LCDWSN:
光通信を用いた，セキュアなWSNを構築する手法

グエン　ゾアン　ミン　ザン[†]　　**親：瀧本拓哉**[‡]
spider　　tacky

1.　背景と問題意識

現在，Wireless Sensor Network が普及し，複数の機能のセンサノードで様々なアプリケーションを設置されつつある．例えば，離れて暮らす老人の安否確認を行うアプリケーションや，留守にしている自宅の警備アプリケーションなどが挙げられる．その際，個人的なデータが流れるので，設置される WSN にはセキュリティが必要である．

また，本研究では近い将来センサノードの設置を，WSN に関する知識や経験のないユーザ（エンドユーザ）が行うようになると想定している．そのため，エンドユーザが操作可能な手法でセキュアな WSN を構築可能な手法が必要である．

2.　シナリオ

近い将来，WSN を用いて様々なアプリケーションが設置され，利用されつつある．例えば，泥棒の侵入を検知して，通知するシステム，健康情報を医者に送信して，リアルタイムに診察するシステム．

また，WSN を用いたアプリケーションを家のサーバにインストールし，必要なセンサノードをユーザが購入し設置するようになると想定している．

そうした，セキュアなセンサネットワークをエンドユーザが手軽に構築可能な手法が必要となる．

3.　目的

本研究の目的はエンドユーザが操作可能な手法を用いてセキュアな WSN を構築する手法を提案することである．また機能が異なる複数のセンサノード間でも追加できる．

4.　機能要件

本研究を実現するための要件を３つ述べる．まず，簡単なインタラクションで WSN の構築を可能にすることである．また，異なる機能のセンサノード間でもデータをやり取りできることである．最後にその際に構築する WSN がセキュアな通信を行うことが挙げられる．

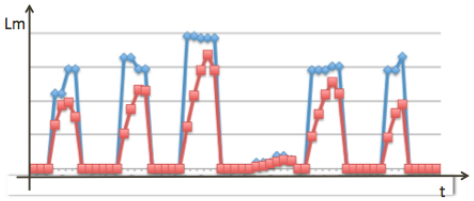
5.　アプローチ

本研究を実現するためのアプローチは３つがある．まず，WSN の構築のインタラクションである．次は，違う機能のセンサノードの追加仕方．最後には，セキュアの設定がある．以下にそれぞれのアプローチについて述べる．

5.1　データ通信

簡単なインタラクションで WSN の構築を可能にするため，近接したデバイス間で LED の点滅パターンを用いてデータの送受信を行う．

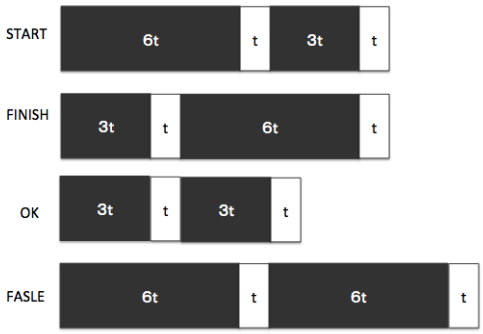
送信された光信号の平滑化のために Gaussian Smoothing アルゴリズムを用いる．



青：スムーズ前
赤：スムーズした後

最小の時間の単位を t で表す (例えば:t=12ms)．送信するデータのビット毎に点滅のパターンと継続時間を変化させてデータを以下の図のように表現する．0 ビットは弱い光で 2t の間光り，t 時間消灯する．また，1 ビットは強い光で t の間光り，2t 時間消灯する．

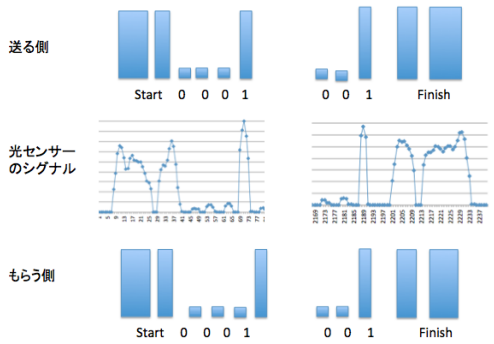
データを送信のため，「START,FINISH,OK,FALSE」の特別の合図を作成した．START は強い光を 6t，t 時間消灯，また強い光は 3t，最後は t 時間消灯を設定する．FINISH は強い光を 3t，t 時間消灯，また強い光は 6t，最後は t 時間消灯を設定する．OK は強い光を 3t，t 時間消灯，また強い光は 3t，最後は t 時間消灯を設定する．FALSE は強い光を 6t，t 時間消灯，また強い光は 6t，最後は t 時間消灯を設定する



[†]慶應大学環境情報学部
[‡]慶應義塾大学, 政策・メディア研究科

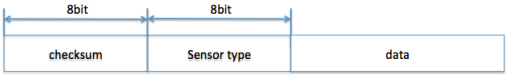
5.1.1 光通信データの結果

実際に光通信を行った結果を下図に示す．128 ビット送信する実験を 69 回行った所，25bit/sec 程の転送速度を示し，データ送信の精度は 85.5 %であった．また，0 ビットと 1 ビットを 928 回ずつ送信した際のビットの精度は 99.5 %であった．



5.2 WSN へのノードの追加方法

コネクタに受信した場合は送信したメッセージの SensorType からセンサノードの機能が判別できる．一方，ノードとコネクタを接地してから，3 秒間コネクタが光パターンを認識しない場合，センサノードが LED を備えていないことが分かる．



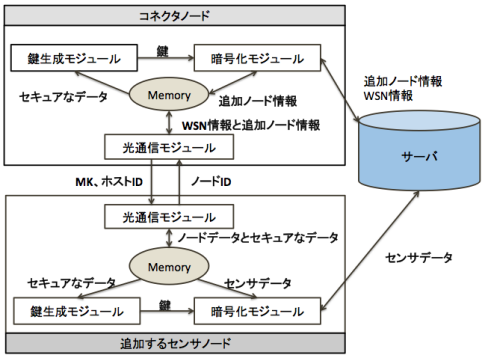
- LED を備えている場合
  WSN から MK をセキュアに受け取れないので，最初の通信でノード ID とそれぞれのノードが持つの仮の鍵をコネクタへ送信することで無線通信でセキュアに MK を受け取る．
- 照度センサを備えている場合
  コネクタから MK とホスト ID を受け取る．そしてノード ID を MK を用いて暗号化して，無線通信でホストに通信する．
- LED と照度センサどちらも備えている場合
  コネクタから光通信で MK とホスト ID とを受け取る．ノードでノード ID を送る．

5.3 セキュアな設定

セキュアな通信を行うために，前節で述べた MK とノード ID とホスト ID の交換後，それらの情報を用いて鍵を生成する．生成した鍵を無線通信データを暗号化する．

$$key = Hash(M|ID_1|ID_2|) \quad (1)$$

6. システム構成図



7. 評価方針

一度のデータ送信で大きなデータを送信するとエーラが増えるので，エーラとデータサイズの相関について定量的に評価を行う．また，20 代の男女 20 名に既存の WSN 構築手法と本研究で提案する手法を用いて，WSN の構築を行ってもらい定性的に評価を行う．

8. まとめ

本研究では照度センサと LED を用いて，センサノードとコネクタがデータ通信が可能にする手法を提案した．また将来的には複数の種類のセンサノードで実装する必要がある．

参考文献

[1] Jun Rekimoto, ”SyncTap: synchronous user operation for spontaneous network connection”, Personal and Ubiquitous Computing, 2004.

[2] Takuro Yonezawa, ”Spot&Snap: An Interaction for Associating Sensor Nodes and Everyday Objects to Realize DIY Smart Object Services”, IPSJ Transactions on Database 48.

[3] Takuro Yonezawa, ”Vib-Connect: A Device Collaboration Interface Using Vibration”, RTCSA, 2011.

[4] Will Archer Arentz, ”Near Ultrasonic Directional Data Transfer for Modern Smartphones”, UbiComp, 2011.

[5] Marcos A. Simpli’cio Jr, ”A survey on key management mechanisms for distributed Wireless sensor networks”, Computer Networks Volume 54.

[6] Roberto Di Pietro, ”Random key-assignment for secure Wireless Sensor Networks”, SASN ’03.

[7] Toshihiko Komine, ”Fundamental Analysis for Visible-Light Communication System using LED Lights”, IEEE Consumer Electronics Society, Feb 2004.