Vol.2013-MBL-69 No.14
2013/12/20

秘密分散法を用いたセキュアなWSNの構築

五百川 貴史[1]　王 家宏[2]　児玉 英一郎[2]　高田 豊雄[2]

概要：無線センサネットワーク (Wireless Sensor Networks: WSN) は重要なネットワーク技術の 1 つであり，この WSN は防災や防犯，施設の監視など様々な分野に利用されている．WSN の利用されるシステムにおいては，様々なレベルのセキュリティが求められている．そして，それは，ネットワークトポロジや WSN において使用されるセンサノードの品質などによって制約を受けている．本研究では，システム利用者の要求するセキュリティレベルに応じ機密性を確保可能なシステムの構築を目指して，監視エリア内にハニカム構造を用いてバックボーンを形成し，そこで，有効に活用できる秘密分散法を提案する．

キーワード：無線センサネットワーク，セキュリティ，ルーティング，ネットワークトポロジ

A Secure Wireless Sensor Network Using Secret Sharing Scheme

Iokawa Takashi[1]　Jiahong Wang[2]　Kodama Eiichiro[2]　Takata Toyoo[2]

Abstract: As an important network technology, Wireless Sensor Network (WSN) has been widely used in various fields such as disaster prevention, crime prevention, and facilities monitoring. Generally different WSN-based system requires different level of security assurance. For the existing technology, the security level of a WSN-base system may be limited by the WSN topology or the quality of sensor nodes. In the paper, we propose an approach to supporting the construction of WSN-based systems that could satisfy various security requirements of system users. The proposed approach will construct a backbone of the honeycomb structure in the monitoring area first, and then applying secret sharing scheme to the constructed honeycomb backbone.

Keywords: Wireless sensor network, security, routing, network topology

1. はじめに

近年，無線センサネットワーク (Wireless Sensor Networks: WSN) [1] は重要なネットワーク技術の 1 つとして注目されている．WSN は環境から湿度や温度，雨量，照明の明るさなど様々なデータを取得するセンサノードと，取得してきたデータの収集や管理を行うシンクノードによって構成される．センサノードはバッテリ駆動，小型，低コストで，計算能力をほとんど持たない．シンクノードは電力供給型で，高い計算能力を持っている．

この WSN は様々な分野に利用されている．例えば，防災テレメータシステム [2] や河川情報システム [3] での利用が挙げられる．防災テレメータシステムは自治体向けの災害監視の支援を目的としており，全国に設置したセンサから花粉，温度，湿度，風向，降水量，雷などの気象データを観測，蓄積し，観測機能，及び，分析機能を自治体に提供している．河川情報システムは雨量や水位などの観測データを収集し，表示するシステムである．

他の利用例としては，オフィス向けの防犯システムが知られている．このシステムでは，WSN を使用してビルや施設に入場を許可されていない人物の侵入を防止し，盗難や放火を未然に防ぐことができる．また，同様のものとして WSN の軍事施設への利用も知られている．

これらの WSN おいては，セキュリティに関する問題が重要である．例えば，WSN を用いたオフィス向けの防犯システムの場合では．ビルや施設へ入場を許可されていな

[1] 岩手県立大学大学院 ソフトウェア情報学研究科
Iwate Prefectural Uniersity, Graduate School of Software and Information Science
[2] 岩手県立大学 ソフトウェア情報学部
Iwate Prefectural Uniersity, Faculty of Software and Information Science

い者が侵入すると，金庫の位置や，防犯システムの穴などの情報が盗まれてしまう．また，防犯システムが収集するデータが改ざんされてしまうと，防犯システムに感知されず，侵入を許すことになってしまう．軍事施設もオフィス向けの防犯システムと同じく，セキュリティに関する問題が重要であり，オフィス向けの防犯システムよりもさらに高い機密性が要求される．

こういった状況の中，本研究では，システムの利用者が要求するセキュリティレベルに応じた機密性を確保可能なWSN システムのモデルを提案する．

2. 関連研究

WSN のセキュリティに関する研究は多く行われている．その 1 つとして，秘密分散法を用いた WSN の機密性確保に関する研究 [4] が挙げられる．この研究では，しきい値秘密分散法を用いて暗号化を行うことにより，WSN の機密性を確保している．しきい値秘密分散法では，データを n 個のシェアに分割し，各シェアでセンサノードとシンクノード間に構築したパスを用いてシンクノードに送信する．シンクノードでは，少なくとも k $(k \leq n)$ 個以上のシェアを受け取った場合に，データを復号できる．

他の秘密分散法を用いた WSN のセキュリティに関する研究として，秘密分散法を用いた WSN のセキュリティと信頼性の向上に関する研究 [5] が挙げられる．前述の秘密分散法を用いた WSN の機密性確保に関する研究 [4] では，マルチパスを用いているが，マルチパスは作成するために多くのセンサノードを使用するため，センサノードとシンクノード間のホップ数が多くなってしまう．ホップ数が多いと通信エラーを引き起こす原因となり，パケットロストが多発する．そこで，この関連研究では，マルチパスになる過剰なノードを減らす工夫を行っている．具体的には，2 種類のパス，Node Disjoint Multiple Path（以下 NDMP と呼ぶ）と Link Disjoint Multiple Path（以下 LDMP と呼ぶ）を用い，パケットロストの増加を抑えている．NDMP はノードが互いに素なマルチパスで，ノード i を通るパスとノード i とノード j 間のリンクが必ず 1 つである．この NDMP の作成には，多くの制御メッセージが必要となる．LDMP はリンクが互いに素なマルチパスで，ノード i を通るパスが 2 個以上の場合もあるが，ノード i とノード j 間のリンクは必ず 1 つである．この LDMP は少量の制御メッセージにて作成できる．この関連研究では，作成コストが低い LDMP を用い NDMP を作成する．

他の関連研究としては，WSN における中継ノードがデータを統合することによりセキュリティや送信効率の向上を行う研究 [6] がある．この関連研究では，図 1 に示すように，マルチパスを使用し，センサノードが取得したデータをセキュリティスキームを用いて暗号化し，シンクノードへ送信する．シンクノードに送信する際，シンクノードへ

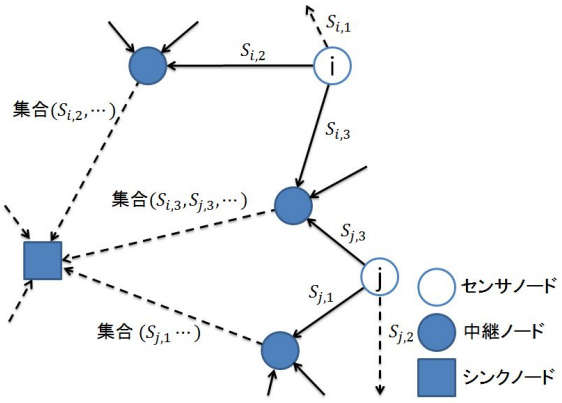

図 1 中継ノードがデータを統合する関連研究が提案している基本的なスキーム

中継しているノード（以下中継ノードと呼ぶ）が受信したいくつかのデータを 1 つにまとめる．そして，1 つにまとめたデータをシンクノードに送信することによって，セキュリティの向上と送信するデータ量の削減を図っている．リンク層にて暗号化機能を備えいることを前提にしており，各ノード間の通信は安全である．

秘密分散法を用いた関連研究では，そのほとんどが多くの NDMP を作成することを前提としている．そのため，これらの手法を有効に活用するには，多くの NDMP を作成するような仕組みが必要である．そこで，多くの NDMP を作成可能な WSN の形成方法や機密性の確保の方法について提案する．

3. 提案手法

本研究で提案する方法を以下に示す．

(1) NDMP ができる限り多く作成できるように，ハニカム構造を用いたバックボーンの形成を行う．
(2) 形成したバックボーン上の通信に対して，秘密分散法を適用する．

本研究で想定している WSN に関する環境を以下に示す．各センサノードは同一の性能であり，秘密分散法を使用するための十分な計算能力を有しており，バッテリ駆動とする．各ノードの最大通信範囲は一定であり，T $[m]$ とする．データを取得するエリアは四角形で，$X \times Y$ $[m^2]$ とする．また，ノードの配置とノード間の通信を阻害する障害物はなく，配置するバックボーンノードの個数は n 個，作成する NDMP 数は p 個とする．

3.1 ノードの配置

エリアからデータを取得したセンサノードは，取得したデータをシンクノードへ送信する．この際，センサノードとシンクノード間に NDMP を構築する．そして，送信するデータに対して秘密分散法を適用する．秘密分散法の各シェアは，NDMP のそれぞれのパスを用いてシンクノー

ドに送信する．そのため，シェア数は作成する NDMP 数と同じになる．少ないシェア（NDMP）の場合は，機密性が低く，送信メッセージ数が少なくなる．多くのシェア（NDMP）の場合は，機密性が高く，送信メッセージ数が多くなる．そのため，システムの利用者が要求するセキュリティレベルに合わせて NDMP 数の調整を行いたい．しかし，センサノードをランダムに配置した場合は，必ずしも一定数以上 NDMP を作成できるとは限らない．そこで，センサノードとシンクノード間の通信を支援するためのバックボーンの形成を行う．これにより，NDMP を多く作成可能とし，様々な利用者の要求するセキュリティレベルに合せて，柔軟に対応可能とする．

バックボーンはハニカム構造を用いて構築する（図 2 参照）．このハニカム構造は 6 個のセンサノードを用いた正六角形により形成する．形成した正六角形を隙間無く並べることによって，ハニカム構造となる．それぞれのバックボーンノードは，自身が所属する正六角形と同じ正六角形を形成している他のバックボーンノードとはリンクを張り，通信を行う（図 3 参照）．シンクノードはバックボーンとは別に配置する．バックボーンノードだけではデータを取得できないエリアがあるため，必要に応じてバックボーンではないセンサノードを配置する．センサノードはエリアからデータを取得し，近くのバックボーンノードにデータの転送を依頼する．データを受け取ったバックボーンノードはシンクノードへデータを送信する．

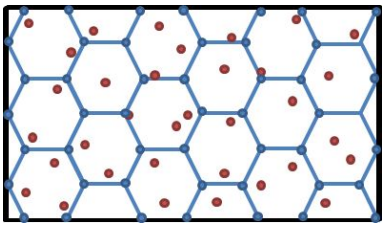

図 2　ハニカム構造を持つバックボーンの例

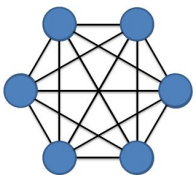

図 3　バックボーンの正六角形

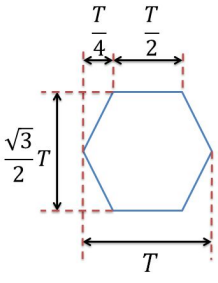

図 4　バックボーンノードの配置

3.2　バックボーンの構築

エリアにバックボーンを配置するためには，配置するバックボーンノード数と正六角形数の算出が必要である．本節では，そのためのアルゴリズムを示す．正六角形を形成するバックボーンノードの配置を図 4 に示す．

最初に，バックボーンノード総数（n）を，Algorithm 1 を使用して求める．ここでは，正六角形の辺を X 軸と平行に配置するとする．以下，$T = 250$，$X = 500$，$Y = 500$ として，Algorithm 1 の説明を行う．最初に，X 軸方向に配置する正六角形数 h_X を求める．エリアに正六角形を隙間なく並べた場合，X 軸方向において各正六角形は $\frac{T}{4}$ が重なる．そこで，重なる $\frac{T}{4}$ を X から引く．引いた値を $T - \frac{T}{4}$ で割った商が X 軸方向に配置する正六角形数である．従って，$h_X = 2$ となる．X 軸方向に配置するバックボーンノード数は h_X から始点になるバックボーンノード数を足した値である．よって，$n_X = 3$ となる．次に，Y を $\frac{\sqrt{3}}{2}T$ で割った商から始点を足した値が Y 軸方向に配置するバックボーンノード数である．すなわち，$n_Y = 5$ となる．最後に，X 軸方向にバックボーンノード数 n_X と Y 軸方向にバックボーンノード数 n_Y を掛け合わせる．これにより，エリア全体におけるバックボーンノード総数 n を求めることができる．この場合，$3 \times 5 = 15$ となる．

Algorithm 1 配置するバックボーンノード数の算出

Require: センサノードの最大通信範囲 T，エリアサイズ $X \times Y$，（$T \leq X$，$\frac{\sqrt{3}}{4}T \leq Y$）．

Ensure: エリア全体におけるバックボーンノード総数 n，X 軸方向に配置する正六角形数 h_X，X 軸方向に配置するバックボーンノード数 n_X，Y 軸方向に配置するバックボーンノード数 n_Y を決める．

1: 次の式で，h_X を算出．

$$h_X = \lfloor \frac{X - \frac{T}{4}}{\frac{3}{4}T} \rfloor$$

2: 次の式で，n_X を算出．

$$n_X = h_X + 1$$

3: 次の式で，n_Y を算出．

$$n_Y = \lfloor \frac{Y}{\frac{\sqrt{3}}{4}T} \rfloor + 1$$

4: 次の式で，n を算出．

$$n_X \times n_Y$$

次に，Algorithm 1 で導き出した X 軸方向に配置する正六角形数 h_X を用いてエリア内に配置する正六角形数を求める．そのアルゴリズムを Algorithm 2 に示す．まず，Y 軸方向に配置する正六角形数を求める．Y 軸の奇数列と偶数列とでは，配置する正六角形数が異なる．奇数列では Y 軸の座標 0 から正六角形を配置するが，偶数列は $\frac{\sqrt{3}}{4}T$ から正六角形を配置する．そのため，奇数列の Y 軸方向に配

置する正六角形数が 3 でも，偶数列の Y 軸方向に配置する正六角形数が 2 の場合がある．そこで奇数列と偶数列で別々の式を用いてそれぞれの Y 軸方向に配置する正六角形数を求める．奇数列では，Y を $\frac{\sqrt{3}}{2}T$ で割った商が Y 軸方向に奇数列に配置する正六角形数 oh_Y である．偶数列では，Y を $\frac{\sqrt{3}}{4}T$ を引いた値に $\frac{\sqrt{3}}{2}T$ で割った商が Y 軸方向に偶数列に配置する正六角形数 eh_Y である．これらから，h を算出する．

Algorithm 2 配置する正六角形数の算出

Require: X 軸方向に配置する正六角形数 h_X.
Ensure: エリア全体における配置する正六角形総数 h を決める.
1: 次の式で，Y 軸方向に奇数列に配置する正六角形数 oh_Y を算出.

$$oh_Y = \lfloor \frac{Y}{\frac{\sqrt{3}}{2}T} \rfloor$$

2: 次の式で，Y 軸方向に偶数列に配置する正六角形数 eh_Y を算出.

$$eh_Y = \lfloor \frac{Y - \frac{\sqrt{3}}{4}T}{\frac{\sqrt{3}}{2}T} \rfloor$$

3: 次の式で，h を算出.

$$h = \lfloor h_X/2 \rfloor \times oh_Y + \lfloor h_X/2 \rfloor \times eh_Y + h_X\%2 \times oh_Y$$

最後に，センサノードからシンクノード間に作成する NDMP 数を算出する．そのアルゴリズムを Algorithm 3 に示す．本研究では，シンクノードの位置を定めていないため，シンクノードがエリアのどの位置にあるかによって NDMP 数を決定する．

Algorithm 3 最大 NDMP 数を算出

Require: シンクノードの配置場所
Ensure: 最大 NDMP 数 p を決める.
1: シンクノードがエリアの角にあるバックボーンノードと同じ位置の場合，$p = 5$ となる.
2: シンクノードがエリアの辺にあるバックボーンノードと同じ位置の場合，$p = 7$ となる.
3: シンクノードが他のバックボーンノードと同じ位置の場合，$p = 12$ となる.
4: シンクノードがバックボーンノードと別の位置にある場合，$p = 6$ とする.

3.3 NDMP の構築

前述のアルゴリズムにより，配置するバックボーンノード数，正六角形数と NDMP 数が決定する．決定した値を基に NDMP を構築する．DART[7] や AODV[8] のような既存のルーティングプロトコルは，そのほとんどがシングルパスを構築するルーティングプロトコルである．そのため，本研究のようなマルチパスを基にしている場合には適用できない．本研究では，既存のルーティングプロトコルを使用せず，システムが要求するセキュリティレベルに応じた個数のパスを，送信時に構築する．パスを構築する方法を Algorithm 4 に示す．この際， Algorithm 3 で求めた NDMP 数と実際に構築した NDMP 数とを比較し，小さい値を NDMP 数とする．

Algorithm 4 NDMP を構築する

Require: NDMP 数 p，送信元のバックボーンノードの位置 $(sourceX, sourceY)$，シンクノードの位置 $(sinkX, sinkY)$，バックボーンノード総数 n，X 軸のバックボーンノード数 n_X，Y 軸のバックボーンノード数 n_Y.
Ensure: 送信元からシンクノードまで p 個のパスを作成する.
1: これから送信を行う送信元を原点 $(0, 0)$ と定めて，シンクノードまでの最も短いパスを構築する.
2: ステップ 1 で作成した最も短いパスに用いたノードを省き，さらに，最も短いパスを構築する.
3: p 個のパスを構築できるまでステップ 2 を繰り返す.

3.4 マルチパスにおける秘密分散法

WSN の各センサノードが取得したデータを送信する際には，秘密分散法を用いる．ここで，秘密分散法におけるシェア数は NDMP 数と同じである．そのため，NDMP 数が多ければ，秘密分散法におけるシェア数も多くなり，機密性が向上する．以下，バックボーンノード i が取得したデータ r_i を，秘密分散法を使用し，分割，暗号化を行う流れについて説明する．

送信を開始するバックボーンノードをノード i とする．ノード i は p 個の NDMP を使用してデータ r_i をシンクノードまで送信する．このとき，シンクノードはが少なくとも k 個以上のシェアを収集すれば，データ r_i を復号できる．

ノード i は，$P_i(0) = r_i$ となるような素体上の $k-1$ 次多項式を作成する．すなわち，ランダムに選ばれた $\alpha_{i,l}, (1 \leq l \leq k-1)$ を使用して $P_i(X) = r_i + \alpha_{i,1}X + \alpha_{i,2}X^2 + ... + \alpha_{i,k-1}X^{k-1}$ のような多項式を作成する．そして，パス q $(1 \leq q \leq p)$ に沿って $P_i(q)$ を含むメッセージを送信する．

シンクノードが少なくとも k 個以上のパスからメッセージを受け取った際には，復号化を行う．環境から取得したデータ r_i を復号するために，$k-1$ 次多項式を使用し，$r_i = P_i(0)$ を計算する．

次に，送信を開始するノード i とノード j を考える．ノード i が環境から取得したデータを r_i，ノード j が環境から取得したデータを r_j とする．ノード i とノード j は NDMP を使用してシンクノードまで送信する．

ノード i が取得したデータ r_i とノード j が取得したデータ r_j を，それぞれ $k-1$ 個のシェアに分割する．ノード i はパス q に沿って $P_i(q)$ を含むメッセージを送信し，ノード j はパス q に沿って $P_j(q)$ を含むメッセージを送信する．

シンクノードでは復号化を行った後，各センサノードが

環境から取得したデータに関する集計を行う．

4. 考察

ハニカム構造を使用することにより，NDMP を多く作成することが，本研究の当初の目的に沿っているどうかの考察を行う．本考察では，比較対象として，エリア内に正四角形を隙間無く敷き詰めた Grid 構造を用いる．この Grid 構造では，正四角形の対辺を T とすると，一辺の長さは $\frac{T}{\sqrt{2}}$ となる．この Grid 構造とハニカム構造の両方にエリアサイズ X と Y を与える．このときの Grid 構造とハニカム構造のエリア全体に配置するバックボーンノード総数の比較を行う．また，Grid 構造とハニカム構造における作成する NDMP 数 (p) の最小値，最大値の比較を行う．この 2 つの比較をもって，本研究の目的が達成できたかを判定する．なお，ノードの最大通信範囲は $T = 250$ $[m]$ とする．

Grid 構造におけるエリア全体に配置するバックボーンノード総数の計算式は，

$$n = (\lfloor \frac{X}{\frac{T}{\sqrt{2}}} \rfloor + 1) \times (\lfloor \frac{Y}{\frac{T}{\sqrt{2}}} \rfloor + 1) \quad (1)$$

である．これに対し，ハニカム構造におけるエリア全体に配置するバックボーンノード総数の計算式は，

$$n = (\lfloor \frac{X - \frac{T}{4}}{\frac{3}{4}T} \rfloor + 1) \times (\lfloor \frac{Y}{\frac{\sqrt{3}}{4}T} \rfloor + 1) \quad (2)$$

である（Algorithm 1 参照）．X と Y にそれぞれ 500, 1000, 1500, 2000 を与えた場合を考察する．**表 1** は Grid 構造における，X と Y を与えた際のエリア全体に配置するバックボーンノード総数である．**表 2** はハニカム構造における，X と Y を与えた際のエリア全体に配置するバックボーンノード総数である．

表 1 Grid 構造におけるノード数
Table 1 Number of Nodes for the Grid Structure.

X \ Y	500	1000	1500	2000
500	9	18	27	36
1000	18	36	54	72
1500	27	54	81	108
2000	36	72	108	144

表 2 ハニカム構造におけるノード数
Table 2 Number of Nodes for the Honeycomb Structure.

X \ Y	500	1000	1500	2000
500	15	30	42	57
1000	30	60	84	114
1500	40	80	112	152
2000	55	110	154	209

表 1 と表 2 を比べて，これは X 軸と Y 軸が 500×500 の時でも，2000×2000 の時でもハニカム構造の方が配置するバックボーンノード総数が多い．また，X 軸と Y 軸をそれぞれ増加させると，Grid 構造とハニカム構造は共に一定の規則に従って増加する．これは Grid 構造もハニカム構造も一定の規則に従ってノードを配置したため，エリア全体における配置するバックボーンノード総数もそれぞれの規則に従って増加するためである．

Grid 構造における NDMP の最小値は 3 であり，最大値は 8 である．ハニカム構造における NDMP の最小値は 5，最大値は 12 である（Algorithm 3 参照）．Grid 構造とハニカム構造の最小値と Grid 構造とハニカム構造の最大値を比較する．最小値，最大値の両方共に Grid 構造よりもハニカム構造の方が大きな値となる．

上述のように，Grid 構造よりハニカム構造の方がバックボーンノードの配置数が多く，同じエリアにおいてバックボーンを構築する際，Grid 構造よりもハニカム構造の方が多くのノードを必要とする．しかし，Grid 構造よりハニカム構造の方が NDMP を多く作成できる．これは各構造における構成要素に起因する．Grid 構造では，正四角形を隙間なく並べることによって Grid 構造を形成する．このとき，正四角形を構成する自身以外のノードと通信を可能とする．だが，ハニカム構造では，正六角形を隙間なく並べることによってハニカム構造を形成する．正四角形と正六角形を比較して使用するノードが多いのは正六角形だが，通信が可能となるノードが多いのも正六角形である．そのため，エリア全体における配置するバックボーンノード総数が多いのは正六角形を隙間なく敷き詰めたハニカム構造であるが，NDMP 数が多いのも正六角形を隙間なく敷き詰めたハニカム構造である．

本研究では，NDMP をできるだけ多く作成することを目的している．ハニカム構造は NDMP をできるだけ多く作成できるため，本研究の目的に適っている．

5. 性能評価

上述した提案手法について性能を評価するために実験を行った．以下，実験内容と実験結果を示し，その考察を行う．本実験では，Grid 構造との比較を行う．

5.1 シミュレーション環境

性能を評価するにあたってネットワークシミュレータ ns-2 [9] を用いた．シミュレーション環境の各設定を **表 3** に示す．バックボーンノード数は Algorithm 1 を用いて求めた．シンクノードはランダムに配置している．

5.2 実験結果と考察

本シミュレーション環境において以下の 3 つの実験を行った．

表 3　シミュレーション環境
Table 3　Simulation environment.

パラメタ	値
エリア	1000×1000, $1500 \times 1500, 2000 \times 2000 (m^2)$
バックボーンノード数	Algorithm 1 を用いて求める
ワークロード	TCP + FTP. データの送受信はシミュレーションの開始時間から 10 秒ごとに終わるまで行う.
ノードの最大通信範囲	250 （m）
シミュレーション時間	100 （秒）
NDMP 数	6 （個）
同時に送信するノード数	10 （個）　（ランダムに選択）

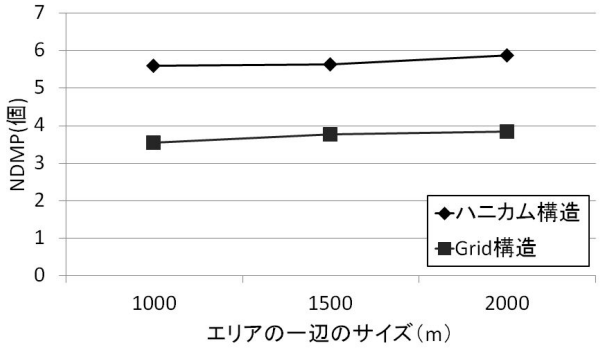

図 5　各送信ノードが持つ平均 NDMP 数

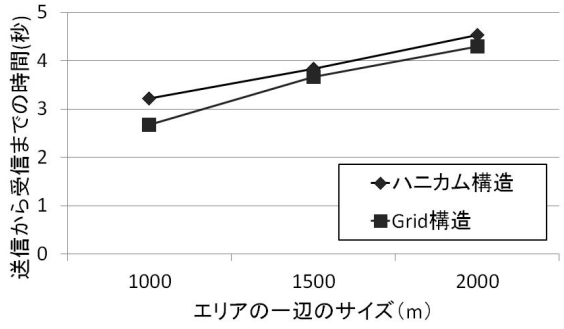

図 6　送信から受信までの平均時間

(1) 各送信ノードが持つ平均 NDMP 数.
(2) バックボーンノードが送信してからシンクノードが受信するまでの平均時間.

実験 1 の結果を図 5 に示す．どのようなエリアサイズを与えても，Grid 構造よりハニカム構造の方が平均 NDMP 数が多い．

実験 2 の結果を図 6 に示す．ハニカム構造と Grid 構造ともにエリアサイズが大きくなると送信から受信までの平均時間が長くなる．これはエリアサイズが大きくなるにつれて，シンクノードから遠く離れたバックボーンノードが送信するノードになることが増えていったためである．

6. おわりに

WSN は重要なネットワークの技術として注目されている．WSN は防災テレメータサービスや防犯システム，軍事施設の防犯など様々なサービスに利用されている．しかし，WSN には，セキュリティに関する問題があり，WSN を使用する環境によって，求められる機密性の高さが異なっている．本研究では，秘密分散法が有効に活用できるように，ハニカム構造を持つバックボーンを監視エリアに配置することによる WSN の形成手法を提案した．また，WSN を使用する環境によって必要な高さの機密性を確保できる秘密分散法を提案した．これにより，WSN を使用する環境によって必要な機密性の高さを確保することができる．

また，本研究では，提案手法の考察と実験も行った．実験により，提案手法の有効性を確認できた．今後の課題としては，エリア内に障害物があり，バックボーンノードが正六角形の形に配置できない場合への対応方法が挙げられる．

参考文献

[1] 安藤繁，戸辺義人，田村陽介，南正輝: センサネットワーク技術，東京電機出版局 (2005).
[2] NTT ドコモ，防災テレメータサービス，http://www. nttdocomo.co.jp/info/news_release/2012/11/30_01.html. (2013/11/26 参照)
[3] 岩手県，河川情報システム，http://kasen.pref.iwate.jp/iwate/servlet/Gamen30Servlet.(2013/11/26 参照)
[4] E. Kohno，T. Okazaki，M. Takeuchi，T. Ohta，Y. Kakuda，M. Aida: Improvement of the Security Against Node Capture Attacks Using Dispersed Data Transmission for Wireless Sensor Networks, in Proc. the 2010 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, pp.340–345 (2010).
[5] A.Kimura，E.Kahna，Y. Kakuda: Security and Dependability Enhancement of Wireless Sensor Network with Multipath Routing Utilizing the Connectedness of Joint Nodes, in Proc. the 2012 International Conference on Distributed Computing Systems Workshops, pp.342–348 (2012).
[6] H.Claveirole，M.Dias，M.Abdalla，Y.Viniotis: Securing Wireless Sensor Networks Against Aggregator Compromises, IEEE Communications Magazine, 46(4), pp.134–141 (2008).
[7] J.Eriksson，M.Faloutsos，S.Krishnamurthy: DART: Dynamic Address RouTing for Scalable Ad Hoc and Mesh Networks, IEEE/ACM Transactions on Networking, 15(1), pp.119–132 (2007).
[8] C. E. Perkins，E. M. Poyer : Ad hoc On-Demand Distance Vector Routing, in Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90–100 (1999).
[9] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns/