【 無線センサ網におけるパラメータと経路の適応的設定が可能な秘密分散法に基づく暗号化セキュア情報転送 】

【 研究キーワード：ネットワークセキュリティ，無線センサネットワーク，IoT，秘密分散法，複数ゲートウェイ 】

情報科学研究科 情報工学専攻　　准教授 河野 英太郎 Eitaro KOHNO

【研究分野 ネットワークセキュリティ、計算機システム・ネットワーク、通信・ネットワーク工学】

研究シーズの概要

端末への計算資源やバッテリ容量などへの制約が大きい無線通信において、有線通信と比べて難しいデータや暗号鍵の漏洩等の問題を解決する手法の研究を進めています。これまでに、秘密分散法を応用し、端末が不正に乗っ取られた場合等のデータ転送時の窃取や無線の盗聴等に対し安全性を向上させる手法を提案しています。

研究シーズの詳細

◆研究例◆

ワイヤレス通信におけるセキュアな通信について研究しています。端末への計算資源，ならびに電源などへの制約が大きいワイヤレス通信において，有線通信と比べて難しくなるデータや暗号鍵の漏洩などの問題を解決する手法について研究を進めています。

特に，IoT(Internet of Things)の一要素として考えられている無線センサネットワークにおいて，これまでに，窃取や漏洩を防ぐため秘密分散法とよばれる手法を応用し，元データを複数の分散されたデータに変換することで，データ転送時の安全性を向上させる方法について提案している．提案法では，端末が攻撃者から不正に乗っ取られるという攻撃を想定しています。それにより，端末の識別子が偽造されてしまうような場合や転送データの窃取があったとしても，そのことを検知したり，重要情報が不正な中継端末に読み取られにくい方式になっています。

◆研究例◆

センサ端末が無線を使って測定した情報を，インターネット上に居るユーザに提供する際にデータを一時的に蓄積しておくゲートウェイを複数用意する際，データを安全にかつゲートウェイの故障が発生した際のバックアップが自動的に取れるようなゲートウェイの配置とデータ転送方式を提案しています。

(a)ユーザ → ゲートウェイ (b) センサ → ゲートウェイ

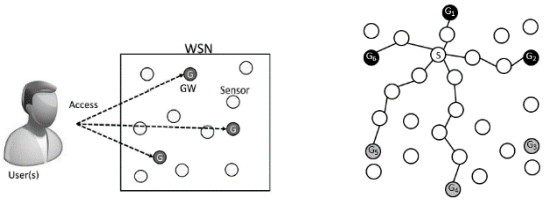

図 1: 提案法の動作イメージ

想定される用途・応用例

◆ IoT に接続されたセンサ端末の転送されるデータの安全性向上
◆ 災害等の情報を検出するセンサ情報を提供するサーバ等の耐故障性向上など

セールスポイント

提案手法は，秘密分散法と呼ばれる従来の秘密鍵・公開鍵のような仕組みを用いることなく転送データの暗号化・復号化が可能です。また，複数のゲートウェイやサーバに対する情報の分散が特殊な機器を用いることなく実現可能であり，その計算負荷も従来の仕組みに比べて軽いものとなっています。

問い合わせ先：広島市立大学 社会連携センター
TEL:082-830-1764 FAX:082-830-1555
E-mail:shakai@m.hiroshima-cu.ac.jp
〒731-3194
広島市安佐南区大塚東三丁目４番１号
（情報科学部棟別館１F）