920MHz帯省電力無線センサーネットワークにおけるネットワークアクセス認証時間のフィールド評価

土江　康太　　八百　健嗣

OKIは、920MHz帯無線センサーネットワーク（Wireless Sensor Networks（以下、WSNと略す））を利用して、橋梁等の社会インフラの老朽化や崖崩れ等の災害を監視するシステムを実証している。これらのシステムでは、電源の敷設工事が困難であるため、電池で長時間動作する無線センサーモジュール（以下、ノードと呼ぶ）が必要になる。またWSNでは、第３者による侵入が容易な無線通信を利用するため、セキュリティー対策も必要になる。特に上述のシステムでは、誤った障害情報や災害情報が投入されると、利用者の混乱を招くだけでなく、システム全体の信頼性が失われる恐れがある。

不正な第３者によるWSNへの侵入を防ぐセキュリティー技術としてネットワークアクセス認証が有効である。しかし、省電力化のため間欠動作するWSNでは、ネットワーク構築時間の増加が問題になる。可用性が重視されるシステムでは、ネットワーク構築時間も重要な要件となるため、省電力WSNにおけるネットワークアクセス認証は、安全性確保だけでなく、ネットワーク構築時間の短縮が重要になる。

本稿では、情報通信研究機構殿保有のテストベッド環境を活用したネットワークアクセス認証方式の性能評価結果を報告する。

ネットワークアクセス認証

ノードはWSNに加入する際、加入先のネットワークとの間で互いの正当性を検証する。正当性を検証する手続きは、ネットワークアクセス認証と呼ばれる。ネットワークアクセス認証では、一般に秘密情報が用いられ、秘密情報の1つにPSK (Pre-Shared Key)がある。PSKは、認証するノード間で共有する秘密の鍵情報であり、互いに同じPSKを所有することを検証する。

PSKは、一般にノードと基地局との間で共有され、共有されるPSKは、全てのノードで共通である場合（以下、共通PSKと呼ぶ）とノード毎に異なる場合（以下、個別PSKと呼ぶ）がある。共通PSKは、いずれかのノードのPSKが漏えいすると、そのノードだけでなく他のノードにもなりすまして不正アクセスされる恐れがある。一方、個別PSKは、いずれかのノードのPSKが漏えいしたとしても、他のノードのPSKは秘密に保たれるため、共通PSKを使用するより安全性が高い。

また、ネットワークアクセスの認証方式にも主に２つの方式があり、1つは基地局で認証する集中認証方式であり、もう1つはネットワーク加入済みの隣接ノードで認証する分散認証方式である。集中認証方式では、全ての参加ノードが基地局と認証するため、例えばノードが一斉にネットワークに参加しようとした場合、認証トラフィックが基地局周辺に集中し、メッセージの衝突や無線チャネルの混雑が生じ、ネットワーク構築に時間がかかる恐れがある。一方、分散認証方式では、参加ノードは隣接ノードと認証するため、メッセージの衝突や無線チャネルの混雑が抑制され、ネットワーク構築時間を短縮できる効果が期待できる。前述の個別PSKは、参加ノードと基地局でのみ共有されるため、集中認証方式をとる必要がある。一方、共通PSKは、全ノードが同じPSKを所有するため、分散認証方式をとることができる。

以上より、個別PSKを用いた集中認証方式では、安全性は担保されるが、ネットワーク構築に時間がかかる恐れがある。一方、共通PSKを用いた分散認証方式では、PSK漏えいの観点で安全性にデメリットがあるが、ネットワーク構築時間を短縮できる見込みがある。つまり、PSKの安全性とネットワーク構築時間はトレードオフの関係にある。本稿では、分散認証方式と集中認証方式の２つの認証方式を開発し、各認証方式のネットワーク構築時間を定量的に比較する。

関連研究と課題

WSN規格の1つであるZigBee*1) IP[1] では、集中認証方式を採用する。ZigBee IPでは、認証の秘密情報にPSKまたは証明書が利用される。また、分散認証方式として、IDベース暗号方式を用いた方式がある[2]。

以上のように、ネットワークアクセス認証方式として集中認証する方式や分散認証する方式は以前より提案さ

＊1）ZigBee は、ZigBee Alliance の登録商標です。

れてきた。しかし、PSKを前提として、2つの認証方式のネットワーク構築時間を実フィールド環境で評価・比較した事例は見当たらない。

ネットワークアクセス認証の実装方式

本稿におけるネットワークアクセス認証の実装方式は、PSKを使用した4メッセージのチャレンジ・レスポンス認証方式である。実装方式の処理シーケンスを**図1**に示す。**図1**において、認証相手は、分散認証方式ではネットワーク加入済みの隣接ノードであり、集中認証方式では基地局である。$Addr_A$、$Addr_B$は、それぞれ参加ノードと認証相手のMACアドレスを表し、r_A、r_Bは乱数値である。また、MIC (Message Integrity Code) (MIC_A、MIC_B) は、HMAC (Hash-based Message Authentication Code)[3] で生成され、第1引数が認証するメッセージ、第2引数が鍵情報を表す。HMACの第1引数に含まれる記号 (||) は文字列の連接記号を表す。

本実装方式では、はじめに認証する主体の間で乱数値を交換する。次に交換した乱数値、MACアドレス、および共通のPSKからMICを生成し、交換する。MICを受信すると、受信側も同じ手順でMICを生成し、受信したMICと一致するかが検証される。

本実装方式で生成されるMICは、正しいPSKを所有しない限り生成できないため、不正なノードのなりすましを防ぐことができる。さらに、乱数とシーケンス番号を認証するメッセージに含めるため、リプレイ攻撃にも耐性がある。また本稿では詳細は省略するが、認証に成功すると、認証したノードの間でのみ共有される暗号鍵（リンク鍵と呼ぶ）が生成される。生成されたリンク鍵は、ネットワーク加入シーケンスで利用される。

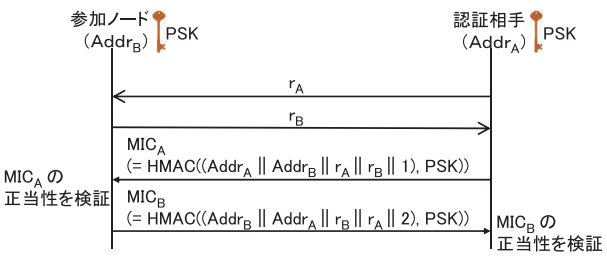


図１　ネットワークアクセス認証実装方式のシーケンス

ネットワークアクセス認証の実装方式

ノードのハードウェアは、OKIの920MHz帯マルチホップ無線ユニット[4] を使用する。ノードは、マルチホップで通信する。マルチホップ通信では、ノードは、基地局と直接無線通信できないノードの送信メッセージを、当該ノードに代わり基地局に中継する。またノードは、スリープ制御により間欠動作する。スリープ制御では、ノードは基本スリープ状態にあり、一定間隔でアクティブ状態となりデータを送受信する。本評価では、ノードは、間欠動作周期100msで動作する。また間欠動作するノード間は、CSL (Coordinated Sampled Listening)に準拠した方式で通信する[5]。

参加ノードのネットワーク加入シーケンスを**図2**に示す。**図2(a)**は分散認証方式によるシーケンスを表し、**図2(b)**は集中認証方式によるシーケンスを示している。

参加ノードは、はじめに親ノードを選択する。親ノードを選択するため、参加ノードはNwkInfoRequestをブロードキャストし、これを受信した近隣ノードはNwkInfoを応答する。参加ノードは、受信したNwkInfoの中から1台を親ノードに選択する。続いて参加ノードは、親ノードにJoinRequestを送信する。

ここからのシーケンスは、各認証方式で異なる。分散認証方式では、親ノードと参加ノードとの間で**図1**のネットワークアクセス認証が実行される。集中認証方式では、JoinRequestは基地局まで中継され、基地局と参加ノードとの間で認証が実行される。

認証に成功した場合、認証相手からデータ通信に使用する暗号鍵データがリンク鍵で暗号化されて送信され、参加ノードは認証相手に受信応答を返信する。最後に基地局からJoinResponseが参加ノードに送信され、参加ノードはこれを受信しネットワーク加入状態となる。

参加ノードは、認証メッセージ送信後、一定時間待っても応答を受信できなかった時に送信メッセージを再送する。再送間隔は、分散認証方式で式 (1) 、集中認証方式で式 (2) として定義される。

$$RTT_{oneHop} = \{sleepCycle \cdot (reSend + 1) + rand\} \cdot 2 \cdot 2^{reTry} \quad (1)$$

$$RTT_{multiHop} = (1) \cdot (1 + hop) \quad (2)$$

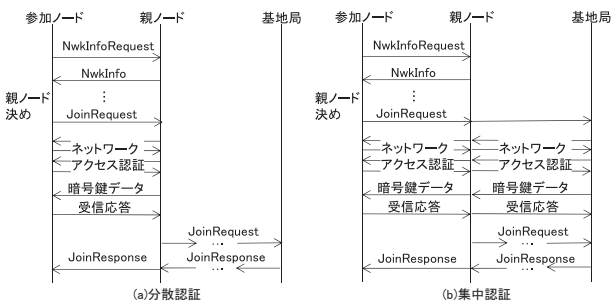


図2　WSN加入シーケンス

式 (1) および式 (2) は、参加ノードと認証相手との間の最大ラウンドトリップ時間を表している。ここで、*sleepCycle*はノードの間欠周期、*reSend*はMAC層での再送回数（本評価では3回とした）、*hop*は親ノードから基地局までのホップ数をそれぞれ表している。また、*rand*は0から0.2秒までの乱数値、*reTry*はMAC層の上位層で認証メッセージを何回再送したかを表しており、再送間隔はネットワークの輻輳を考慮してノード毎にばらつくようになっている。本評価では、認証メッセージを3回再送しても応答を受信できなかった場合には、参加ノードはNwkInfoRequestの送信からやり直す。

式 (1) および式 (2) より、再送間隔は再送の度に指数関数的に増加していくため、ノードのネットワーク加入にかかる時間は、再送回数に比例して増加する。

評価環境と評価内容

本評価は、情報通信研究機構殿保有のテストベッド環境で実施する。本環境は基地局を含め50台のノードからなる。**図3**は、各ノードが実フィールド上にどのように配置されているかを示している。**図3**では、ノードは丸印で示され、ノード間を繋ぐ線が無線リンクを表している。本環境では、最大ホップ数が5～7ホップとなるマルチホップネットワークが形成される（**図3**は5ホップの例を表している）。基地局とノードの設置例を**写真1**に示す。**写真1(a)**は基地局の設置例であり、屋内に設置され、ゲートウェイ装置と接続する。ゲートウェイは、本WSNを管理するLinux装置[6]である。**写真1(b)**はノードの設置例であり、外部センサーと共に筐体の中に入れられ、屋外に設置されている。

本評価では、基地局および全ノードを一斉起動した時のネットワーク構築時間（基地局を含め50台のノードがネットワークに加入するまでの時間）を測定する。ここでノード1台当りのネットワーク加入時間は、**図2**のシーケンス全体にかかった時間として評価する。

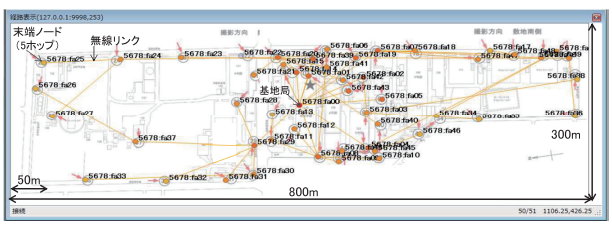
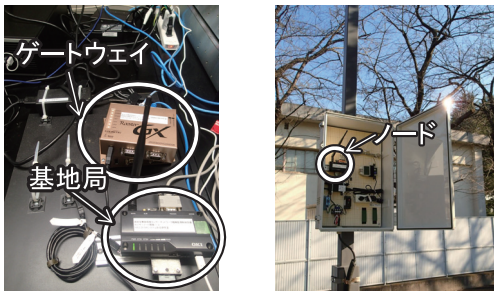


図 3　テストベッド環境



(a)基地局とゲートウェイ　(b)ノード

写真1　設置例

評価結果

分散認証方式および集中認証方式のネットワーク構築時間の測定結果を**図4**に示す。**図4**は、ネットワーク構築を10回試行した内の平均値と最大値を示している。**図4**の横軸はノードを一斉起動してからのネットワーク加入台数を表し、縦軸は基地局がネットワーク加入状態になってからの経過時間を表している。

図4より、各認証方式のネットワーク構築時間の平均値では、分散認証方式は集中認証方式と比較して約29%ネットワーク構築時間が短縮された。また最大値でも約30%ネットワーク構築時間が短縮された。これは、集中認証方式では、基地局周辺に認証トラフィックが集中したことでメッセージロスが発生し、参加ノードが認証メッセージを再送しネットワーク加入時間が増加したのに対して、分散認証方式では、基地局周辺の認証トラフィックが抑制され、ノードの再送回数が減りネットワーク加入時間が減少したためと考えられる。

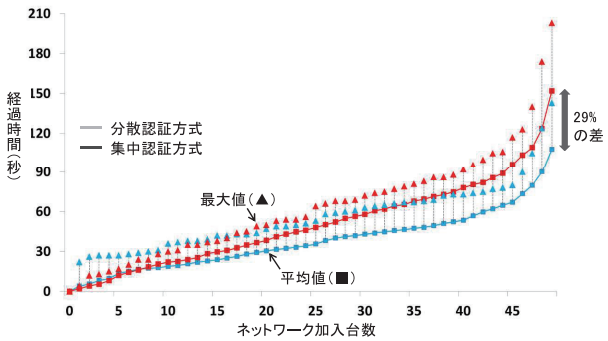


図 4　ネットワーク構築時間の測定結果

各認証方式のメッセージロス数とメッセージ送受信数の比較結果を**図5**、**図6**を用いて説明する。**図5**、**図6**は、10回試行した内の各ノードにおける最多メッセージ数を示している。

図5は、各ノードにおけるメッセージロス数を示している。図5より、集中認証方式では、基地局周辺（特に基地局の右上に位置するノード）でメッセージロスが多発し、輻輳が発生したことが確認された。一方、分散認証方式では、基地局周辺のメッセージロス数が削減され、輻輳が抑制されたことが確認された。

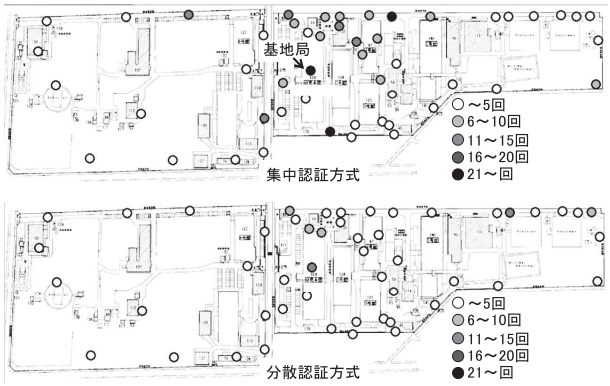


図5　各ノードにおけるメッセージロス数

図6は、各ノードのメッセージ送受信数を示している。図6より、集中認証方式は、基地局周辺のノードのメッセージ送受数が分散認証方式より大幅に多いことが分かる。ここで、基地局周辺の6台のノードのメッセージ送受信数に着目すると、分散認証方式は集中認証方式より最大で90%少ないことが分かり、基地局周辺ノードの省電力効果が確認された（図6の右下の棒グラフ）。

以上より、分散認証方式は、集中認証方式と比較して、PSKの安全性の面でデメリットはあるものの、ネットワーク構築時間や通信量の抑制による省電力化の観点で利点があることを実フィールド評価により確認できた。

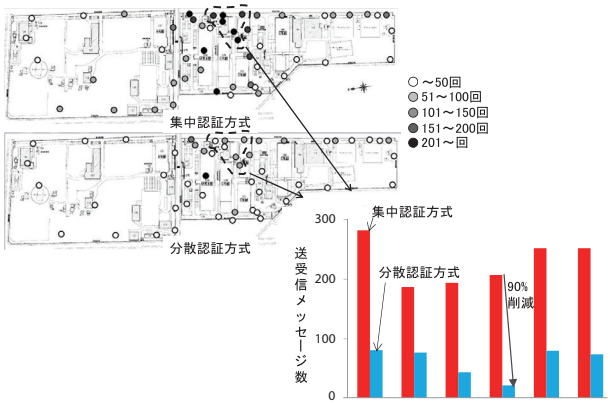


図6　各ノードにおけるメッセージ送受信数

まとめ

本稿では、WSN向けのネットワークアクセス認証方式として、分散認証方式と集中認証方式の2つの方式のネットワーク構築時間を、実環境で定量的に比較した。

ネットワーク構築時間を増加させる別の要因に、参加ノードの親ノード選択がある。今後は、親ノード選択時間を短縮する方式を開発し、各認証方式のネットワーク構築時間の更なる短縮を目指す予定である。

謝辞

本研究開発は、国立研究開発法人情報通信研究機構との共同研究「無線センサーネットワークの監視制御技術」により実施したものである。◆◆

■参考文献

1) ZigBee Alliance:Zigbee IP Specification,ZigBee Document 095023r31, January 2013.
2) A. Al-Mahmud, and R. Akhtar:Secure Sensor Node Authentication in Wireless Sensor Networks,International Journal of Computer Applications, Vol. 46-No. 4, pp.10-17, May 2012.
3) H. Krawczyk, M. Bellare, and R. Canetti: "HMAC: Keyed-Hashing for Message Authentication", RFC2104, February 1997.
4) 920MHz帯マルチホップ無線ユニット、http://www.oki.com/jp/920M/mh/unit/、（2017年2月9日）.
5) 野崎、他：無線マルチホップ技術を用いた社会インフラモニタリングシステム、OKIテクニカルレビュー第226号、2015年12月.
6) サン電子：GX110、http://www.sun-denshi.co.jp/sc/gx110/、(2017年2月9日).

●筆者紹介

土江康太：Kota Tsuchie. 情報・技術本部 研究開発センター スマートネットワーク技術研究開発部
八百健嗣：Taketsugu Yao. 情報・技術本部 研究開発センター スマートネットワーク技術研究開発部