプールを探し，お互いが共通の鍵を共有するかどうかを決定する；もし，あれば，両方のノードはそれを使用してセッション鍵を確立する．すべてのノードの組が共通鍵を共有しているというわけではないが，もし，鍵確立確率が十分に大きければ，ノードは，十分に多くのノードと鍵確立を行い，その結果，完全連結ネットワークを得ることができる．鍵確立の本手法は，信頼され

た中央基地局を含む必要性から回避できる．本アプローチの欠点は，十分に多くのノードにセキュリティ侵害を行った攻撃者ならば，完全な鍵プールを再構築し，この手法を破ることが可能となることである．

将来は，我々は，ノードへのセキュリティ侵害に対する回復力（resilience）を与えるよりよいランダム鍵事前配布法の研究成果や，公開鍵暗号系あるいはより効率のよい公開鍵暗号系（例えば楕円曲線暗号）に対するハードウェアサポートの研究成果を期待する．究極的には，我々は，大規模センサネットワークのため単純な鍵確立を可能にする安全で効果的な鍵配布機構を必要としている．

秘密厳守と認証

従来のネットワークと同様，ほとんどのセンサネットワークアプリケーションは，傍受（eavesdropping），挿入（injection），パケット改竄（modification）に対する保護を必要としている．暗号は，標準的な防御手段である．センサネットワークに暗号法を組み込むもうとすると，興味深いシステムトレードオフが生じる．1 対 1 通信（point-to-point）のためには，端末間（end-to-end）暗号は高レベルのセキュリティを達成するが，鍵はすべての端末（end point）間で設定されなければならず，また，受動的参加や局所的ブロードキャストとは両立することができない．ネットワークワイドの共有鍵を持つリンク層暗号（link-layer cryptography）は鍵設定を単純にし，受動的参加と局所的ブロードキャストをサポートするが，中間ノードでのメッセージ傍受や改竄が可能となる．

最も初期のセンサネットワークは，リンク層暗号を使用していたようである．というのは，このアプローチが現在利用可能なネットワーク暗号のアプローチの中で最も容易に配備できるからである．より高度な暗号の使用法の開発が進めば，後続のシステムは，よりセキュリティの高い要求に応えていけるようになるだろう．

暗号は，往々にしてパケットサイズを増加させる余分な計算のために必要な性能コストが伴う．暗号のためのハードウェアサポートは，効率をよくするが，ネットワーク実装コストも増加させてしまう．それゆえに，センサノードの研究者や担当者が直面する重大な疑問は次のようなものである：合理的なセキュリティと性能レベルは，ソフトウェアのみの暗号実装で達成できるのか，あるいは，ハードウェアサポートが必要なのか．

最近の研究では，ソフトウェアのみの暗号は，実際に今日のセンサ技術にとって実用的であるということを例証している．すなわち，ハードウェアサポートは，満足できるセキュリティや性能レベルを達成するには必要がない．例えば，カリフォルニア大学バークレー校が実装した TinySec では，ソフトウェアのみの方法を使用しても 5%～10%の余分な性能オーバヘッドしか生じなかった．これらの実験は，また，興味深い現象を明らかにした：ほとんどの性能オーバヘッドがパケットサイズの増加に起因している．対照的に，暗号計算は，転送とオーバラップできるので，待ち時間（latency）やスループットにはほとんど何の効果もない．これは，専用ハードウェアがどれだけ貢献するかの限界を与えている．ハードウェアは，計算コストだけを削減するが，パケットサイズを削減しない．

究極的には、我々は，大規模センサネットワークのため単純な鍵確立を可能にする安全で効果的な鍵配布機構を必要としている．

プライバシー

センサネットワークはまた，プライバシーの懸念も最前線に押しやってしまった．最も明確なリスクは，ユビキタスセンサ技術の発展に伴い，悪意ある個人が，被害者に気づかれないで監視するために，秘密監視（secrete surveillance）ネットワークを配備できるようになることである．雇用主は従業員を監視できよう．店長は消費者を監視できよう．隣人はお互いに監視し合うことができよう．さらに，法律施行機関は，公共の場を監視できよう．これは，確かに妥当な懸念である：歴史的に見ても，監視技術は，より低価格に，より効果的になっているので，プライバシー悪

用（privacy abuse）にますます多く関連するようになってきている．技術動向からは，この問題は時とともに悪化するように思える．装置が小型化するにつれて，隠しやすくなる．装置が低廉化するにつれて，監視ネットワークはより手頃な値段になっていく．

もう 1 つのリスクは，もともと合法的目的のために配備されたセンサネットワークが，その後，予想外の，しかも，非合法的目的のために使用される可能性である．利用目的の逸脱（function creep）という概念は，プライバシー関連文献では普遍的である．例えば，米国の社会保障番号（Social Security number）は当初はソーシャルセキュリティプログラムにだけ使用されることが意図されていたが，徐々にあらゆる目的用個人同定番号として使用されるようになっている．

センサネットワークのネットワーク化された性質のため，世界中の私的な市民がこれまでに直面してきたこととは，質的に異なる新しい脅威が引起されている．センサネットワークのおかげで，データ収集，協調的な分析，さらには自動事象相関（event correlation）が可能になる．例えば，センサのネットワーク化システムは，長期間にわたった人々や自動車のルーティン的な追跡が可能になる．もちろん，面倒な影響はあるが．

技術だけでは，プライバシー問題を解決できそうにない．むしろ，社会規範との統合，新しい法律，そして，技術の応答が必要となる．手始めに，正しい情報訓練を行えば，よりよくプライバシーを保護するシステムの構築法について，合理的なガイドラインを与えることができるかもしれない．現在，センサノードの存在やデータ獲得に対するアウエアネス（訳注：センサノードに目立つ色をつける；センサの稼動中はランプがつく）を与えることは特に重要である．監視の存在，形式，意味に問題に気づき，影響を受けた団体は，そのような技術を受け入れる可能性がより高い．しかし，我々のセンサネットワークにおけるプライバシーに対する理解は現時点では未熟であり，さらに多くの研究が必要とされる．

サービス妨害攻撃通信に対する頑健性

攻撃を仕掛ける者（adversaries）は，サービス妨害攻撃を通してワイヤレスセンサネットワークの価値を大きく制限する[9]．その最も単純な手口として，彼らは，高出力信号をブロードキャストすることによってネットワーク動作を混乱させようとする．もし，送信が十分に高パワーであれば，全システムの通信が渋滞（jam）するであろう．より高度な攻撃も可能である．例えば隣人が転送している最中に転送を行って IEEE802.11 メディアアクセス制御（MAC）プロトコルを妨害することによって，あるいは，request-to-send 信号を使ってチャネルアクセス要求を連続的に行うことによって，通信を不能にできよう．

ジャミングに対する標準的防御法の 1 つとして，スペクトラム拡散通信（spread-spectrum）[1]がある．しかし，暗号化による安全なスペクトラム拡散無線は商用てきにはまだ利用できない．さらに，この防御法は，ノードをキャプチャし，その暗号鍵を入手した攻撃者に対して安全ではない．

センサネットワークのネットワーク化された性質のおかげで，サービス妨害攻撃に対して，新しい自動化された防御が可能となる．もし，ジャミングがネットワークの一部の場所でしか影響が出ていないのであれば，ジャミング防止（jamming-resistant）ネットワークはジャミングを検出し，影響を受けた場所を同定し，渋滞地域を回避するようにルーティングすることで，攻撃を防御できる[8]．この分野でのさらなる進歩が，うまく行けば，サービス妨害攻撃に対してより優れたセキュリティを可能にするだろう．

安全なルーティング

ルーティングとデータ転送はセンサネットワークにおける通信を可能にするための必須のサービスである．残念なことに，現在のルーティングプロトコルは数多くのセキュリティ脆弱性（vulnerabilities）に苦しんでいる[5]．例えば，攻撃者は，ルーティングプロトコル上で，サービス妨害攻撃を開始し，通信を妨害する．最も単純な攻撃は，悪意あるルーティング情報をネットワークに挿入し(injection)，その結果ルーティング情報の矛盾を引起す．単純な認証でもインジェクション攻撃を防護できるが，いくつかのルーティングプロトコルは，攻撃者が適法のルーティ

ングメッセージを送ることで，それを再送してしまう可能性がある[4].

ルーティングプロトコルは，特にノードキャプチャ攻撃を受けやすい．例えば，研究者は，センサネットワークでのルーティングのためのプロトコルを分析し，いずれのプロトコルもノードキャプチャ攻撃の影響をとても受けやすいということを発見した．いずれの場合にも，たった 1 つのノードでもセキュリティ侵害が起こると，ネットワーク全体を乗っ取ってしまうのに，あるいは，ネットワーク内のあらゆる通信を妨害してしまうのに十分である[5]．ネットワーク研究者は，そのような攻撃に対して頑健である安全なルーティングプロトコルを考案することによってセンサネットワークを大きく改善するであろう．

ノードキャプチャに対する回復力

センサネットワークが直面している最も挑戦的な課題の 1 つに，ノードキャプチャ攻撃に対する回復力がある．従来の計算では，物理的セキュリティが当然のこととみなされることが多かった．つまり，攻撃者からの我々のコンピューターへの物理的なアクセスを拒否するだけでよい．センサネットワークはそのようなパラダイムを崩壊した．多くのアプリケーションで，センサノードは攻撃者が容易にアクセスできるような場所に設置されることが多い．そのような野ざらし状態のために，攻撃者はセンサノードをキャプチャしたり，暗号の秘密を取り出したり，プログラムを改竄したり，あるいは，攻撃者の支配下にある悪意あるノードと置換したりできる可能性が高くなる．

改竄防止パッケージングは，1 つの防御法であるが，現在の技術では高いレベルのセキュリティを提供できないので高価なものになる．ノードキャプチャ攻撃問題には，アルゴリズムによる解決が望まれる．

ここでのチャレンジは，我々に気づかれずに複数のノードでセキュリティ侵害が生じ，その結果，それらが勝手に悪意ある方法で行動を始めたとしても，正常に機能するネットワークを構築することである．回復力のあるネットワークを構築する有望な方法として，ネットワーク全域で状態を複製し，多数決法や他の方法を利用して，不一致を検出する．例えば，複数の研究者たちは，書くパケットを複数の独立した経路で送信し，目的地で受信したパケット間の整合性をチェックすることによって，ノードキャプチャに対するある種の回復力を達成するルーティングプロトコルを設計している[2].

回復力に対する第 2 の方向は，環境に対する複数の冗長な観察を集め，それらの整合性をチェックすることである．例えば，ネットワークは興味深い事象の 3 回のレポートを要求してから始めてその事象に応答するようにする．一方で，たくさんのデータが得られる場合には，ヒストグラムを作成できよう．極端に外れたデータは，悪意ある偽データである可能性を示しているので，無視すべきである．

冗長性に基づいた防御法はセンサネットワークには特によく適している．というのは，星座のように多数の安価なノード群の方が，小さなグループのより洗練されたデバイス群よりも信頼度のより高いネットワークを提供できる可能性がある．にもかかわらず，ノードキャプチャは，センサネットワークセキュリティにおいて，最も悩ましい問題の 1 つである．我々がよい解決策を得るためにはまだ時間がかかりそうである．

ネットワークセキュリティサービス

これまでに我々は，センサネットワークを安全にするための低レベルセキュリティ要素技術について概観してきた．ここでは，安全なグループ管理（group management）や，進入検知（intrusion detection），及び，安全なデータ集約（data aggregation）を含む高レベルなセキュリティ機構を概観する．

安全なグループ管理

ワイヤレスセンサネットワーク内の各ノードは，計算能力と通信能力に制限がある．しかし，興味深いネットワーク内データ集約や分析が，ノードのグループで実行されている．例えば，ノードグループは，ネットワークを通してある自動車を共同で追跡する責任を負わされている．グループを実際に構成するノードは，連続的にすばやく変化する．ワイヤレスセンサネットワークの他の多くの鍵となるサービスもグループで実行されている．従って，新しいメンバーを安全にグループに受け入れ，安全なグループ通信を支援するグル

ープ管理のための安全なプロトコルが必要とされている．グループによる計算の結果は，普通に基地局へ送信される．その出力は，有効なグループから来たものであると補償するために認証されなければならない．どの解決策も，多くの古典的なグループ管理の解決法を排除して，時間とエネルギーの点で効率的（あるいは，計算コストや通信コストの低いような）でなければならない．

侵入検知

ワイヤレスセンサネットワークは，あらゆる形式の侵入を受けやすい．有線ネットワークでは，典型的には，さまざまな集中点で，異常検出するためにトラフィックと計算が監視され分析される．これは，もともとバンド幅に限界がある上に，ネットワークのメモリやエネルギー消費の点でコストがかかることがしばしばある．ワイヤレスセンサネットワークは通信，エネルギー，メモリに関する要求条件の観点から完全に分散された安価な解決法を必要としている．異常を発見するために，アプリケーションや典型的な脅威モデルが理解されなければならない．研究者や担当者は，協力で攻撃するグループが，どのようにシステムを攻撃するかを理解することが特に重要である．安全なグループを使用することは，非集中型侵入検知システムのために，有望なアプローチになるだろう．

安全なデータ集約

ワイヤレスセンサネットワークの 1 つの利点は，大規模で密度の高いノードの集団から得られるきめ細かいセンシングにある．計測された値は，圧倒する量のトラフィックが基地局へ返送されるのを避けるために集約されなければならない．例えば，システムは，地理的な範囲の気温や湿度を平均化してもよいし，移動物体の位置や速度を計算するためにセンサデータを組み合わせてもよいし，実世界の事象を検知する際の間違い警報（false alarm）を回避するためにデータを集約してもよい．ワイヤレスセンサネットワークのアーキテクチャに依存して，集約はネットワークの多くの場面で生じうる．すべての集約場所は安全でなければならない．

アプリケーションが，大まかなセキュリティ対策が許容できるのならば，強力な技術が利用可能である．ある程度の信頼が成り立つのであれば，小さな部分のノード群をランダムにサンプリングして，それらが適切に動作しているかをチェックすることによって，多くのさまざまな形式の攻撃の検知をサポートできる[7].

研究のチャレンジ

ワイヤレスセンサネットワークの厳しい制約と要求の厳しい配備環境のため，これらのシステムのためのコンピュータセキュリティは，従来のネットワークのそれより，もっと難しいものになっている．しかし，センサネットワークのさまざまな特性のおかげで，皆が安全なネットワークの構築というチャレンジを明確な言葉で表現することができよう．第 1 に，セキュリティ対策が，まだ初期の設計と研究段階にあるので，我々は，初めからこれらのシステムにセキュリティソリューションを組み入れる機会がある．第 2 に，多くのアプリケーションが，たった 1 つの管理領域の下でセンサネットワークの配備を必要としているようなので，脅威モデルを単純化できる．第 3 に，冗長性，規模，及び，ソリューションでの環境の物理的特長を追求することが可能になろう．たとえセンサ群の一部分に障害が起こっても，稼動し続けるようにセンサネットワークを構築したら，我々は，さらなる攻撃に抵抗できるように，冗長なセンサを使用する機会がある．究極的に，センサネットワークの独特の側面のおかげで，従来のネットワークでは利用できなかった革新的な防御ができるかもしれない．

ほかの多くの問題もさらなる研究が必要である．1 つは，傍受，改竄，通信分析，サービス妨害に対して，ワイヤレス通信リンクをどのようにして安全にするかという問題である．他には，資源の制限などがある．現在の研究方向には，非対称プロトコルが含まれ，そこでは，大部分の計算負荷が基地局にかかり，公開鍵暗号システムでは，低位の端末装置では効率的にしている．最終的に，おそらく冗長性や物理的な環境についての知識を通して，物理的なセキュリティの欠如を許容する方法を発見することは，継続する全体的なチャレンジとして残っている．我々は，すべての問題が解決できる大いなる進展があるものと楽観視している．

文献

1. Adamy, D. EW 101: *A First Course in Electronic Warfare*. Artech House Publishers, Norwood, MA, 2001.
2. Deng, J., Han, R., and Mishra, S. A performance evaluation of intrusion-tolerant routing in wireless sensor networks. In *Proceeding of the 2nd IEEE International Workshop on Information Processing in Sensor Networks* (IPSN 2003) (Apr. 2003), 349-364.
3. Eschenauer, L. and Gligor, V. A key-management scheme for distributed sensor networks. In *Proceeding of the 9th ACM Conference on Computer and Communication Security* (Washington, D.C., Nov.). ACM Pres, New York, 2002, 41-47.
4. Hu, Y.-C., Perring, A., and Johnson, D. Packer leashes: A defense against wormhole attacks in wireless ad hoc networks. In *Proceeding of IEEE Inform 2003* (San Francisco, Apr. 1-3, 2003).
5. Karlof, C. and Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proceeding of the 1st IEEE International Workshop on Sensor Network Protocols and Applications* (Anchorage, AK, May 11, 2003).
6. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. SPINS: Security protocols for sensor networks. *J. Wireless Nets.* 8, 5 (Sept. 2002), 521-534.
7. Przydatek, B.,Song, D., and Perrig, A. SIA: Secure information aggregation in sensor networks. In *Proceeding of the 1st ACM International Conference on Embedded Network Sensor Systems (SenSys 2003)* (Los Angeles, Nov. 5-7). ACM Press, New York, 2003, 255-265.
8. Wood, A., Stankovic, J., and Son, S. JAM: A mapping service for jammed regions in sensor networks. In *Proceedings of the IEEE Real-Time Systems Symposium* (Cancun, Mexico, Dec. 3-5, 2003).
9. Wood, A. and Stankovic, J. Denial of service in sensor networks. *IEEE Comput.* (Oct. 2002), 54-62.

ADRIAN PERRIG

（perrig@cmu.edu）は，PA 州ピッツバーグにあるカーネギーメロン大学の電気・計算機工学と公共政策の助教授である．

JOHN A. STANKOVIC

（stankovic@cs.virginia.edu）は，VA 州シャーロッツビルにあるバージニア大学計算機科学科の BP America 冠講座教授であり，学科長である．

DAVID WAGNER

（daw@cs.berkeley.edu）は，カリフォルニア大学バークレー校の電気工学・計算機科学の助教授である．

訳：田崎豪（京都大学・情報学研究科）