無線センサネットワークにおける暗号パラメータと経路の適応的設定が可能なセキュア情報転送

代表研究者　河　野　英太郎　広島市立大学　大学院　情報科学研究科　講師
共同研究者　角　田　良　明　広島市立大学　大学院　情報科学研究科　教授

1 はじめに

無線センサネットワークは，災害時の生存情報の転送といった非常に高度な情報を扱う場合があり，転送データの機密性が必要[1][2]だが，有線ネットワークと比較し，攻撃に遭いやすい．我々は秘密分散法[3][4]を応用しデータの分散転送による内容の改竄防止機構を用いデータの暗号化を行なう暗号化手法と，ネットワークの変化にも適応可能なスケーラブルな複数経路の設定方式であるセキュア分散データ転送の提案を行い評価した[5][6]．ネットワーク上で可能な限り多くの複数経路を求めることが望ましい．複数経路には，経路の特徴によりリンク素経路，ノード素経路があるが，より多くのノード素経路を用いると，最もセキュリティ耐性が向上することが分かっている．しかし，多くのノード素経路を求めることは一般的に困難であり複数の経路が重複するノードの存在を許容する必要がある．ネットワーク上に複数の経路重複ノードが存在する場合，リンク素複数経路を求めることとなる．その際，暗号化手法として秘密分散法を用いると，しきい値を適切に見積もることにより，悪意のある転送ノード上での元データの復号を阻止することが可能である．上記の特性を持つ複数経路を生成するプロトコルを実装し，シミュレーション実験により評価する．それに基づき，文献[5][6]では考察されていない攻撃に対するセキュリティ耐性を計測し評価する．

また，ワイヤレスセンサネットワークでは，マルチホップ通信が用いられるため，中継ノード等によるデータの盗聴，改ざんやなりすましといった攻撃を受ける．我々はBloom Filter [7]を応用し，送信元端末が持つ経路情報ならびに経路の認証により，中継ノードによるなりすまし攻撃の検知手法を提案する．

2 秘密分散法を用いたセキュア分散データ転送

2-1 概要

文献[5][6] では，ノードキャプチャ攻撃を回避するために秘密分散技術[3] [4] を用いたセキュアデータ転送（以降，分散データ転送）が提案されており，宛先ノード以外のノードによるデータの復号を困難にすることで攻撃を回避する．秘密分散法は，秘密情報を分散保管するために，Shamir[3]，Blakley[4] らによってそれぞれ独立して提案された手法である．分散データ転送はデータをシェアと呼ばれる複数の暗号化情報に分割し転送する．シェアは単体では元データを復号できず，しきい値個以上のシェアを収集することで元データの復号が可能となる．しかしこの手法は宛先ノード以外のノードでもしきい値以上のシェアが集まればデータの復号が可能となる．分散データ転送では送信元・宛先ノード間で複数経路を構築し，それぞれのシェアを異なる経路を使用して転送する必要がある．その際，相異なる複数経路を用いることにより，シェア同士が同じ経路を通らずに宛先ノードまで到達でき，中継ノードはしきい値個以上のシェアを集めることが困難になる．

2-2 パラメータ設定

1.節で述べたとおり，複数経路を使用した分散データ転送において，分散させるシェア数と復号するためのしきい値を適切な値に設定することが重要となる．しきい値の値を大きくすると，中継ノードにデータを復号されにくくなるが，大きくし過ぎると，シェアの転送中にパケット損失が生じた場合，宛先ノードはシェアの収集が困難となりデータの復号に失敗する可能性が高くなる．一般にはシェア数としきい値の最適な値はネットワークトポロジや経路制御手法，また経路数によって異なるため算出は困難であるが，使用する経路特性を想定することで，パラメータの値と攻撃耐性との関係を求めることが可能になると考えられる．

3. ノード ID の偽造とその影響

図 1にノード ID の偽造とその影響の概念図を示す．本研究では，送信元ノード ID の偽造を以下のようなものと考える．（1）悪意のあるノードが送信元ノードの ID を中継したデータパケットから窃取し，（2）窃取した送信元ノードの ID を自ノード ID の代わりに挿入したデータパケットを転送する．図 2 には中継ノードへ制御パケットが窃取される様子を示す．WSN では図 2 のように中継ノードの情報が窃取されると，悪意のあるなりすましノード（以降攻撃ノード）がノード L の ID を入れたパケットを送信し，不正にパケットを中継できる可能性がある．

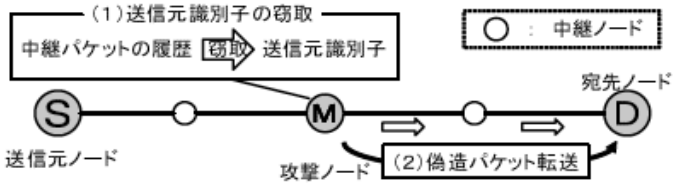


図 1:送信元ノード ID の偽造による攻撃の概念図

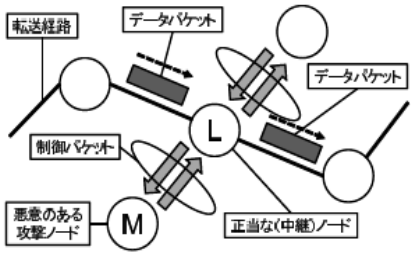


図 2: 攻撃ノードによる制御パケットの窃取

4. Bloom Filter

Bloom Filter(以降 BF)[7] はビット列からなるデータ構造であり，複数のデータが格納できる．データ格納時に複数のハッシュ関数でデータを変換することで格納に必要なデータサイズを減少させる．また，ハッシュ関数が持つ一方向性により，ビット列から元のデータを得られない．

5. 分散データ転送のための複数経路構築手法

本節では，まず分散データ転送で使用する経路の構築手法（以降，提案法）について述べる．分散データ転送は重複の少ない複数経路の使用が性能を向上させるために重要となる．

5-1 概要

提案法は，まず経路上の重複が考慮されていない既存の経路制御手法である SRIDR[8]による複数経路を用い，その経路同士の重複を減らすための経路について述べる．拡張 DART は二進数の独自のアドレスを使用することでフラッディングをせずに経路構築を行うことが可能なため，他複数経路制御に比べ制御パケットを大幅に低減できる．拡張 DART の経路の重複を減らすために Joint Count プロセスという手続きを導入する．Joint Count プロセスは複数経路制御手法の一つである AODV-based Multipath Routing Protocol [9] の，経路上の重複ノード数を計算する方法を応用した．Joint Count プロセスは経路上の重複ノード検知し，経路表に記録する手続きである．このとき *JointCount* 値という値を使用する．*JointCount* 値はデータパケット転送時の経路選択において重複の少ない経路を選択する指標としての役目を果たす．

提案法は，拡張 DART と Joint Count プロセスを組み合わせ，重複ノードの少ない複数経路の構築を試みる．また，提案法独自の経路表として Joint Count プロセスでは各ノードに JCTable（Joint Count Table）を保持させる．

5-2 動作

制御メッセージの転送に拡張 DART の経路表を用いることで，拡張 DART によって構築された経路上の重複ノードの制御を実現している．提案法の動作は以下の 3 つのフェーズからなる．

（ 1 ） 拡張 DART による経路制御（拡張 DART 経路表の作成）
（ 2 ） Joint Count プロセス（JCTable の作成）
（ 3 ） JCTable 使用による経路選択

以降，それぞれのフェーズについて説明する．

（1）拡張 DART による経路制御拡張

DART では，任意のノード間で通信が必要になると経路が作成される．そのためあるノードで通信要求が発生したら，拡張 DART の経路制御により各ノードは経路表を作成し保持する．これにより，ネットワークは送信元・宛先ノード間の経路が構築された状態になる．

（2）Joint Count プロセス

拡張 DART による経路制御終了後，Joint Count プロセスを開始する．送信元ノードは制御メッセージをユニキャストすることで宛先ノードに対し JointCount 値付加要求を行う．その際の経路選択には拡張 DART の経路表を用いる．

JointCount 値付加要求を受けた宛先ノードは，送信元ノード方向に向かって JointCount 値の付加をした制御メッセージを転送する．それにより，制御メッセージが送信元に到達するまでの経路上の重複ノードを検知し，それを記録することが可能となる．まず，宛先ノードは制御メッセージを作成する．このとき制御メッセージの JointCount 値フィールドには初期値として 0 を格納し，これを隣接ノードにブロードキャストする．制御メッセージを受信したノードは，自身が重複ノードならば受信した JointCount 値を計算し，その値を格納した制御メッセージを次ホップノードにユニキャストする．このとき次ホップノードの決定には拡張 DART 経路表を用いる．JointCount 値は制御メッセージを受信するノードにより次のように計算される．

（i）制御メッセージを受信したノードが重複ノード

複数のノードから制御メッセージを受信した場合，それぞれの JointCount 値は異なる可能性がある．その場合，最も JointCount 値の小さい値を採用し，その値をインクリメントした値を制御メッセージに格納する．

（ii）制御メッセージを受信したノードは重複ノードではない

受信した JointCount 値を変えずに次ホップノードへユニキャストする．制御メッセージは送信元ノードまで転送される．制御メッセージ転送時，各ノードは JCTable を作成し，受信した JointCount 値と次ホップノードのアドレスを対にして記録する．

（3）JCTable 使用による経路選択

Joint Count プロセス終了後，各ノードは JCTable を用いた経路選択が可能となる．その際，JCTable から JointCount 値の昇順により次ホップノードを決定することで，重複ノードが少ない経路を優先して使用する．

6. 提案法経路特性と分散データ転送

本稿では 3.2 節の手続きで構築された経路を使用して分散データ転送を行う．提案法によって構築される経路の特性を解析し，その特性から，分散データ転送の効果を向上させるためパラメータの設定値について検討する．

まずパラメータの設定値を検討する際の前提として，分散データ転送で複数経路を使用する際の経路の分岐点となるノードでの動作，及び攻撃ノードとデータ窃取について明示する．

分散データ転送の経路分岐点での動作

分散データ転送において，3. 節で述べた経路制御手法により構築される経路の，分岐点となるノードの動作について説明する．図 3(a) に経路の分岐点となるノードでの動作を示す．

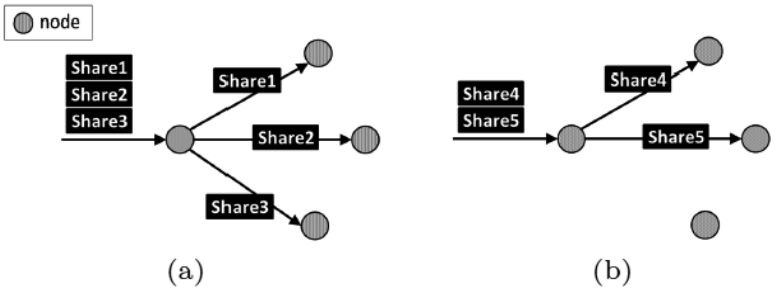


図 3:経路の分岐点となるノードでのシェアの分散方法

シェア中継時，経路の分岐点となる転送ノードは 3.2（3）で述べた経路制御手法の経路選択方法に従い経路を決定する．その後，各々の経路に対しシェアを均等に分散する．例えば，図 3(a) のように経路の分岐点である重複ノードが 3 つのシェアを分散する場合，3 つのシェアを特定の次ホップノードに転送するのではなく，複数の異なる次ホップノードに順番に転送する．次ホップノードの決定順序は，提案法の経路制御の場合，*JointCount* 値の昇順で決められる．図 3(b) のように，重複ノードの分岐数を超えるシェアの転送が必要な場合，再度経路表に登録された次ホップノードを順番に選択する．

6.1 転送経路とパラメータの関係

攻撃ノードとその動作について定義する．中継ノードは宛先ノードと同様にしきい値以上のシェアを受信できれば復号が可能となる．分散データ転送のシェア数としきい値のパラメータ設定値は 2.2 節で述べたように，攻撃ノードによるデータ窃取数等の攻撃耐性に関わるため，適切な値に設定する必要がある．ここで，本稿では分散データ転送で用いられるシェア数としきい値というパラメータの設定値が満たすべき目標を次の通りとする．

目標 1 攻撃ノードから窃取されるデータ数を最小限に抑制

目標 2 ネットワークの負荷を軽減させるため，分散するシェアは極力少ないこと

目標 1，2 で示した条件を満たすシェア数としきい値の組み合わせの条件について，次に定義する．

［パラメータ設定条件 4.1］（適切なパラメータの設定条件）すべての中継ノードでのデータ窃取数が最小となるシェア数としきい値の組み合わせの内，最小のシェア数を持つときのしきい値とシェア数自身の組み合わせが設定されること

以降，上記で示した条件 4.1 に適合するパラメータ設定値を**適合パラメータ**と呼ぶ．

ネットワークのトポロジや経路制御手法に依存せず適合パラメータを算出することは困難だが，トポロジや使用する経路に特性や条件が多いほど適合パラメータの算出が容易になる．算出には経路特性の情報を利用できる場合があり，提案法の経路においても適合パラメータの算出が可能であるか検討する．

7. 提案法による経路での分散データ転送のパラメータ設定

3. 節で示した手法で構築される経路の一例を図 4 に示す．

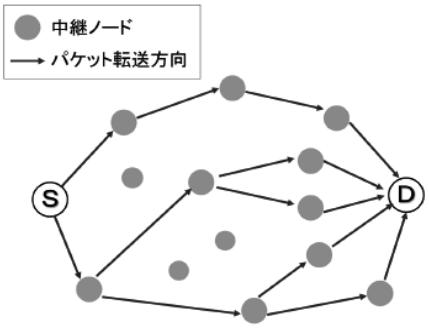


図 4:提案法で構築される経路の一例

提案法の経路は，宛先ノード方向への経路の分岐を許すが，送信元ノード方向への分岐はしない．この特性は 3.2 節で示した Joint Count プロセスにおいて，各ノードは JCREP を複数のノードから受信した場合でも，送信元ノード方向の 1 つの次ホップノードへしか JCREP の転送をしないことが起因している．

7.1 適合パラメータの導出

提案法で構築される経路から，適合パラメータのシェア数としきい値の組み合わせを求める．図 5 は提案法で構築される一般的な経路の例を示す．

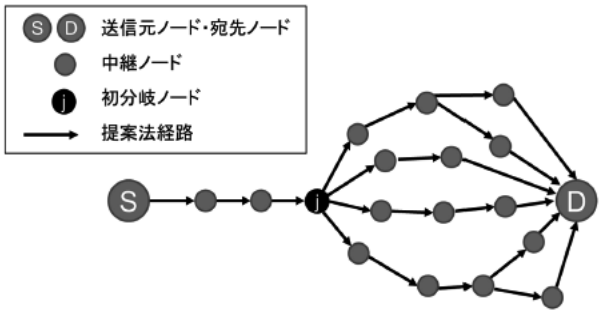


図 5:提案法で構築される一般的な経路の例

以下に，適合パラメータの導出を行うために計算に用いる変数を示す．n_1，m は 0 以上の整数とし，その他の変数は自然数とする．また，それぞれについて説明を補足する．

- シェア数：ns（ >=kk）_ しきい値：kk（ >=2）
- シェア数としきい値の差分：d（ = ns - kk）
- 経路として使用される全中継ノード数：n
- 送信元ノードと初分岐ノード間のノード数：n_1
- 初分岐ノードの経路分岐数：p（ >=1）
- 元データ窃取が可能な中継ノード数：m

ここで初分岐ノードとは，送信元ノードが分岐経路を持っていない（次ホップノードが 1 つしかない）場合，宛先ノード方向への転送経路が初めて分岐するノードである．図 5で初分岐ノードはノード j にあたる．送信元ノードと初分岐ノード間のノード数 n_1 は，初分岐ノード自身を含む初分岐ノードまでに経由する中継ノード数を表す．但し，送信元ノードを除く．図 5 の例においては，$n_1 = 3$ となり，初分岐ノード j の経路分岐数 p は $p = 4$ である．適合パラメータを導出するとき，初分岐ノードから分岐した後の各経路上には，それぞれの経路で同等の中継ノードが存在すると仮定する．

経路として使用される全中継ノード数 n は，ns 個のシェアが転送される際，提案法の経路選択で必ず経由する中継ノードの総数とする．データ窃取が可能な中継ノード数 m は，ns 個のシェアが転送される際，中継ノードによる復号で元データの窃取が可能な（提案法の経路選択によって kk 個以上のシェアが経由する）中継ノードの総数である．

上記に示した各変数が変化した時の，窃取ノード数 m を算出した．経路の分岐特性から，シェアがしきい値以上通る経路と，しきい値未満しか通らない経路数を算出し，一定数以上の中継ノードに元データを復号されない条件式を求めた．この条件式から，構築される経路数が少なくても適用可能となるようなシェア数としきい値を求めた．それによって得られた m から，条件 4.1 が満たされる適合パラメータを導出した．

導出した適合パラメータ（シェア数：ns，しきい値：kk）を以下に示す．

$ns = 2d + 2$ (1)

$kk = d + 2$ (2)

この適合パラメータを分散データ転送に使用することで条件 4.1 が満たされる．

8. シミュレーション実験

提案法と適合パラメータの設定による分散データ転送の性能を評価するため，シミュレーション実験[10]を行った．

評価項目

提案法で構築された経路を分散データ転送に適用した際の有効性を調べるため，宛先ノードにおけるデータパケット到達率，またデータ転送中に攻撃を受けた指標として，中継ノードによるデータ窃取成功率を集計した．中継ノードによるデータ窃取成功率は，中継ノードになり得るすべてのノード数に対し，データの窃取に成功した中継ノードの数を示す．

実験環境

実験環境を表 1 に示す．分散データ転送はアプリケーション層に実装した．ノード密度による提案法の性能の違いを調べるため，ネットワーク内のノード数を 300，400，500 でそれぞれ実験した．フィールドサイズが固定のため，平均隣接ノード数はそれぞれ，約 10，14，17 となる．

表 1:実験環境

シミュレータ	QualNet ver.5.0 [8]
MAC 層プロトコル	IEEE 802.11a
フィールドサイズ [m^2]	2400×2400
最大通信可能距離 [m]	250
シミュレーション時間 [sec]	1600
データ送受信ペア数	10
データパケット送信間隔 [sec]	1.0
データパケットサイズ [Byte]	64
ネットワーク内ノード数	300，400，500
トランスポート層プロトコル	UDP
ガロア (拡大) 体 GF(2^l)	GF(2^8)
GF(2^l) の既約多項式	$x^8 + x^7 + x^2 + x + 1$
シミュレーション回数	30

8.1 実験方法

実験では，各データ送受信ペアはネットワーク内のノードからランダムに選択され，シミュレーション開始から 20 秒後に，最初の送信元ノードはデータ転送を始めようとする．そのとき送信元ノードは提案法による経路構築を開始する．経路構築後，送信元ノードはデータを複数のシェアに変換し，宛先ノードへ向け送信する．送信元ノードは 1 秒間隔で計 10 回データを送信する．1 秒の間隔をとっているのはネットワークの混信を避けるためである．その後，20 秒ごとに次の送信元ノードも最初の送信元ノードと同様に 1 秒間隔で計 10 回データの送信を行う．シミュレーション時間が 1600 秒となったら，シミュレーションを終了する．

ノードキャプチャ攻撃の模擬

シェアを転送するすべての中継ノードは，中継したシェアを破棄せず自身のバッファに記憶した後，次ホップノードへ転送する．ノードキャプチャ攻撃の模擬として，各中継ノードはシェア受信時にデータの復号を試みる．その際，中継ノードは宛先ノードと同じデータ復号アルゴリズムを使用する．すべての中継ノードを攻撃ノードとして動作させ，ネットワーク全体でそのデータ窃取数を計測することで攻撃耐性を評価する．

分散データ転送のパラメータ設定値について

パラメータを任意の値に設定した場合と，適合パラメータに設定した場合とで性能を比較する．分散データ転送のパラメータを 3 つのパターンで実験した．任意の値に設定した場合の，シェア数やしきい値の増加にともなう性能の傾向を調べるため，任意の値には下記（設定 1），（設定 2）の二通りのパターンを調査する．適合パラメータの設定は式（1），式（2）より下記に示す（設定 3）のパラメータを使用する．

（設定1）任意の値： シェア数ns=8，しきい値kk=1～7

（設定2）任意の値： シェア数ns=kk+1，しきい値kk=1～8

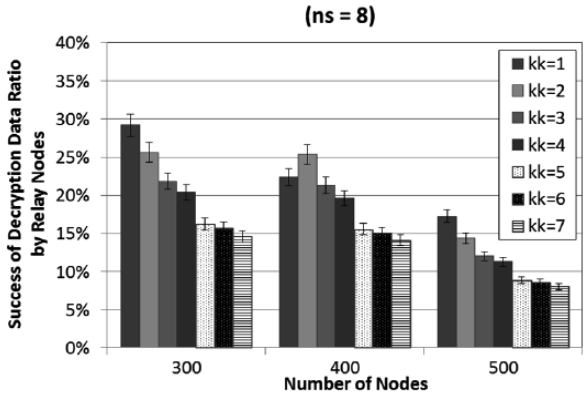
（設定3）適合パラメータの設定： シェア数ns = 2d+2，しきい値kk=ns □ d

8.2 実験結果

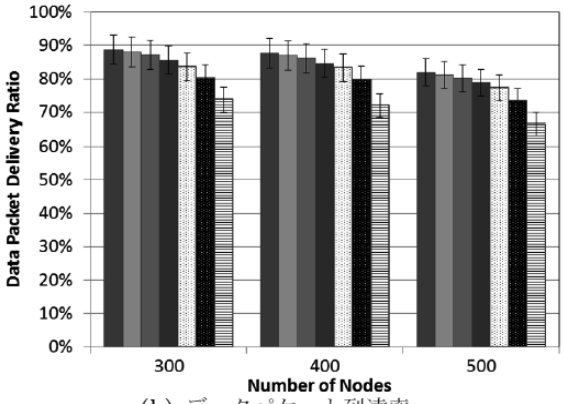
経路制御に用いた制御パケット量，及びパラメータを(設定 1)～(設定 3) にしたときの宛先ノードでのデータパケット到達率，中継ノードによるデータ窃取成功率(データの窃取に成功した中継ノード数／ネットワーク上の中継ノード数) について，シミュレーション実験を行った結果を示す．横軸をネットワーク上のノード数とし，エラーバーは 95%の信頼区間を示す．なお，実験結果の詳しい考察については 7. 節で述べる．

9. 考察

シミュレーション実験の結果から，各パラメータ設定での分散データ転送の性能と提案法の有効性について考察する．



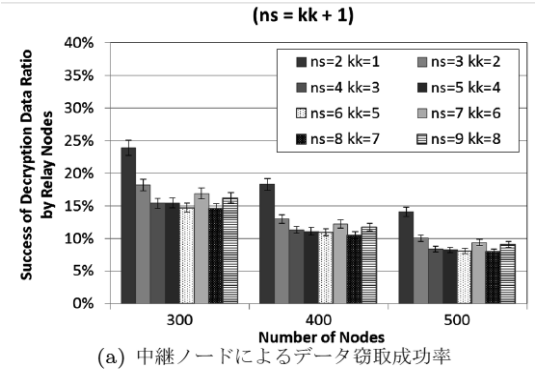
(a) 中継ノードによるデータ窃取成功率



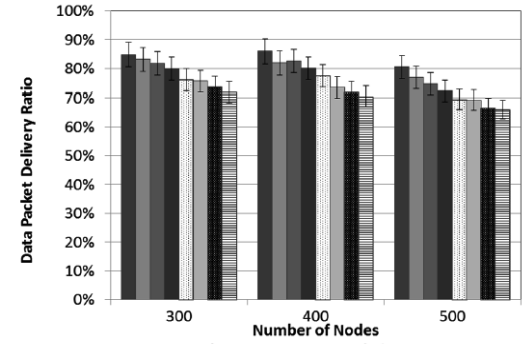
(b) データパケット到達率

図 6: ns = 8 のとき（設定 1）

パラメータを（設定 1）にしたときの実験結果を図 6 に示す．（設定 1）はシェア数を 8 に固定し，しきい値を変化させたときの設定である．図 6(a) より，しきい値が 5〜7 のとき中継ノードによるデータ窃取成功率は，他のしきい値よりも低い値を示している．しきい値 5〜7 の結果のみで比較すると，7 のとき最小で，その差はわずかである．これは図 6(b) のデータパケット到達率の低下傾向から，シェア転送中のパケット損失の影響によるものと考えられる．しきい値 5〜7 の実験結果のうち中継ノードによるデータ窃取成功率のわずかな差を無視すれば，シェア数を 8 に固定した設定 1 では，しきい値が 5 のとき高いデータパケット到達率で攻撃中継ノードからのデータ窃取数が少ないことがわかる．ここで，シェア数 8 のときの適合パラメータを考える．今回シェア数は確定しているので適合パラメータの式（1）からしきい値との差分 d を求めることでしきい値が算出できる．式（1）にシェア数を代入すると $8 = 2d+2$ となるので，これを変換すれば $d = 3$ となる．適合パラメータのしきい値は式（2）より，$kk = 5$ と算出できる．このシェア数としきい値の設定値を実験結果と照らし合わせれば，しきい値 5 のときの性能は前述した通り高いパフォーマンスを示すことができている．



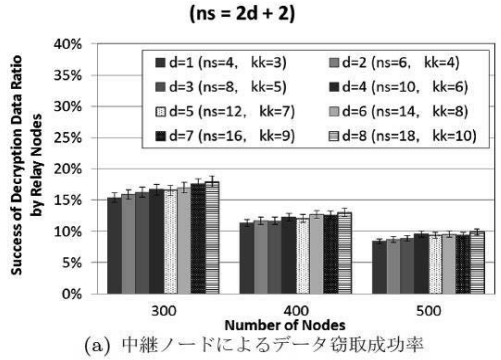
(a) 中継ノードによるデータ窃取成功率



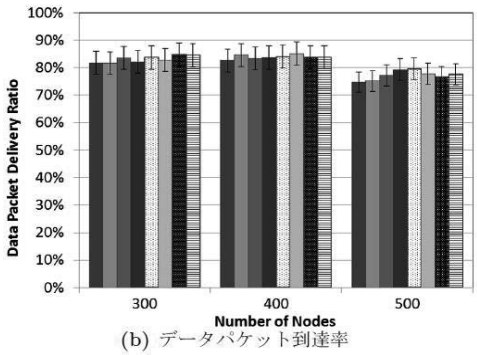
(b) データパケット到達率

図 7: ns = kk + 1 のとき（設定 2）

図 7は分散データ転送のパラメータ設定を任意の値（設定 2）にしたときの実験結果である．図 7(a) で示す中継ノードによるデータ窃取成功率は，主にシェア数 4，5，6，8 のとき低い値を示している．ここで，この実験のパラメータを設定では，シェア数としきい値の差分は 1 である．この差分から適合パラメータのシェア数としきい値を求めることができる．シェア数は式(1) より 4，しきい値は式(2) より 3 と算出できる．図 7(b) のデータパケット到達率では，データ窃取成功率が低い値を示していた設定群のうち，適合パラメータに合致するシェア数 4，しきい値 3 のとき最も高い値を示している．これは，シェア数としきい値との差分が 1 のとき，最もデータが窃取されにくくデータパケット到達率が高い設定は，適合パラメータに該当する設定であることを示す．この実験では適合パラメータは条件 4.1 を満たしているといえる．また，適合パラメータのシェア数よりシェア数の設定値が高いときデータパケット到達率は低下している．これは，設定したシェア数に対ししきい値が大きくなるため，シェア転送中に少しでもパケット損失が起こると宛先ノードはデータの復号が困難となるためである．シェア数の設定が 5，6，8 のときも，適合パラメータのシェア数 4 しきい値 3 のときと同様に中継ノードによるデータ窃取成功率が低かった要因として，データパケット到達率の結果をもとに分析すると，宛先ノードと同様に中継ノードでもパケット損失によってシェアの収集が困難となったことが原因と考えられる．



(a) 中継ノードによるデータ窃取成功率



(b) データパケット到達率

図 8: 適合パラメータのとき（設定 3）

（設定 3）の実験結果を図 8 に示す．（設定 3）はすべての設定が適合パラメータで算出した設定値である．ここでは，適合パラメータの唯一の変数であるシェア数としきい値の差分 d を変化させて実験を行った．差分 d の値が性能に与える影響を考察する．図 8(a) で示す中継ノードによるデータ窃取成功率は d の増加にともないに多少の増加が見られる．これは，シェア数の増加に応じて使用する経路数が増えるため，シェアを中継するノードの数も増加しデータ窃取成功率に影響を及ぼしていると考えられる．しかしこの増加量は全体で約 2〜4%であるため，分散データ転送の性能への影響は小さい．また，適合パラメータを採用した際，図 8(b) で示すデータパケット到達率は d の値に関わらず，ネットワーク上のノード数 300, 400 で 80%以上，500 ノードでも約 75%以上と安定して高い値を維持していることがわかる．提案法の経路を使用した分散データ転送において，パラメータの値を任意に設定した場合の（設定 1）と（設定 2）ではシェア数の増加にともないデータパケット到達率が低下し，シェア数が適切でなければ中継ノードによるデータ窃取成功率も高くなっている．これに対し，シェア数としきい値の設定に提案法の経路特性を利用して導出した適合パラメータを設定した場合では，分散されるシェア数が大幅に増加しても，中継ノードによるデータ窃取成功率が低いまま高いデータパケット到達率を維持できることがわかった．

以上の実験結果と考察から，分散データ転送のパラメータの設定は経路の特性から適合パラメータを算出することが可能であり，その設定値を適用することで分散データ転送の効果は向上するといえる．

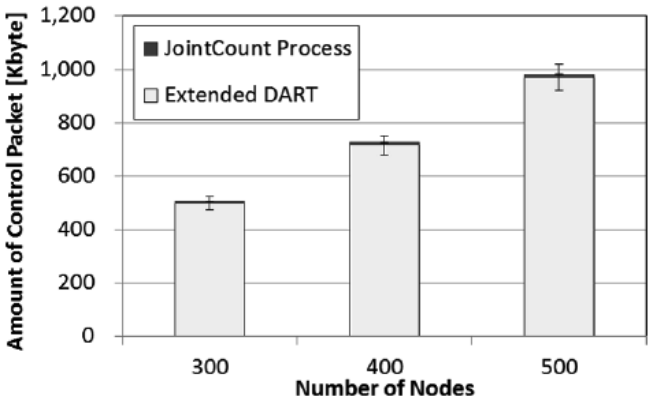


図 9: 制御パケット量

最後に，提案法による経路制御のネットワーク負荷について考察する．提案法の経路制御に用いた制御パケットの総量を図 9. に示す．内訳をみると，Joint Count プロセスに用いた制御パケット量は拡張 DART で用いた制御パケット量に対しわずかであり，Joint Count プロセスは既存の経路制御手法に加えてもネットワークへ与える負荷はわずかである．また，拡張 DART は他の経路制御手法より少ない制御パケット量で経路の構築を行う[8]．したがって，拡張 DART と Joint Count プロセスを組み合わせた提案法は少ない制御パケット量で経路制御が可能であるといえる．

10. ID の偽造への対抗手法

10.1 送信元ノード ID の偽造への対抗手法

認証情報として送信元ノードの隣接ノードアドレス群を格納した BF（以降 AIBF（Authentic Information Bloom Filter)）を用いる[10]．この手法では，まず送受信ノード間でコントロールパケットにより AIBF を宛先ノードへ転送する．その後，AIBF を格納したデータパケットを転送する．データパケットを受信した宛先ノードは AIBF を比較することで送信元ノード ID の偽造を検知する．この提案法は以下の 3 つの手順からなる．

1 転送経路と送信元ノードの認証情報の作成
2 送信元ノードによる認証情報の通知
3 データパケット転送と認証情報の比較

以降，提案法の手順について詳説する．

1. 転送経路と送信元ノードの認証情報の作成：まず，送信元ノードは SRIDR [8] によって経路表を作成する．SRIDR は単一経路構築手法である DART（Dynamic Address Routing）を拡張した複数経路構築手法である．その後，作成した経路表から AIBF を作成する．

2. 送信元ノードによる認証情報の通知：送信元ノードは宛先ノードへ認証情報を転送するために AN（Authentication Notify）シェアを作成する．送信元ノードが転送する AN シェアの改ざんの有無を宛先ノードにおいて判定するため，AIBF のハッシュ値(以降 AIBFHASH（AIBF Hash)）を作成する．送信元ノードは AN シェアに AIBF と AIBFHASH のシェアを格納し，複数経路を用いて AN シェアを宛先ノードへ転送する．AN シェアを受信した宛先ノードは復号を行い，AIBF’と AIBFHASH’ を生成する．復号に成功した宛先ノードは AIBF’ の改ざんの有無を判定する．AIBF’ の改ざんの有無を判定するため，AIBF’をハッシュ値（以降 AIBF’HASH）に変換する．そして，AIBF’HASH と AIBFHASH’ を比較し一致した場合，AIBF’ の改ざんは無いと判断し，AIBF’ を保存する．

3. データパケット転送と認証情報の比較： 宛先ノードが AIBF’ を保存した後，送信元ノードは宛先ノードへのデータパケットの転送を開始する．データパケットには AIBF，AIBFHASH，データのそれぞれのシェアが含まれている．宛先ノードはシェアの復号により AIBF” 等を生成する．データパケットを受信した宛先ノードは AN シェア取得時と同様に，AIBF” の改ざんの有無の判定を行う．そして，AIBF” が改ざんされていないと判断した場合，宛先ノードは受信したデータパケットから復号した AIBF” と，AN シェア受信時に保存した AIBF’ を比較することでなりすましの検知を行う．不一致だった場合，宛先ノードは受信したデータパケットが攻撃ノードにより生成されたものと判断する．

10.2 送信元ノード ID の偽造への対抗手法

この提案法[13] では往路のパケット（以降 REQ パケット）と復路のパケット（以降 REP パケット）を使用する．これらのパケットには BF を格納するフィールドがあり，中継ノードは自身の経路表を BF に格納し転送する．そして，送信元ノードにおいて REQ パケットと REP パケットの BF を比較することで経路認証を行い，攻撃ノードを検知する．提案法は以下の 3 つの手順に分けることができる．

1. REQ パケットの転送
2. REP パケットの転送による受信応答
3. 経路認証

以降，提案法の各動作について詳説する．

1. **REQ パケットの転送：**まず，送信元ノードは複数の REQ パケットを作成し，REQ パケットを宛先ノードへ複数経路を用いて転送する．この時，REQ パケットは中継ノードの経路表を BF に格納していく．
2. **REP パケットの転送による受信応答：**REQ パケットが宛先ノードに全て到達すると，宛先ノードは REQ パケットが持つ BF を連結させる．この連結した BF を認証情報とする．宛先ノードは認証情報である BF を秘密分散法によって暗号化し，REP パケットに格納し，送信元ノードへ転送する．REP パケットの転送には REQ パケット転送時の複数経路を用いる．その手順は次の[その 1]，[その 2]に従う．[その 1]：まず，送信元ノードの隣接ノードへ REP パケットを転送する．[その 2]：[その 1] で指定したノードに到達すると，送信元ノードへ直接 REP パケットを転送する．REP パケットは REQ パケット転送時と同様に，自身の BF に中継ノードの経路表を格納する．
3. **経路認証：**送信元ノードは全ての REP パケットの受信後，暗号化された BF の復号と，REP パケット転送時に作成した BF の連結を行う．復号した BF と連結した BF を比較し，一致すれば攻撃ノードは経路上に存在しないと判断する．一方，一致しなければ攻撃ノードが経路上に存在すると判断する．

10.3 シミュレーション実験

提案法の効果を確かめるため，提案法をシミュレータ上に実装し，以降に示す実験を行った．表 1 に送信元ノード ID の偽造の検知手法（以降実験 1）と中継ノード ID の偽造の検知手法（以降実験 2）の実験パラメータを示す．実験 1 では分割するシェアの個数を，送信元ノードの全隣接ノード数 n の半数とし，しきい値を(シェアの個数-1) とした．AIBF にデータを格納する際に使用するハッシュ関数の個数 k を，n と AIBF 長 m から計算式(mn) _ $\log_e(2)$ より求め，計算結果に最も近い整数を k とする．一方，実験 2 ではシェア数は 4，しきい値は 3 とした．

実験 1 の攻撃ノードの動作：フィールド内の送受信ペア以外のノードを全て攻撃ノードとする．攻撃ノードが AIBF の復号に成功した場合，復元した AIBF を使用し，宛先ノードへ偽造パケットを転送する．一方で失敗した場合，AIBF のビット毎に乱数により 1 か 0 を任意に格納することで，送信元ノードの AIBF の偽造を試みる．そして，偽造した AIBF を用いて宛先ノードへデータパケットを転送する．

実験 2 の攻撃ノードの設定と動作：REP パケット作成時，各経路上の 1 つの中継ノードを攻撃ノードとしてランダムに選択する．攻撃ノードは REP パケットを受信すると，受信した REP パケットの BF に対して次の動作を行う．

その 1 乱数により作成した経路情報を BF に格納

その 2 BF に何も格納しない

図 10 と図 11の x 軸は共にシミュレーションにおけるフィールド内のノード数である．図 10 と図 11 の y 軸はそれぞれ送信元ノード ID の偽造の検知成功確率と，中継ノード ID の偽造の検知失敗確率を示す．

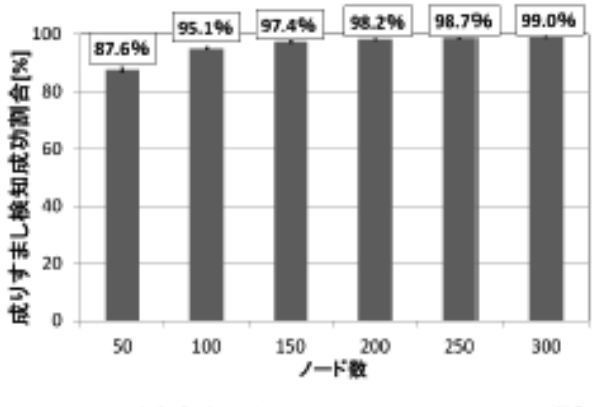


図 10: 送信元ノード ID 偽造の検知成功割合

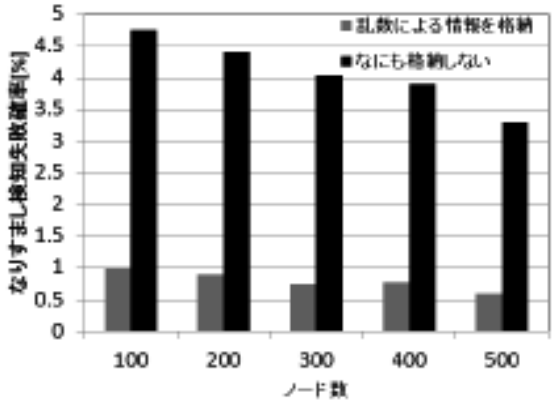


図 11：中継ノード ID 偽造の検知失敗確率

11. まとめ

本稿では，ノードキャプチャ攻撃を回避するため，分散データ転送の性能の向上を目指した．重複の少ない複数経路の構築手法を新たに提案し，また，分散データ転送の性能を上げるための条件に適合するようなパラメータの設定値について，提案法で構築される経路の特性を利用し導出した．提案法と適合パラメータを使用した際の分散データ転送の性能を評価するためシミュレーション実験を行い，その有効性を示した．

また，ノード ID の偽造に対抗する手法として BF を用いた認証データによって検知する手法を提案した．図 10，図 11 共に，ノード数の増加に伴い提案法の効果が上がることが分かった．

【参考文献】

［1］ I.Stojmenovi´c (ed.), “Handbook of sensor networks: algorithms and architectures,” Wiley, 2005.

［2］ W.Zhang, et al., “Security in wireless sensor networks: a survey,” In Security in Sensor Networks, Y.Xiao ed., Auerbach Publications, pp.237-272, 2007.

［3］ A. Shamir, “How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

［4］ G. R. Blakley, “Safeguarding cryptographic keys," in *American Federation of Information Processing Societies National Computer Conference*, vol. 48, Arlington, Virginia, USA, September 1979, pp. 313-317.

［5］ E. Kohno, T. Okazaki, M. Takeuchi, T. Ohta, Y. Kakuda, and M. Aida, “Improvement of the security against node capture attacks using dispersed data transmission for wire-less sensor networks," in *Proceedings of the Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing (UIC-ATC 2010)*, Xi'an, China, Oct. 2010, pp. 340-345.

［6］ E. Kohno, T. Ohta, Y. Kakuda, and M. Aida, “Improvement of dependability against node capture attacks for wire-less sensor networks," *IEICE Transactions on Information and Systems*, vol. E94-D, no. 1, pp. 19-26, Jan. 2011.

［7］ B.H.Bloom, “Space/time trade-offs in hash cording with allowable errors,” Communications of the ACM, vol.13, no.7, pp.423–426, 1970.

［8］ T. Okazaki, E. Kohno, T. Ohta, and Y. Kakuda, “A multipath routing method with dynamic ID for reduction ofrouting load in ad hoc networks." in *ADHOCNETS'10*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, J. Zheng,D. Simplot-Ryl, and V. C. M. Leung, Eds., vol. 49, no. 2,2010, pp. 114-129.

［9］ S. Motegi and H. Horiuchi, “AODV-based multipath routing protocol for mobile ad hoc networks," *IEICE Transactions on Communications*, vol. E87-B, no. 9, pp. 2477-2483,Sep. 2004.

[10] Scalable Network Technologies, Inc., “QualNet network simulator." [Online]. Available: http://www.scalable- networks.com/
[11] A. Kimura, E. Kohno, and Y. Kakuda, “Security and dependability enhancement of wireless sensor networks with multipath routing utilizing the connectedness of joint nodes," in *Proc. 32nd International Conference on Distributed Computing Systems Workshop (ICDCSW 2012),at the Eleventh International Workshop on Assurance in Distributed Systems and Networks (ADSN2012)*, China, Macau, 2012, pp. 342-348.
[12] N. Tanabe et al., “An impersonation attack detection method using bloom filters and dispersed data transmission for wireless sensor networks,” Proc. 2012 IEEE International Conference on Green Computing and Communications (GreenCom), pp.767–770, Nov. 2012.
[13] N. Tanabe et al., “A path authenticating method using bloom filters against impersonation attacks on relaying nodes for wireless sensor networks,” Proc. 33rd International Conference on Distributed Computing Systems (ICDCS) Workshops, pp.357–361, July 2013.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
On parameters for the secure dispersed data transfer scheme using a multipath routing method	Proc. 34th International Conference on Distributed Computing Systems (ICDCS 2014), The Thirteenth International Workshop on Assurance in Distributed Systems and Networks (ADSN2014)	2014 年 6 月
A self-organized approach for the communication method to adapt connectivity of terminals in Bluetooth MANETs	Proc. 17th IEEE Symposium on Object/Component/Service-oriented Real-time Distributed Computing(ISORC2014), 5th IEEE Workshop on Self-Organized Real-Time Systems (SORT2014)	2014 年 6 月
Tree structured group ID-based routing method for mobile ad hoc networks	Proc. NexComm 2014, The Thirteenth International Conference on Networks (ICN 2014)	2014 年 2 月
Experimental evaluation of the effects with backtrack search and notification messages in the node-disjoint multipath scheme for secure dispersed data transfer method	Proc. Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU 2014)	2014 年 1 月
A node-disjoint multipath scheme for secure dispersed data transfer in ad hoc networks	Proc. First International Symposium on Computing and Networking (CANDAR'13), 6th International Workshop on Autonomous Self-Organizing Networks (ASON'13)	2013 年 12 月
The assessment information acquisition and dissemination system based on delay and disruption tolerant MANETs for the hiroshima national confectionery exposition	Proc. First International Symposium on Computing and Networking (CANDAR'13), 6th International Workshop on Autonomous Self-Organizing Networks (ASON'13)	2013 年 12 月
A path authenticating method using bloom filters against impersonation attacks on relaying nodes for wireless	Proc. 33rd International Conference on Distributed Computing Systems Workshops	2013 年 6 月

sensor networks	(ICDCSW2013), the Twelfth International Workshop on Assurance in Distributed Systems and Networks (ADSN2013)	
An impersonation attack detection method using bloom filters and dispersed data transmission for wireless sensor networks	Proc. 2012 IEEE International Conference on Green Computing and Communications (GreenCom 2012), Conference on Internet of Things (iThings 2012), and Conference on Cyber, Physical and Social Computing (CPSCom 2012), at Workshop on Security of Systems and Software resiliency (3SL 2012)	2012 年 11 月
A routing ID-based node-disjoint multipath scheme for ad hoc networks	Proc. 2012 9th IEEE International Conference on Autonomic and Trusted Computing (ATC 2012), The Third International Symposium on Multidisciplinary Emerging Networks and Systems (MENS2012)	2012 年 9 月
An assurance enhanced route-split routing for non-uniform node density in mobile ad hoc networks	Proc. 2012 9th IEEE International Conference on Autonomic and Trusted Computing (ATC 2012), The Third International Symposium on Multidisciplinary Emerging Networks and Systems (MENS2012)	2012 年 9 月
A New Generation Children Tracking System Using Bluetooth MANET Composed of Android Mobile Terminals	Proc. 2012 9th IEEE International Conference on Autonomic and Trusted Computing (ATC 2012)	2012 年 9 月
Security and dependability enhancement of wireless sensor networks with multipath routing utilizing the connectedness of joint nodes	Proc. 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW 2012), at the Eleventh International Workshop on Assurance in Distributed Systems and Networks (ADSN2012)	2012 年 6 月
ノード密度の異なるアドホックネットワークに対する適応性の向上を目指すセキュア分散データ転送のための複数経路制御手法	電子情報通信学会 アシュアランスシステム研究会	2013 年 12 月
静的なアドホックネットワークにおけるノード密度の変化への追従を目指す セキュア分散データ転送のための複数経路制御方式	第 15 回 IEEE 広島支部学生シンポジウム	2013 年 11 月
アドホックネットワークにおけるセキュア分散転送を想定したノード素な複数経路構築手法の評価	電子情報通信学会 ディペンダブルコンピューティング研究会	2013 年 10 月
アドホックネットワークにおけるセキュア分散転送を想定したノード素な複数経路	電子情報通信学会 ネットワークシステム研究会	2013 年 10 月

構築手法の評価		
無線センサネットワークにおける Bloom Filter を用いた経路認証に関する実験的評価	電子情報通信学会 2013 年ソサイエティ大会	2013 年 9 月
重複回避メッセージを用いたアドホックネットワークのためのノード素な複数経路構築手法の実験的評価	電子情報通信学会 2013 年第 1 回アシュアランスシステム研究会	2013 年 5 月
アドホックネットワークにおけるセキュア分散データ転送のための経路重複ノード数を低減する複数経路に関する考察	電子情報通信学会 情報ネットワーク研究会	2013 年 3 月
ワイヤレスセンサネットワークにおける秘密分散法を用いたセキュア分散データ転送とその応用	電子情報通信学会 第 18 回ネットワークソフトウェア研究会	2013 年 1 月
ワイヤレスセンサネットワークにおける BloomFilter を用いた経路認証手法の実験的評価	電子情報通信学会 アシュアランスシステム研究会	2012 年 12 月
無線センサネットワークにおける分散データ転送のための重複を低減する複数経路の構築とノードの経路分岐数通知によるパラメータ設定方式	電子情報通信学会 ディペンダブルコンピューティング研究会	2012 年 10 月
アドホックネットワークのためのノード素な複数経路による分散転送手法の評価	電子情報通信学会 第 17 回ネットワークソフトウェア研究会	2012 年 10 月
無線センサネットワークにおけるハッシュ関数群と分散転送を用いた偽造パケット挿入によるなりすまし検知手法	電子情報通信学会 2012 年ソサイエティ大会	2012 年 9 月
ルーティング ID と後戻り探索軽減メッセージを用いたアドホックネットワークのためのノード素な複数経路構築法	電子情報通信学会 第 16 回ネットワークソフトウェア研究会	2012 年 6 月