Term プロジェック：
LCDSN:光通信を用いた，セキュアな WSN を構築する手法

spider[†]　　**親：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せつつある．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，設置される WSN にはセキュリティが必要である．

他に複数の WSN を区別して設置のために，使う前に，知識や経験で設置が必要になる．

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と言える．

2.　シナリオ

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，通知するシステムとか，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とかがある．

近い将来，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．

そうした未来において，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．本システムが提案する手法を用いることで，エンドユーザは家庭に様々なアプリケーションを設置可能となる．

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．または複数の機能が異なる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．最後，その際に構築する WSN がセキュアな通信を行うことが可能であることが挙げられる．

5.　アプローチ

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

そして，ノードの機能によって，違い仕方を用いる．

また，WSN でセキュアな通信を行うために，センサノードのペアリング毎に異なる鍵を生成し，データの暗号化を行う．本研究では，ノード ID と MasterKey でハッシュファンクション (1) を用いて一意な鍵を生成する．

5.1　データ通信

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表現する．

0 は弱い光で 2t の間光り，t 時間消灯する．また，1 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．

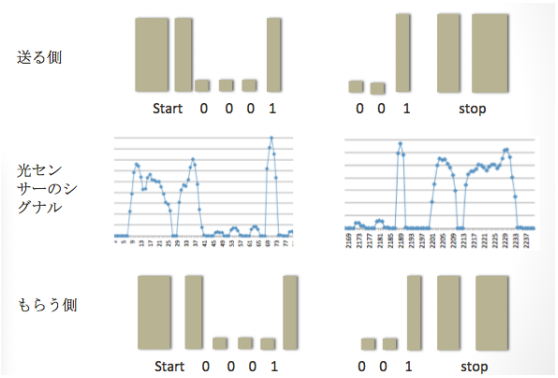
- 通信　：START(6t,t,3t,t),FINISH(3t,t,6t,t)
- チェック：OK(3t,t,3t,t),FALSE(6t,t,6t,t)

START は強い光は 6 t，休憩 t，また強い光は 3 t，最後は休憩 t を設定します．他の合図は同じに設定する．

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．

5.1.1　実装の結果

実際で光パータンの通信は以下の感じになった．



5.2　ノードを追加ステップ

ノードの機能によって，仕方が違う．

- LED だけがある場合はノードで繰り返す自分の ID と仮の鍵を送る，ホストからリクエストを待つ．後に仮の鍵で暗号化して，MasterKey とホスト ID を通信する．
- 照度センサだけがある場合は，コネクタで繰り返すホストの ID とネットワークの MasterKey を送る，ホストでノードのリクエストも持つ．後に MasterKey で暗号化し，通信でノードの ID を確認する．

[†]慶應大学環境情報学部 3 年
[‡]慶應大学修士 1 年

- LED と照度センサがある，ノードの ID とホストの ID とネットワークの MasterKey を送信．

5.3 セキュアな設定

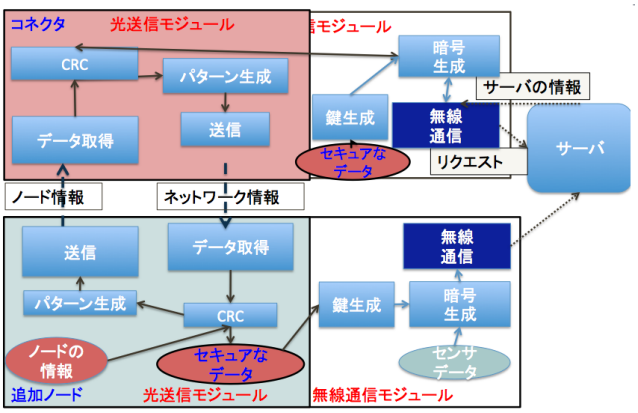
5.3.1 鍵はどうする？

コネクタは追加したいノードに basestation の ID とネットワークの MasterKey を送って，追加したいノードで ID を送る．この情報で鍵を計算する．

$$key = Hash(M|ID_1|ID_2|) \tag{1}$$

6. システム構成図

6.1 システム構成図



7. 評価

7.1 データ通信の評価

128 ビット送信する実験を 69 回行った所，25bit/sec 程の速度を示した．また，69 回の送信で得られたデータの送信精度は 85.5 %であった．また，ビットの誤佐渡は０と１を９２８回の送信で０の精度は１００%，１の精度は９９%であった．

7.2 システムの評価

WSN の知識と軽減がない人の実験でかかる時間とユーザのアンケートで評価する

8. まとめと考察

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．この手法で簡単なインタラクションでセキュアな WSN が構築が出来た．

また，データ通信の速度はまだ低い，小さいデータだけが効果である． フューチャーワークはデータ通信の精度があがって，長いデータを送るときに失敗すると，後ろが全部ずれちゃうのを解決する．また，複数種類のセンサノードで実装すると思う．

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.

[8] http://www.sunspotworld.com