特集論文

無線メッシュネットワーク対応セキュリティ技術

小林信博*
山口晃由**
村上ユミコ**

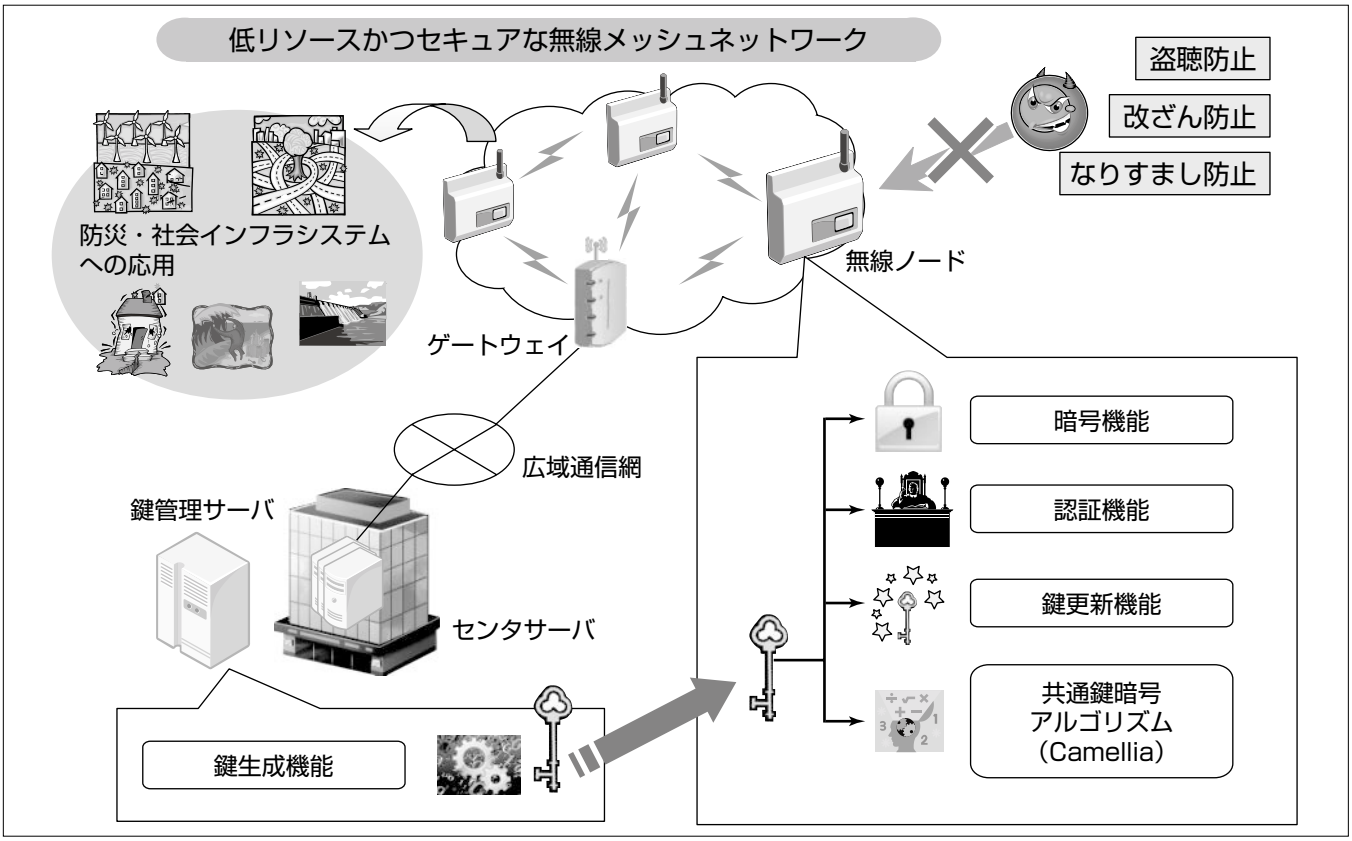
Security Technologies for Wireless Mesh Network

Nobuhiro Kobayashi, Teruyoshi Yamaguchi, Yumiko Murakami

要　旨

近年，災害対策及びスマートグリッド・スマートコミュニティ等の防災・社会インフラ分野において，ワイヤレスセンサネットワークの一つである無線メッシュネットワークを用いたITシステムに期待が高まっている。無線メッシュネットワークシステムでは，多数の小型かつ省電力な無線ノードと一つのゲートウェイが分散配置され，自律的に無線メッシュネットワークを構築するとともに，各無線メッシュネットワークを広域通信網に接続し，センタサーバと無線ノードの連係によって情報収集，分析，制御を行うことが検討されている。無線メッシュネットワークを構成する無線ノードは，演算能力や電力等の限られたリソースの範囲で動作することが望まれる一方，社会インフラ分野へ適用する際には，我々の生活に悪影響を及ぼすおそれのある不正アクセスやサイバー攻撃などの脅威に対して，十分なセキュリティが確保されている必要がある。特に考慮すべき脅威としては，無線で送受信するデータの盗聴・改ざん，不正機器のなりすまし，機器の盗難や内部解析による秘密情報の漏洩，暗号鍵の推定・流出等が挙げられる。

本稿では，無線メッシュネットワークの制約条件とセキュリティ要件について整理のうえ，三菱電機における安全性と低リソースの両立を指向したセキュリティ対策技術として，共通鍵暗号アルゴリズム“Camellia”を用いた鍵生成機能，暗号機能，認証機能，鍵更新機能について述べる。この技術によって，安全性を確保しつつ無線ノードの小型化，低コスト化が可能となり，防災・社会インフラ分野への無線メッシュネットワークの適用範囲拡大が期待できる。



無線メッシュネットワーク対応セキュリティ技術

無線メッシュネットワークでは，通信データの盗聴，改ざん，無線ノードへのなりすまし等の攻撃が想定され，セキュリティの確保が必須となる。計算機資源などのリソースが乏しい無線ノードに，当社保有の共通鍵暗号技術を応用した暗号機能，認証機能，鍵更新機能を備え，鍵管理サーバの鍵生成機能によって各無線ノードの鍵を生成することで，低リソースかつセキュアな無線メッシュネットワークを構築することができる。

*情報技術総合研究所　**同研究所（工博）

1. まえがき

近年，災害対策及びスマートグリッド・スマートコミュニティ等の社会インフラ分野で，ワイヤレスセンサネットワークの一つである無線メッシュネットワークを用いたITシステムに期待が高まっている。無線メッシュネットワークシステムでは，多数の小型かつ省電力な無線ノードと一つのゲートウェイが分散配置され，自律的に無線メッシュネットワークを構築するとともに，各無線メッシュネットワークを広域通信網に接続し，センタサーバで情報収集，分析，制御を行う。この無線メッシュネットワークシステムの利用によって，地震や豪雨などの異常現象を的確に把握して避難指示や人命救助につなげる防災基盤の高度化や，地域，施設，住宅での電力需給を最適化することで低炭素化社会の実現につながるスマートグリッド・スマートコミュニティを実現することなどが期待されている[(1)(2)]。しかし，今後の防災・社会インフラ分野を支えるシステムとして適用する際には，不正アクセスやサイバー攻撃等の脅威に対するセキュリティの確保が必須となる。

本稿では，無線メッシュネットワークの制約条件とセキュリティ要件，そして当社における安全性と低リソースの両立を指向したセキュリティ対策技術について述べる。

2. 無線メッシュネットワークにおける制約条件とセキュリティ要件

2.1 無線メッシュネットワーク

無線メッシュネットワークとは，一つのゲートウェイと複数の無線ノードが，自律的に無線通信を行うことで構築される無線ネットワークのことである。ゲートウェイは無線メッシュネットワークと広域通信網をつなぐ装置であり，広域通信網に接続されているセンタサーバと無線メッシュネットワーク内の無線ノードとの通信を中継したり，無線メッシュネットワークの管理を行ったりする。無線ノードは分散配置され，自身のデータを送受信したり，近隣の無線ノードからのデータを中継したりする(**図1**)。

2.2 無線メッシュネットワークのセキュリティ要件

社会インフラを支えるシステムに無線メッシュネットワークを適用する場合，次のような脅威にさらされることが想定される。

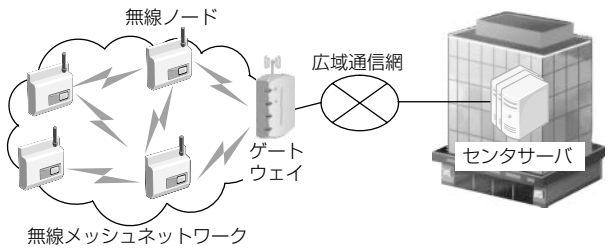


図1．無線メッシュネットワーク

①偽の無線ノードによる，なりすまし
②無線通信データの盗聴による情報漏洩(ろうえい)
③攻撃者による不正データの送信
④暗号化された無線通信データの解読(鍵の推定)
⑤攻撃者による妨害電波の発信
⑥無線ノードを分解，内部の秘密情報(鍵)を不正入手

このような脅威に対して，次のような対策を行う必要がある。

(1) 認証

攻撃者によるなりすましを防ぐため，ネットワークに参加している無線ノードの正当性を確認するための認証が必要となる。

(2) 暗号化

無線通信によって送受信されるデータには，プライバシー情報などの機密情報が含まれる可能性があることから，情報漏洩を防ぐために暗号化によるデータの秘匿が必要となる。

(3) 改ざん検知

制御情報や収集するデータの完全性を確保するため，通信データの認証によって改ざんを検知する必要がある。

(4) 鍵共有・更新

認証，暗号化，改ざん検知で用いられる鍵の共有と，同じ鍵を使い続けることによって低下する安全性を回復するために鍵の更新が必要となる。

(5) 通信妨害対策

無線通信を利用するため，攻撃者からの不正電波の発信による局所的な通信妨害を根本的に排除することは難しいが，通信チャネルの変更などの対策が考えられる。また，不正データの検出によってネットワーク内の伝播(でんぱ)を遮断するフィルタの導入も必要となる。

(6) 耐盗難性

攻撃者による機器の盗難や内部解析が行われる前提のもと，システム全体の危殆(きたい)化を回避し，可用性を維持可能なセキュリティ方式を採用する必要がある。

2.3 セキュリティ機能実装における制約条件

無線メッシュネットワークシステムを構成する無線ノードは，設置場所に対する制約が少ない反面，物理的に保護されない状況下で攻撃者による盗難や内部解析の脅威にさらされるおそれがある。また，内蔵電池や太陽電池などから供給される限られた電力で動作することが求められる。さらに，コスト上の理由から限られた演算能力とメモリ容量しか与えられない。これら無線ノードにおける制約条件を次に示す。

①演算能力が乏しく複雑な処理に時間がかかる。
②メモリ容量が乏しく大量のデータが扱えない。
③電力が乏しく演算や通信が制限される。
④攻撃者からの隔離が難しい。

社会インフラ分野で無線メッシュネットワークシステムを利用する場合には，これらの制約を踏まえてセキュリティを考慮する必要がある。

3. 当社の取組み

当社では，考えうる最高の安全性を追求するのと同様に，限られたリソースの中で必要な安全性を確実に担保することを重視している。無線メッシュネットワークの適用先として想定している防災・社会インフラ分野では，その特質からシステム構築の費用が，最終的な受益者の人々への負担につながることが避けられない。そこで今回は，必要な安全性の確実な担保というポイントにフォーカスし，無線メッシュネットワークにおける制約条件とセキュリティ要件を，リソースに乏しい無線ノードでも実現可能なセキュリティ技術を開発した。

無線ノードに求められるセキュリティ機能のうち，**3. 1節**で認証，暗号化，改ざん検知について，**3. 2節**で耐盗難性について，**3. 3節**で鍵共有・更新について述べる。

3. 1 省リソース志向の機器認証と通信データ保護技術

計算機資源などの各種リソースが乏しい無線ノードで，メッシュネットワークへ参加する際の正当性を証明する認証，無線経由の通信データを攻撃者の盗聴や改ざんから保護する暗号化及び改ざん検知の各セキュリティ機能を実現するには，計算量の少ない軽量な暗号技術を利用することが求められる。具体的な暗号技術としては，共通鍵暗号技術やハッシュ関数が該当する。一方で，最新のセキュリティ技術動向に対応した安全性の確保も重要である。システムに用いる暗号アルゴリズム，プロトコルの選定にあたっては，国際標準化団体であるISO/IEC（International Organization for Standardization/International Electrotechnical Commission），電子政府推奨暗号の安全性評価・監視プロジェクトであるCRYPTREC（Cryptography Research and Evaluation Committees），米国国立標準技術研究所NIST（National Institute of Standards and Technology）によって公表されている指針・推奨に則することが，防災・社会インフラ分野で重要視される公正な判断に基づく安全性の確保についての証明にもつながる。当社では，共通鍵暗号アルゴリズムの選定にあたり，NIST SP800-57 [4][5]に基づいてセキュリティ強度として 128ビット安全性が長期の運用にも余裕を持って耐えうると判断した。そこで，通信データの暗号化及び改ざん検知のために，当社とＮＴＴが共同開発し，既に国際標準規格ISO/IEC 18033-3[6]及び電子政府推奨暗号リスト[7]に採用されている128ビットブロック暗号アルゴリズム“Camellia[8]”を選択し，暗号の利用モードとして，NIST SP800-38C[9]で規定されている守秘・認証用の暗号利用モードであるCCM（Counter with Cipher block chaining-Message authentication code）モードを採用した。また，認証のプロトコルとしてISO/IEC 9798-4-4に採用されている Three pass authentication を用いることで，共通鍵暗号を利用した相互認証を実現した。

3. 2 耐盗難性を考慮した無線ノードの鍵生成技術

無線ノードは設置場所に対する制約が少ない反面，盗難などの物理的脅威にさらされており，内部解析による情報漏洩を防ぐためにデータ暗号化などの対策が施される。データ暗号化は入力としてデータそのもののほかに鍵を必要とし，多くの場合，この鍵は銀行口座の暗証番号のように第三者には秘密にしておかなければならない。すなわち，鍵の情報が漏洩すると，強固に設計された暗号でも安全性が著しく低下してしまうため，暗証番号と同様，第三者が容易に予測できる生成法は避けるべきである。

図 2にあるように，鍵の生成には共通鍵暗号アルゴリズムを採用した。この共通鍵暗号アルゴリズムは，先に述べたデータ暗号化処理と本質的に同じである。つまりデータと鍵の入力を必要とする。データ暗号化処理の出力を一般に暗号文と呼ぶが，鍵生成の場合はこの暗号文が，目的の“鍵”となる。この出力された“鍵”と区別するため，**図 2**では入力の鍵はマスタ鍵と表記している。マスタ鍵は，鍵生成者（無線ノードメーカーなど）だけが知る値を用いる。もう一つの入力となるデータには，無線ノードや無線メッシュネットワークの識別子などを用いる。無線ノード識別子を用いた場合は無線ノードごとに異なる鍵が生成され，無線メッシュネットワーク識別子を用いた場合は，同一の無線メッシュネットワーク内の無線ノードは同一の鍵を持つことになる。万が一この鍵が漏洩した場合，同一の鍵を持つ他の全無線ノードに影響が及ぶため，無線ノードごとに異なる鍵を持つことがセキュリティ上望ましいが，これはセキュリティ強度が上がる反面，鍵の管理が煩雑になるため，運用に応じた使い分けが必要になる。なお，**図 2**にあるように，この識別子は，共通鍵暗号アルゴリズムに入力する前に一度ハッシュ関数に通しておき，その出力（ハッシュ値）を共通鍵暗号アルゴリズムの入力データとする。これによって，偏りがちな識別子の分布を散らすことができる。

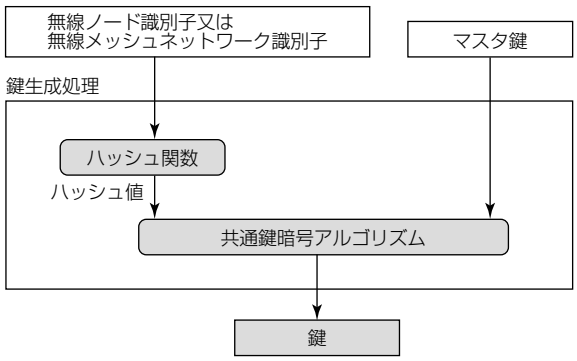


図 2．鍵生成処理の概略

3.3 時刻の非同期を許容可能な暗号鍵の更新技術

無線メッシュネットワークでは，リソースの制約から，事前に共有した共通鍵だけを用いて暗号通信を行う必要がある。同一の共通鍵を長期に使用することは，鍵の推定による危殆化を招く。そのため，共有した共通鍵と，無線ノード間で同期したパラメータから一時暗号鍵を生成して通信に用いる必要がある。

ノード間で同期に使用できるパラメータとして，時刻が考えられるが，リソースの乏しいノードでは，高精度な時刻同期を期待できない。NTP(Network Time Protocol)などの時刻同期プロトコルを用いた場合も，時刻同期のパケットを改ざんされるおそれがあるため，同パケットをメッセージ検証する仕組みを別に用意する必要がある。

そこで，各ノードで単調増加のカウンタを保持し，カウンタ値と共通鍵から一時暗号鍵を生成する方式を採用した。カウンタ値の最大値は更新頻度と製品寿命から決定する。タイマによってカウンタをインクリメントすることで，過去に使用した一時暗号鍵を無効化する。また，カウンタ値は，送信パケットに付与される。受信側ノードはパケットの真正性を確認したのち，自身が持つカウンタ値と比較し，パケットの受理判定とカウンタ値の更新を行う。各々のメッセージとカウンタ値は一時暗号鍵でメッセージ検証されるので，カウンタ値だけの改ざんを行うことはできない。また，正規の無線ノードは共通鍵を持っているので，メッセージを否認されても，新しいカウンタ値で再送できる(**図3**)。

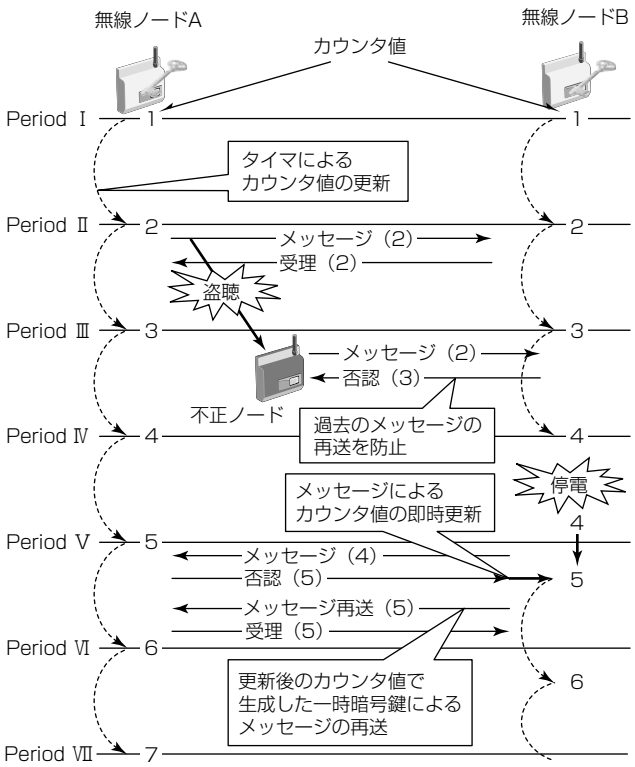


図3．一時暗号鍵の同期と更新

4. むすび

無線メッシュネットワークシステムの制約条件とセキュリティ要件，そして当社における安全性と低リソースの両立を指向したセキュリティ対策技術について述べた。この技術によって，安全性を確保しつつ無線ノードの小型化，低コスト化が可能となり，防災・社会インフラ分野への無線メッシュネットワークの適用範囲拡大を通じて，地球環境及び社会へのより一層の貢献が実現できるものと考える。

今後も，当社が保有する情報セキュリティ技術と無線通信技術の融合によって，防災・社会インフラ分野を支える次世代システムの実現にむけた技術開発を継続する。

参考文献

(1) 嶋田　博，ほか：スマートグリッドを支えるネットワーク技術，三菱電機技報，**86**，No.2，134～138（2012）
(2) 三菱電機 ニュースリリース2011年2月16日：スマートグリッド実証実験「自動検針用無線メッシュネットワーク技術」
http://www.mitsubishielectric.co.jp/news/2011/0216-a.html
(3) 独立行政法人 情報処理推進機構：重要インフラの制御システムセキュリティとITサービス継続に関する調査報告書（2009）
(4) NIST：Recommendation for Key Management Part 1：General（Revised），NIST Special Publication 800-57（2007）
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
(5) NIST：Recommendation for Key Management Part 1：General（Revised 3），NIST Special Publication 800-57（2012）
http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
(6) ISO/IEC：ISO/IEC 18033-3 Information technology-Security techniques-Encryption algorithms-Part 3：Block ciphers（2010）
(7) CRYPTREC：電子政府推奨暗号リスト
http://www.cryptrec.go.jp/list.html（2003）
(8) 三菱電機 ニュースリリース2005年5月26日：128ビットブロック暗号アルゴリズム「Camellia」がISO国際標準規格に採用
http://www.mitsubishielectric.co.jp/news/2005/0526-c.html
(9) NIST：Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality，NIST Special Publication 800-38 C（2004）