1Y-9

無線小型デバイスにおける暗号化通信

橙 幸宏† 芝 公仁† 岡田 至弘†
†龍谷大学理工学部

1 はじめに

近年，無線センサデバイスを用いた環境モニタリングが行われるようになってきている．これは，無線センサデバイスは設置場所の制約が少なく，また，広い範囲をモニタリングすることが可能になる等の利点があるためである．

しかし，無線通信を用いるため，悪意のある者からの傍受，改竄，なりすましによってシステムの安全性が損なわれる可能性がある．本稿では，無線センサデバイスの認証による安全なデータ伝送が可能である環境モニタリングシステムを提案する．以下に本システムの特徴を示す．

- 暗号化通信を用いてセンシングデータの送受信を行う
- 無線通信において互いに認証を行う
- 少ない計算機資源で動作可能である

悪意のある者が盗聴しても通信内容を理解できないようにする．無線センサデバイスが保持している鍵のペアを持つ無線センサデバイス以外が理解できないように，すべての通信を暗号化する．

基地局と無線センサデバイスの通信を改竄やなりすましから守るために認証を行い，安全なデータ伝送が可能になる．無線センサデバイスが証明書より軽量な送信データのハッシュ値と受信データのハッシュ値の比較を行い，改竄を検知する．また，受信したデータの送信者のなりすましを検知する．

無線センサデバイスは使用できるメモリ量が少なく，演算能力も低いことが多い．本システムはこのような環境でも安全に通信を行うことができる．本研究では，組み込みデバイスで用いられることの多い J2ME 環境に本システムを実装し，動作することを確認した．

2 システムの構成

本章では無線センサデバイス間の認証，および，安全なデータ伝送を行う環境モニタリングシステムの構成を述べる．本システムは，施設の管理者が施設内を見回りながら無線センサデバイスの付近に移動し，センシングデータを回収する環境を想定している．本システムは，サーバ，ゲートウェイ，デバイスから構成されている．全体の構成図を図 1 に示す．サーバは，ゲートウェイが回収したデバイスのセンシングデータの保存やゲートウェイと通信する役割を果たす．ゲートウェイは，施設の管理者がサーバと一緒に施設内を見回りながら，近くのデバイスと通信する際，サーバとデバイスは直接通信することができないため，その間に入り，要求を受け渡す．デバイスは，センシングデータの取得，そのデータの蓄積，ゲートウェイと通信する役割を果たす．

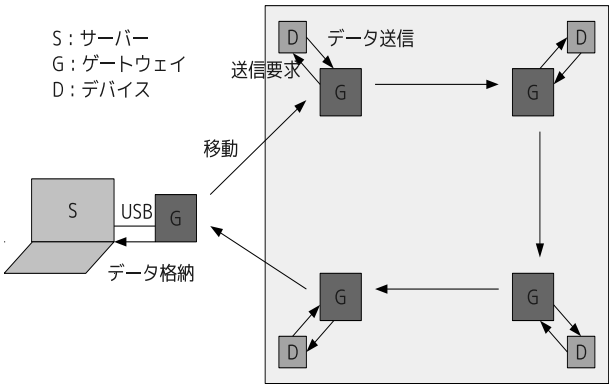

図 1 提案システムの構成図

サーバは，ゲートウェイとの通信機能，ゲートウェイとデバイスのアドレスを管理する機能，また暗号化通信に用いる秘密鍵（以下 SK とする）を持つ．ゲートウェイは，サーバ，デバイスとの通信機能を持つ．デバイスは一定時間毎に環境情報をセンシングする機能，ゲートウェイとの通信機能を持つ．また暗号化通信に用いる公開鍵（以下 PK とする）を持つ．

ゲートウェイとデバイスは無線で通信をするため，暗号化，認証を行い安全性を実現する．

3 システム動作

ゲートウェイがデバイスとの通信を安全に行なうために，送信するデータとそのハッシュ値，および現在時刻を暗号化し，デバイスに送信する．暗号化された送信データとそのハッシュ値，および現在時刻は暗号化した暗号鍵の対になる復号鍵を持つデバイスのみ正しく復号化を行える．デバイスが復号化したハッシュ値と受信したデータのハッシュ値を比較する．比較したハッシュ値が一致すれば通信を行う通信相手と認証できる．また，現在時刻をこれまでに受信した時刻と比較することで，これまでに同じ受信データが到着し

Encrypted Communication in Environmental Monitoring with Wireless Devices
Yukihiro Daidai†, Masahito Shiba†and Yoshihiro Okada†
†Faculty of Science and Technology, Ryukoku University

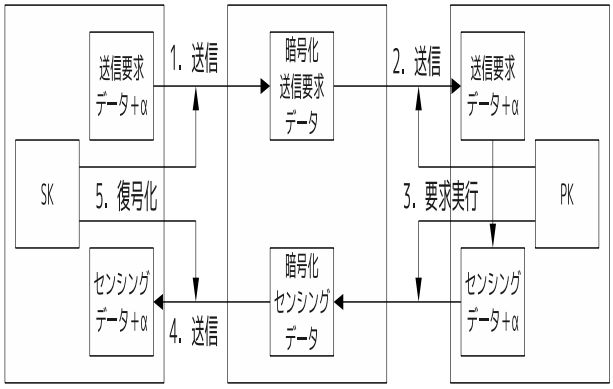

図 2　全体のデータ遷移図

ていないかの検証も行う．新しい現在時刻であれば以前受信したデータを再び受信していないとして取得する．この処理は攻撃者が暗号化されたパケットを記録し，そのパケットを送信する攻撃に対処できる．復号化や認証に問題がなければ，デバイスが保存しているセンシングデータをすべてゲートウェイに送る．その場合も上記と同じ様に暗号化，および認証を行う．

図 2 に，サーバとデバイスがお互いに認証し，通信内容の暗号化を行う流れを示す．図 2 で行う手順を以下に示す．

(1) サーバが暗号鍵を生成する機構で秘密鍵（SK）を生成し，送信要求データ，送信要求データのハッシュ値を SK で暗号化し，それをゲートウェイに送信する．
(2) ゲートウェイがサーバから，デバイスのセンシングデータを取得するという要求を受け，サーバから送られてきたデータをデバイスに送信する．
(3) デバイスが暗号鍵を生成する機構で公開鍵（PK）を生成する．そして受信したゲートウェイからの暗号化されたデータ，そのハッシュ値を PK で復号化する．また復号化した受信データのハッシュ値と受信したハッシュ値の検証を行う．ハッシュ値が一致すれば，センシングデータを送信する．デバイスがセンシングデータ，そのハッシュ値，現在時刻を PK で暗号化する．そして暗号化したセンシングデータ，そのハッシュ値，現在時刻をゲートウェイに送信する．
(4) ゲートウェイがデバイスから受信したセンシングデータ，そのハッシュ値，時刻をサーバに送信する．
(5) サーバが暗号化されたセンシングデータ，そのハッシュ値，現在時刻を SK で復号化する．そしてサーバが復号化したハッシュ値と復号化したセンシングデータのハッシュ値を比較する．

(2) では復号化した送信要求のハッシュ値と，復号化したハッシュ値が一致すれば PK と対の SK を持つサーバと認識する．ハッシュ値が一致しなければ PK と対の SK を持たないサーバと認識して送信要求に応じない．(4) でも (2) と同様に復号化したセンシングデータのハッシュ値と，復号化したハッシュ値が一致すれば SK と対の PK を持つデバイスと認識する．ハッシュ値が一致しなければ SK と対の PK を持たないデバイスと認識してすべての受信データを破棄する．

4　議論

無線センサネットワークで安全なデータ伝送を行うためには盗聴，改竄，なりすましからセンシングデータ等を守る必要がある．

4.1　前提条件

本システムは次の条件を満たすとき安全にセンシングデータを送受信することが可能である．

- ゲートウェイは耐タンパ性を有する
- サーバとゲートウェイ間の通信は信頼できる

デバイスはセンシングデータをゲートウェイを経由してサーバに送信する．ゲートウェイが盗難されると，デバイスから環境情報を通常の手順で取得でき，センシングデータの盗聴が可能になるためゲートウェイは耐タンパ性を有する．サーバとゲートウェイ間の通信が信頼できないと，ゲートウェイからサーバにデータを送る際に改竄が可能になるためサーバとゲートウェイ間の通信は信頼できるとする．サーバとゲートウェイ間の通信は USB ケーブルを使い通信を行うため安全にデータ伝送が行なえる．

4.2　本システムで行う攻撃に対する対処

公開鍵暗号方式を用いて通信内容を暗号化しているため，第三者は内容を知ることができない．送信するデータとそのハッシュ値を送信するデータに付加し送信することで，通信データが変更された場合，受信者が受信したデータのハッシュ値と，付加されたハッシュ値を用いることで改竄を検知できる．また，なりすましを行う攻撃者は公開鍵，および秘密鍵のどちらかを手に入れなければデバイス，ゲートウェイのどちらとも通信を行えない．

5　おわりに

本稿では，認証による安全なデータ伝送を可能にしたシステムについて述べた．本システムを用いることで，安全なデータ伝送が可能になり，どのような場所でも安全なモニタリングを構築できる．

参考文献

[1] 山口 登: 通信回数を削減した環境モニタリングシステムの実装, *USN,* **ユビキタス・センサネットワーク，** *Vol．108*，*No．399* , 111–116 (2009).