2W-01

RPLにおける自律ノードに基づいたセキュア通信方式の提案

小山 峻矢† 中村 嘉隆† 稲村 浩†
公立はこだて未来大学† システム情報科学部†

1. はじめに

現在，低消費電力センサ機器の開発や無線通信技術の進歩により，IoT サービスの普及を始めとするセンサネットワークの利用が進められている．その規模は非常に大きく，2020 年には 500 億台のデバイスが接続され，様々な分野において利活用されることが予想されている[1]．

その一方で，センサネットワークにIPを導入する際に，通信機器の処理性能や通信環境に対して厳しい条件を求めるネットワークが存在する場合がある．それらはLLN(Low power and Lossy Network)と呼ばれ，省電力性や低CPU性能，少メモリなどの計算資源の限られた通信機器と低通信帯域及び高パケット損失率といった低品質な通信環境が求められる．

IETF はこのような特殊な環境下に対応するための案の 1 つとして，RPL(IPv6 Routing Protocol for Low Power and Lossy Networks)と呼ばれるルーティングプロトコルを標準化している[2]．RPL は ZigbeeIP(920IP)や Wi-SUN などの多くの通信方式の構成要素としても取り入れられており，LLN を構築する上の中心技術としてスマートグリッドやスマートファクトリーを始めとする様々な環境での利用が想定されている．

このようなRPLの利用を前提とした通信方式が普及していくと予想される一方で，センサネットワーク上でやり取りされる貴重な情報資産を狙った不正アクセスなどの攻撃も顕在化している[3]．しかし，同通信方式に対する研究の大部分は，そのネットワーク構築に関わるものであり，セキュリティに関する議論は十分にされていない．また前述した LLN の特性により従来のセキュリティ技術を適用することは困難である．

そこで本研究では，RPL において認証付き暗号による共通鍵暗号方式を基盤とした LLN に適応するセキュア通信方式の提案を行う．計算資源の限られたノードを配慮することに加え，セキュア通信による通信オーバヘッドを削減することを目的とした設計を行っていく．

2. 関連研究

2.1 RPL

RPL とは LLN に向けて策定されたルーティングプロトコルであり，トポロジーとしてシンクノードの設置を前提とした DODAG(Destination Oriented Directed Acyclic Graph)と呼ばれるシンクノードに向けた閉路の有向グラフを構築し，マルチホップ通信への対応，通信品質やノードの状態に応じた経路構築などが可能となっている．DODAG におけるシンクノードは DODAG root と呼ばれ，通常子ノードと比較して十分に優れた計算資源を保有している．また，RPL は多様なアプリケーションの要求に応えるため，複数ノードから 1 つのノードへ向けた MP2P(Multi Point to Point)通信，1 対 1 のユニキャスト通信である P2P(Point to Point)通信，1 つのノードから複数へのマルチキャスト通信に対応する P2MP(Point to Multi Point)通信をサポートした設計となっている．

2.2 認証付き暗号

認証付き暗号とは，メッセージの機密性保持及び認証を1つの鍵で同時に行うことができる暗号モードの1種であり，CWC モードや OCB モードが代表する[4]．CBC モードなどのブロック暗号と比較して，メッセージの伸長が僅かであることや復号処理を並列処理できるため，不安定なパケット到着順序の影響を受けないこと，また鍵管理の簡易化といった LLN に適応する利点を得ることができる．

3. 提案手法

本研究では，認証付き暗号による共通鍵暗号方式を基盤としたセキュア通信方式の提案を行う．次節で述べる前提条件のもと，DODAG root が負荷処理の多くを担う設計とすることで，処理性能が制限される子ノードへの負担軽減を図る．また，完全性を保つための認証付き暗号のパラメータとして通信上でやり取りされる Initialization Vector（初期化ベクトル，IV）を圧縮することで，ペイロードの圧迫を削減する．なお，ここでは想定される通信パターンのうち，センサデータの集約など特に利用頻度の高いとされる MP2P 通信と P2P 通信のみに対応する．

3.1 前提条件

本提案方式の前提条件として，以下を満たすものとする

- DODAG root は十分に信頼できる機関である
- DODAG root は十分な計算資源を持つ
- DODAG root を除くノード（子ノード）は計算資源が制限される

十分な計算資源とは，LLN において高負荷とされる処理に対して受容可能な処理速度と，子ノード数に応じた複数の鍵を保有するのに十分な記憶領域，また長期的に運用可能な電源を保持していることとする．

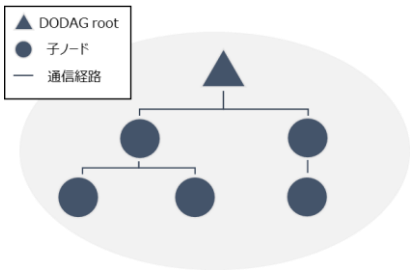

図 1. ネットワーク構成例

3.2 新規ノード参加時の動作

DODAG root と新規ノードは，新規ノードごとに異なるマスタ鍵M_xを共通鍵として共有する．その後，両ノードが共有する疑似乱数関数（PRF）とマスタ鍵から，通信方向に合わせたセッション鍵の生成を行う．例えば，DODAG root A と子ノード B 間のセキュア通信を実現する際には，マスタ鍵M_{AB}から PRF を用いて，セッション鍵$S_{A\to B}$と$S_{B\to A}$の計 2 つを生成する．セキュア通信時には，このセッション鍵を用いて平文を暗号化する．

“A Secure Communication Method Based on the Autonomous Node in RPL”
Shunya Koyama†, Yoshitaka Nakamura†, Hiroshi Inamura†
† School of Systems Information Science, Future University Hakodate

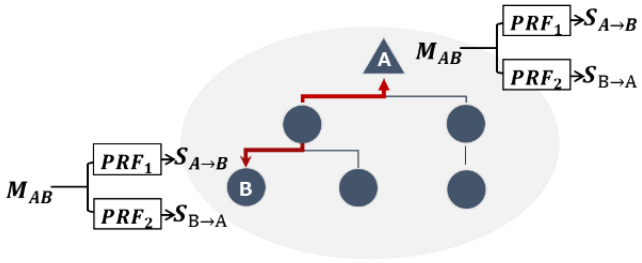

図 2. セットアップ作業

3.3 MP2P 通信及び P2P 通信への対応

3.3.1 IV の設定

認証付き暗号化及び復号に用いられるパラメータの IV には，カウンタ値を利用する．カウンタ値とは，あるセッション鍵による暗号化を行ったパケット数のことを指す．ここで，パケット損失によるノード間の IV の同期漏れを防ぐため，カウンタ値全体をメッセージに含めることは，ペイロード圧迫の観点から LLN に不適である．そこで，完全なカウンタ値はノード内に保管し，下位 N ビットのみをメッセージに含めることとする．これにより，カウンタ値をCntとすると$\log_2 Cnt+1-Cnt$（但し，$\log_2 Cnt+1>Cnt$）ビットのペイロード圧迫を削減することができる．

また，2^N回以上連続してパケットの損失をした場合は，連続パケット損失前後での IV の区別が困難となる．そこで，一度 IV を完全に同期するために，セッション鍵$S_{A→B}$を用いたメッセージ認証コード(MAC)とノンスN_Aを利用して次のようなメッセージを送ることとする．

$$[\text{メッセージ}]\ \mathrm{A}\rightarrow\mathrm{B}:\langle Cnt\,|\,MAC(Cnt|\,N_A)_{S_{A→B}}\rangle$$

上記の例では，DODAG root A と子ノード B 間の通信において，B がカウンタ値に不整合があることを検知し，正しいカウント値を DODAG root A に要求する場合を示している．N_Aは子ノード B が不整合を検知した時点で A に送信され，リプレイ攻撃への対策として用いる．

3.3.2 DODAG root と子ノード間通信

新規ノード参加時に生成された鍵と，認証付き暗号を用いてメッセージの機密性と完全性を確保する．この時，前述したカウンタ値（Cnt）と完全性を検証する認証タグ(MAC)がメッセージに付加される．結果として，例えば DODAG root A が子ノード B に送るメッセージは，平文をMとすると以下のようになる．

[メッセージ]

$$\mathrm{A}\rightarrow\mathrm{B}:\langle Enc\{M\}_{S_{A→B}}\,|\,Cnt_{N_{bit}}|\,MAC(Enc\{M\}_{S_{A→B}})\rangle$$

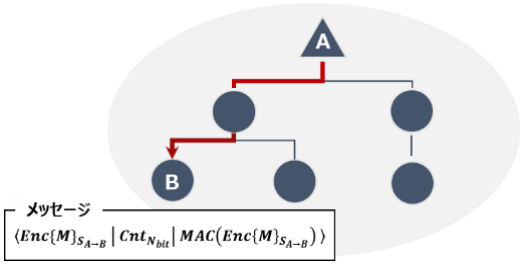

図 3. DODAG root と子ノード間通信

3.3.3 子ノード間通信

DODAG root は各子ノード全てに対応する複数のマスタ鍵Mを保有しているため，どの子ノードに対してもセキュア通信を行うことが可能である．しかし，子ノードはリソース制約により全ノードに対応する複数のマスタ鍵を保有することは困難であるため，セキュア通信は DODAG root との間に限られる．そこで，子ノード間通信に関しては，一度 DODAG root を経由する通信方式をとることとする．

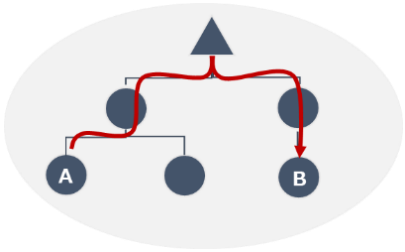

図 4. 子ノード間通信

4. 評価実験

ContikiOS 上に提案方式を実装し，同 OS 上にバンドルされるセンサネットワーク向けネットワークシミュレータ Cooja を用いて評価を行う[5]．

評価項目として，共通鍵暗号方式におけるブロック長や暗号アルゴリズムごと，また通信品質とカウンタ値の設定ビット数による各ノードに掛かる負荷(消費電力，RAM 使用率など)を検討している．これらの評価値から本研究の有効性を検証する．

5. おわりに

本研究では，RPL において認証付き暗号による共通鍵暗号方式を基盤とした MP2P 通信及び P2P 通信に対応するセキュア通信方式の検討を行った．これにより，計算資源の限られた通信機器と低品質な通信環境で構成される LLN に適応することが期待される．しかし，P2MP 通信への対応や，DoS 攻撃などによる可用性を狙った攻撃への防御は行えていない．また，カウンタ値の設定ビット数においては，RPL でやり取り通信品質などの情報から最適値を求めることが可能であると考えられる．今後は，これらの問題について提案手法の改善を検討していく．

6. 参考文献

[1]. Cisco, “How the Next Evolution of the Internet Is Changing Everything,” 2013.

[2]. T. Winter, P. Thubert, et al., “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” RFC6550, 2012.

[3]. D. Airehrour, et al., “Secure Routing for Internet of Things: A survey,” JNCA 66, vol. 1, pp. 404-412, 2016.

[4]. 情報処理推進機構(IPA), “ブロック暗号を使った秘匿，メッセージ認証，及び認証暗号を目的とした利用モードの技術調査報告,” <http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/documents/mode_wg040607.pdf>, 2013.

[5]. “Cooja Simulator,” <http://anrg.usc.edu/contiki/index.php/Cooja_Simulator>