情報理論的安全性に基づく通信方式の設計と評価

津田 航[1,a)]　堀 良彰　櫻井 幸一

概要：計算量的安全性によって成り立つ暗号は現状では十分な安全性を持っているため，この安全性を満たす暗号を用いた通信が主流となっている．しかしながら，現代のめざましい計算機の発展を考慮すると，攻撃者の計算能力が高くなり，計算量的安全性によって成り立つ暗号は安全でなくなる可能性がある．本研究では計算量的安全性に比べ，より強力な安全性を確立できる情報理論的安全性によってなりたつ完全安全性通信方式に着目した．マルチホップ無線通信を用いた，完全安全性通信方式について，攻撃者の種類とパケットロスを考慮したシミュレーションによって評価を行い，完全安全性通信方式を実装した際に必要となる通信量を明らかにした．

キーワード：秘密分散，ワイヤレスセンサネットワーク，情報理論的安全性，完全安全性通信

Design and evaluation of a communication method based on information theoretic security

Abstract: The mainstream encryption are based on computational safety has enough safety. However, if the computing power of the adversary becomes higher, the encryption may not be safe. In this study, we focus on PSMT(Perfectly Secure Message Transmission) which based on informational theorentic security that could establish the safety stronger than computational safety.We evaluated the PSMT using the multi-hop wireless communication by simulation.

Keywords: secret sharing,wireless sensor network,information theoretic security,PSMT

1. はじめに

近年インターネットの普及に伴いセキュリティの需要が増加している. セキュリティを向上させる手法として，以下の２つの手法があげられる．

(1) 通信路の安全性を確保する．

(2) 安全でない通信路上では暗号を用いた通信を行う．

現代の主流の通信方式においては，後者の手法がとられており，公開鍵暗号や共通鍵暗号が使われている．しかしながら，例えば公開鍵暗号で必要となる公開鍵暗号基盤は第三者機関が必要になり，余分なコストと時間が必要となることに加え，第三者機関が攻撃者に狙われて利用されたという報告も上がっており問題になっている．さらに，現代のめざましい計算機の発展を考慮すると，攻撃者の計算能力が高くなり，計算量的安全性によって成り立つ公開鍵暗号や共通鍵暗号は安全でなくなる可能性がある．そこで本研究では計算量的安全性よりも，より強力な安全性を確立できる情報理論的安全性によってなりたつ暗号技術に着目する．情報理論的安全性をもつ暗号を用いた通信方式として完全安全性通信方式や量子暗号，ワンタイムパッドが存在する．その中でも，完全安全性通信方式は複数の非連結経路を構築すれば実装は容易である．しかしながら，完全安全性通信方式を実装する為に必要となる通信量コストと経済的コストが大きいという理由により，完全安全性通信方式は理論研究を主としていて，実装は行われていない．本研究では攻撃者の種類とパケットロスを考慮したシミュレーションによって評価を行い，完全安全性通信方式を実装した際に必要となる通信量について調査を行った．

[1] 九州大学工学部電気情報工学科
Department of Electrical Engineering and Computer Science, Kyushu University
[2] 九州大学システム情報科学府情報学専攻
Department of Imformatics, Kyushu University
[a)] tsuda@itslab.inf.kyushu-u.ac.jp

2. 関連知識

2.1 ワイヤレスセンサネットワーク

ワイヤレスセンサネットワークとは通信を行いたい対象の周辺領域にノード (センサ付無線端末装置) 群を設置し，ノードが持つ中継機能を使って他のノードを経由する事で端末同士が直接通信するだけでなく，より広い範囲の端末と通信を可能にするネットワークである．ワイヤレスセンサネットワークはアドホック機能と，各ノードからノードへデータを送るためのルーティング機能の２つを有している．

2.2 秘密分散法

秘密分散法は，シャミアにより提案されたリスク分散の為に情報を分散して管理し，その一部が流出したり漏えいしても元の情報を推測できないようにするセキュリティ技術である．秘密分散法では，まず元のデータをシェアと呼ばれる複数の分散データに分け，シェアを別々に管理する．次に複数のシェアに分けられた元データを得る為には，分散したデータをある一定数以上集めないと復元する事ができない．

2.2.1 (k, n) 閾値秘密分散法

元のデータを s とし，$v_1, v_2, v_3, ...v_n$ のシェア n 個に分けたとすると，(k, n) 閾値秘密分散法では以下の２つの条件を満たす．

(1) n 個に分散されたデータのうち，任意の k 個からのシェアで元のデータ s を復元できる．
(2) 任意のシェアを $k-1$ 個集めたとしても，s を復元することができない．

2.3 set systems

本項は完全安全性通信方式の構築に必要となる，set system について紹介する [4]，[8]，[3]．

2.3.1 定義１

$X := 1, 2, ..., n$ であり，B は $B_i \subset X$ を満たす，ブロック $B_i (i = 1, 2, .., b)$ の集合である．以上を満たす組み合わせ (X, B) を set system と呼ぶ．完全安全性通信方式では，X は構築したすべての経路の集合，B は経路の組み合わせの集合を意味する [8]．

Desmedt らは set system を用いて，以下の様に定義している [4]．

2.3.2 定義２

以下の条件を満たすとき，(X, B) を (n, b, t)-verifiers set system と呼ぶ．

(1) $|X| = n$
(2) $|B_i| = t + 1 (i = 1, 2, ..., b)$

	鍵を共有しなければならない	鍵を共有する必要がない
計算量的安全性	秘密鍵暗号	公開鍵暗号
情報理論的安全性	ワンタイムパッド	PSMT

図 1 暗号を用いた通信方式

(3) 部分集合 F が $F \bigcap B_i = \emptyset$ であり，$F \subset X, |F| \geq t, \exists B_i \subset B$ を満たす．
b は $b =_{n-1} C_{t+1}$ であり，t は構築した経路のうち攻撃者が存在する経路の数，F はブロックの構成要素の経路にすべて攻撃者が潜んでいる部分集合である．

Erotokritou らは (n, b, t)-verifiers set system をより一般的な形で以下の様に定義している [3]．

2.3.3 定義３

以下の条件を満たすものを (n, b, t', t)-verifiers set system とする．

(1) $|X| = n$
(2) $|B_i| = t' + 1 (i = 1, 2, ..., b)$
(3) 任意の部分集合 F が $F \bigcap B_i = \emptyset$ において $F \subset X, |F| \geq t, \exists B_i \subset B$

(n, b, t', t)-verifiers set system では，ブロックを構成している経路の数に対してある程度の自由度を持たせている．つまり, 経路構築の際，経路数 n が $n \leq 2t + 1$ を満たし、$n - (2t + 1) = i$ と仮定したとき，定義 3 における t' は $t \leq t' \leq t + i$ の値をとる．

(n, b, t)-verifiers set system と (n, b, t', t)-verifiers set system はブロックの集合に対して，少なくとも一つのブロックは攻撃者が支配している t の要素を含まない事を示す重要な特性である．したがって完全安全性通信方式において，通信を成功させる為の条件として，(n, b, t)-verifiers set system または (n, b, t', t)-verifiers set system を満たす必要がある．

3. 既存研究

完全安全性通信方式は，以下の性質を同時に満たす．

(1) 可用性：必要時に許可された者が確実に情報にアクセスできる環境である事．
(2) 機密性：アクセスを認可された者だけが情報にアクセスできるようにする事．
(3) 完全性：情報および処理方法が正確であることおよび

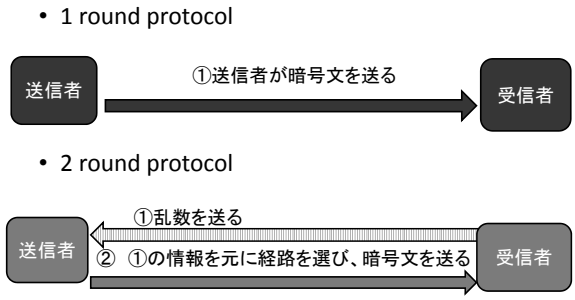

図 2 PSMT のプロトコルの種類

完全であることを保護する事.

完全安全性通信方式 (Perfectly Secure Message Transmission) は図 1 に位置付けられる暗号である [1], [14]. 以下完全安全性通信方式は PSMT と表記する. 現在の主流の暗号方式が計算量的安全性に基づく暗号であるのに比べ, より強力な情報理論的安全性に基づいており, さらに事前に鍵を共有する必要がないという利点をもつ.

PSMT は以下の 2 つの条件を満たす.

(1) 攻撃者は暗号文に関して情報を一切得ることができない.

(2) 受信者が受け取る暗号文は完全に信頼できる.

PSMT の研究では, 様々なネットワークモデルにおけるプロトコルの特性や, 様々な攻撃者を想定した上で安全性を向上させるプロトコルについて考案されている. 通信方式にも図 2 に示すように, 1-round, 2-round といった様々なプロトコルが存在する. 1-round 方式は, 送信者が受信者へ一方的に暗号文を送るのプロトコルであるため, 受信者から送信者に対して連絡を取ることはない. 2-round 方式は送信者と受信者が相互に連絡を取り合い, 通信を行うプロトコルとなっている.

送信者と受信者が通信に用いる経路の総数を n 本とし, そのうち攻撃者に支配されている経路の本数を t 本とすると, 1-round では $n \geq 3t+1$, 2-round では $n \geq 2t+1$ を満たす n が必要十分条件である事が証明されている [1].

3.1 HPSMT(Human Perfectly Secure Message Transmission)

HPSMT は従来の PSMT と比較して, コンピュータを使わず人でもに元の暗号文にもどせるほど, 簡単な秘密分散を使用しており, 従来の PSMT にくらべて計算量を削減することができる. よって, 本研究において用いる PSMT のプロトコルは HPSMT（Human Perfectly Secure Message Transmission）を採用している [3]. HPSMT に用いられている秘密分散は (n,n) 閾値秘密分散法を利用している. メッセージ Ms に秘密分散を適用し, $s_1, s_2, s_3, ...s_n$ のシェアに分ける場合, (n,n) 閾値分散法では以下の条件を満たす.

(1) n 個すべてのシェアを集めることで, メッセージ Ms を復元できる.

(2) 任意の分散データを $n-1$ 個集めたとしても, Ms を復元することができない.

HPSMT で用いる秘密分散は以下の式で示される.

$\forall \in 1, 2, ..., k : D_i(s) = \Sigma_{j=1}^{n} D_i(s_j) mod |A|$

s:メッセージの一部

$s_j (1 \leq j \leq n)$:n 個に分散されたデータ

$k : s$ の桁数

$|A|$ は通信で送りたい情報によって変化する. 仮に A の要素が 0, または 1 であるとき, 送る情報は 0 または 1 の 2 進数の値となる. また, A の要素が 0 から 9 の場合, 送る情報は 0 から 9 の値で構成される 10 進数となる. この秘密分散はシャノンによって成り立つ事が証明されている [2].

3.1.1 Mod 10 を用いた 2-round HPSMT protocol

Mod 10 を用いた 2-round HPSMT protocol について紹介する. 攻撃者のモデルとして, 攻撃者は通信路に存在しており, その通信路を通るシェアの値を改ざんする. 暗号文を送る人を送信者, それを受け取る人を受信者, 両者間を n 本の非連結経路でつながれているものとし, 構築した経路うち攻撃者が潜んでいる経路の本数を t 本とすると, n は $n \geq 2t+1$ の関係を満たすものとする. これは $n \geq 3t+1$ の関係を満たす必要がある 1-round 型と比較すると, 必要となる通信路の経路の数が少なくて済む. 以下にプロトコルを述べる.

step1:受信者は各ブロック $B_1, B_2, ..., B_b$ に対して $(Z_{10})^k$ からランダムに要素 r_i を選択する. $|B_i| = x_{i_1}, x_{i_2}, ..., x_{i_{t'}} (1 \leq i \leq b)$ であるとき, 受信者は B_i を構成する全ての $x_{ij} (1 \leq j \leq t')$ に対して r_i を与えて送信者へ送る.

step2:送信者は受信者から受け取った, すべて同じ値であるべき $x_{i_1}, x_{i_2}, ..., x_{i_{t'}}$ が, 一つでも異なっていた場合そのブロックをブラックリストに登録する. これを B' とする. 送信者は B から B' を除いた集合 $B''(B'' = B - B')$ を作成する. ここで, $B'' = B_{j_1}, B_{j_2}, ..., B_{j_l}$ とすると, 送信者は B'' から受け取った r_i の和, $r = r_{j_1} + r_{j_1}, ... + r_{j_l}$ を計算し, 受信者へ送りたいメッセージ M_s を足し合わせた $V = r + M_s$ の関係を満たす, V とブラックリスト B' を受信者へ送る.

step3:受信者は受け取ったブラックリスト B' より, 攻撃者が潜んでいないブロックを見つける事ができ, s の値を計算する事ができる. また受け取った $V = r + M_s$ により, 送信者が送った M_s の値を得る事が可能である.

3.2 PSMT の問題点

PSMT 全体の問題点として以下の 2 つがあげられる．

(1) データを分散して伝送する為，オーバヘッドが存在し通信量が増加してしまう．

(2) 現在のネットワーク上で非連結経路を複数確保する事は難しい．

通信量の問題点に関して，通信量を減らす事を目的とした既存研究が存在する [5]，[6]，[7]．PSMT は 1993 年にはじめて提唱されており，その時点での通信量は 2-round では $O(2^n)$ となっており，1-round では $O(n)$ であった．これ以降 1-round プロトコルに関する通信量は改善されておらず，現在のところ 1-round においては最も通信量が少ないプロトコルとされている．しかしながら，2-round プロトコルの必要とする経路数 $n \leq 2t+1$ と比較すると，1-round プロトコルで必要となる経路数は，$n \leq 3t+1$ となり 2-round プロトコルよりも多くなるという欠点を持っている．想定する攻撃者の数 t が少ない場合に関しては大きな影響を与えるとは言えないが，t の値が大きくなるにつれて必要となる経路数の差が大きくなってくる為，本項で挙げている PSMT の問題点 (2) の解決が困難になる．また，現在のネットワークは複雑な構造となっており，パケットが通る経路を把握することは非常に難しい．さらに，現在のネットワークのパケット転送において、経路を指定する事は難しく，PSMT で必要となる非連結経路を複数構築する事は困難であるといえる．

4. SPREAD(Security Protocol for REliable dAta Delivery)

SPREAD(Security Protocol for REliable dAta Delivery) は信頼できるデータ転送を行う事を目的としており，秘密分散と非連結な経路を使ってデータを送ることによって通信の安全性を高めている [10]．SPREAD では無線 LAN の状況やデータリンク層でのフレームの衝突，古い経路情報によってパケットが紛失する可能性が高い事を考慮して，安全性と冗長性を両立させるために (k,n) 閾値秘密分散法を適用している．SPREAD の安全性は分散値を各経路に分散させる事によって，向上させている．しかしながら，冗長性を高める為に k の値を小さくすると安全性が高くなり，逆に，安全性を高める為に k の値を大きくすると，冗長性が失われる．SPREAD では，適切な (k,n) を選ぶことによって，安全性と信頼性を両立する事を目指しており，非連結経路を構築するためにソースルーティングとオンデマンド マルチパス ルーティングを使用している．

4.1 経路構築の流れ

SPREAD の経路構築の流れを記す．

Step1:修正ダイクストラ アルゴリズムによって最も安全な経路を探す．

Step2:

a. 経路のリンクを送信者の方向を指したリンクへ取り換える．変えたリンクのコストは元のコストの負の値にする．元のリンクは取り除く．

b. 経路に使われているノードを二つに分割し，併置する．ふたつのノードをコスト 0 のリンクでつなぐ．

c. 元のリンクとつないでいる各外部リンクを同じコストで取り換える．

Step3:修正ダイクストラ　アルゴリズムを適用し，Step2 までに変換されたグラフの中で最も安全な経路を構築する．ここで経路が発見できなかった場合は Step6 へ移行する．

Step4:node やリンクを元の状態のグラフへ戻す．

Step5:新しい経路の安全性を計算し，前回の経路と比較を行う．新しい経路群が前のセットよりも安全性が向上してなければ，Step 6 へ移行する．そうでなければ，経路を記録して Step2 へ戻る．

Step6:経路群を記録し，プロトコルを終了する．

4.2 SPREAD における攻撃者のモデル

SPREAD ではワイヤレスセンサネットワークにおいて改ざんの攻撃を行った場合，intrusion mechanism や watchdog によって，攻撃者が見つかる危険性が大きくなる為，攻撃者はデータの盗聴は行うが，改ざん等は行わないものと想定している [11]，[12]．

5. 提案手法

秘密分散法を用いた通信方式である SPREAD は仮に攻撃者が改ざんを行う場合，通信が失敗する可能性がある．一方，PSMT は情報理論的安全性に基づく強力な安全性を満たしており，改ざんを行う攻撃者が存在する場合に対しても，問題なく通信を行う事ができる．しかしながら，PSMT の通信を行う際は非連結な経路を確保する必要がある．仮に，有線で非連結経路を構築すると仮定すると，通信相手ごとに有線でつなぐ必要があり非常にコストが大きくなる為，実装を行うには非現実的である．一方ワイヤレスセンサネットワークを用いる場合，通信相手ごとに経路を構築する事が容易である，それに加えて，ワイヤレスセンサネットワークは基地局が不用であるため，基地局のない地域でも安価にネットワークの利用が可能となる．よって，PSMT の問題点の 1 つである非連結経路の構築に有効であるといえる．そこで，本研究では非連結経路構築方法として，ワイヤレスセンサネットワーク上で非連結経路を構築する事ができる SPREAD を用いる．しかしながら，ワイヤレスセンサネットワークを用いる場合，有線の通信と比べパケットドロップ率が高くなってしまう．よって本

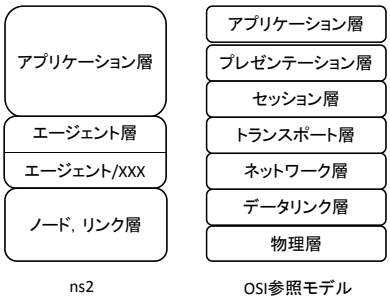

図 3 OSI 参照モデルと ns のレイヤー構成比較

研究では，ネットワークシミュレータを用いて仮想ネットワークを構築を行い，その仮想ネットワーク上でワイヤレスセンサネットワークを用いた PSMT の通信量について，攻撃者の種類とパケットドロップ率に基づき，評価を行うことで PSMT を実装した際に必要となる通信量について明らかにする．

5.1 ネットワークシミュレータ

ネットワークシミュレーションはネットワーク技術を研究する基本的な方法の一つである．本実験では PSMT を用いた新しいプロトコルの開発と評価を行う為に, ns-2(Network Simulator 2) を用いた．

現実世界においてネットワークを構築するにはコストと時間を要する． そこで，コンピュータ上で仮想ネットワークを構築して 実験を行い，その結果を可視化することができるネットワークシミュレータの ns-2 が広く利用されている．本研究では参考文献や資料が多数存在する ns-2 を用いてネットワークを構築し，その上で PSMT を用いたアプリケーションのシミュレーションを行う [13]．ns-2 において新しいアプリケーションの開発を行う際には ns-2 のネットワークモデルのレイヤー構成について意識しなければならない．ns-2 のレイヤー構造は図 5.1 の様になっており，OSI 参照モデルと比較すると ns-2 の階層は 3 つしか存在しない．

ノード，リンク層では，ノードの数や，ノードの接続先，ノード間をつなぐ経路の帯域や遅延時間等の設定を行うことができる．ノードは複号オブジェクトとなっており，入口オブジェクトと分類機構によって構成されている．ノードにはユニキャストノードとマルチキャストノードの 2 種類のモデルが存在し，マルチキャストはユニキャストノードの機構に加え，マルチキャストルーティングを行うためのマルチキャストアドレス分類機構を備えている．本実験では，情報理論的安全性に基づく通信に関する通信量を明らかにする事を目的としているが，経路構築に必要な通信量と，メッセージを送るのに必要となる通量はそれぞれ独立したものとみなせる．本来であればノードは周囲のノードの状況に影響し経路を変更するため，マルチキャストノードが適している．しかし，本実験においてはまず後者の通信量について明らかにするために，経路はすでに構築されたものとして扱うため，ユニキャストノードを使用している．リンクも同様に複号オブジェクトとなっており，単方向の通信である simplex-link，双方向通信が可能である duplex-link を選択する事ができる．本実験では，中継ノードにおいてパケットが失われる事を考慮して，パケットを失った際に送信者にパケット再送要求を行う為に，duplex-link を選択している．

エージェント層は OSI のトランスポート層とネットワーク層の機能を担っている．この層の UDP や TCP 等のプロトコルをノードリンク層のノードに与える為に，シナリオスクリプトで該当するオブジェクトをノードオブジェクトに attach-agent で与える事ができる．シナリオスクリプトとは，プログラムの通信が何秒後に開始し，停止するか等のシナリオが記述されたものである．本実験は，ワイヤレスセンサネットワークを想定している．よって，ノードにおいてパケットが失われる機会が増加する為，パケットが相手に届く可能性は低くなってしまう．ブロードキャストやマルチキャストを実現するために用いるエージェントは，信頼性は低いが，効率性が高い通信に適している UDP を使用する．また，エージェント層よりも上位層のアプリケーション層において，パケット再送要求機能等のエラー修復機能を持たせる事によって，信頼性を向上させている．

アプリケーション層では, FTP, CBR, Telnet, HTTP などさまざなフロータイプが定義してあり，利用する際に該当する下層のエージェント層のプロトコルに attach-agent を使って，関連づける必要がある．本実験では新しいアプリケーションを開発する為，アプリケーション層とエージェント層とのインターフェイスについて新たに定義する必要がある．

5.2 実験シナリオ

実験のモデルとして，短距離での機密性の高い無線通信を想定する．具体的には，任意のノードから半径 1 キロ以内にあるノードとの無線通信について検討を行う．送信者，受信者それぞれのノードを node(S)，node(R) とし，また送信者と受信者の距離を 1 キロとする．node(S)，node(R) は UDP 上で動く PSMT を利用したアプリケーションを用いて通信を行い、送信者はメッセージ Ms を受信者へ送る．無線接続の方式として，IEEE802.11x 規格を使用するものと仮定する．IEEE 802.11x は，通信半径が 100m 程度と広いのが特徴を持つ．よって各ノードの最大無線通信可能距離は半径 100 メートルとする．隣接するノード間の距離を平均 80m と仮定し，経路 1 つを構成するノードの数は 12

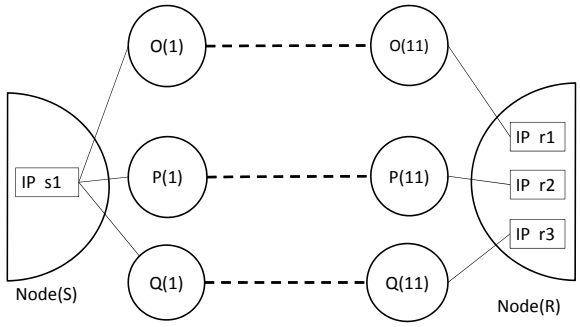

図 4 仮想ネットワーク構成図

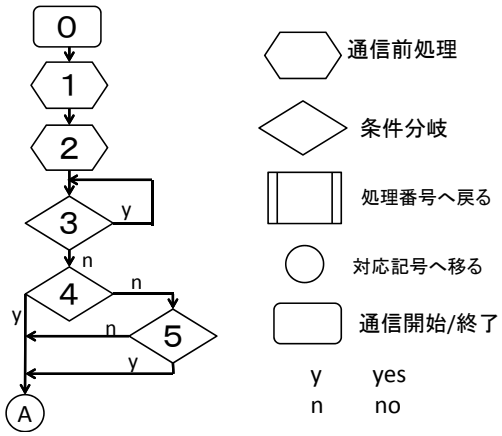

図 5 HPSMT を用いた通信のフローチャート 1

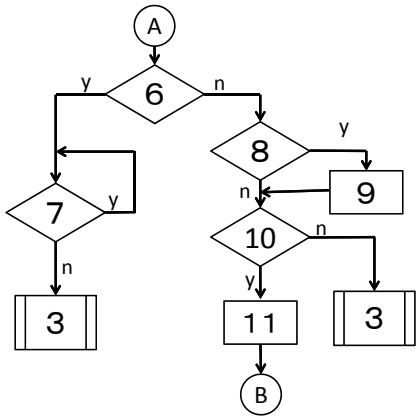

図 6 HPSMT を用いた通信のフローチャート 2

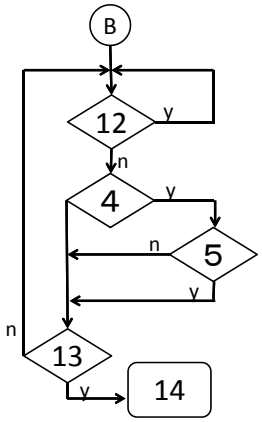

図 7 HPSMT を用いた通信のフローチャート 3

個とする．各ノードを通るパケットは，ある一定の確率でパケットを失う可能性をもつ．本実験では，まず HPSMT を利用する際に必要となる最低限の通信量を求める為に，必要となる通信路と攻撃者の数を最低の値にする．構築した経路の数を n，そのうち攻撃者が存在する経路を t とすると，$n \geq 2t+1$ の関係から通信に利用する経路の本数は３本とし，そのうちの１本に攻撃者が潜んでいるものとする．アプリケーション上でやり取りするメッセージは 1000 バイトで固定し，１パケットで送ることのできる程度の短いものであるとする．また，経路が１本の場合は，送信者は受信者にメッセージを送る際に，宛先の IP アドレス等を指定する．本実験においては複数の経路を用いるが宛先は同じである為，宛先によって経路を選択する事は困難である．解決方法として，考えられるものを２つ述べる．

１つ目は各経路に対してフロー ID と呼ばれる識別子を与え，それを送信者側で選択し，パケットのヘッダーに情報を与える．これによってノードはフロー ID によってパケットを渡す経路を選択することができる．

２つ目は受信者に複数の宛先を持たせることである．受信者はＩＰアドレス等を複数持ち，どの経路から届いたメッセージか判断できる環境ならば通信が可能となる．本実験では後者の方法を採用している．ネットワークの構成図を以下に示す．

本実験で流れるパケットの大きさはすべて等しい為，通信量はパケット数によって決定される．攻撃者の種類によって通信量に影響を与える為，攻撃者の種類によってそれぞれ実験結果を求めた．

5.3 攻撃者の想定

攻撃者は非連結通信路を構築しているノードのいずれかに潜んでおり，経路を通る暗号文に対して改ざん，または盗聴を行うものとする．

5.3.1 通信アルゴリズム

通信のフローチャートを図 5，6，7 に示す．グラフの番号の各動作について以下に説明する．

(1) 送信者と受信者間でできるだけ多くの独立した非連結経路を確保する．ここで構築できた経路数を n' とする．
(2) 受信者は確保できた経路の本数で対応できる最大限の

攻撃者の数 t を想定し，t の攻撃者に対して最低限の経路数 n を求める．よって以下の式が成り立つ．
$n' \geq n = 2t + 1$
このとき，n と t を用いて (n, b, t)-verifiers set system を構築する．

(3) 受信者は各ブロックごとにランダムな値 (0-9) を送信者に送る．このときパケットが経路上で失われる．
(4) 攻撃者が存在する．
(5) 攻撃者がパケットを改ざんする．
(6) 送信者はパケット ID を調べた結果，パケットロスが発生している．
(7) 受信者への再送要求のパケットが経路上で失われる．
(8) パケットの値が改ざんされていないかをブロックごとに比較した結果，改ざんされている．
(9) ブロックをブラックリストへ登録する．
(10)パケットがすべて受信者へ届いている．
(11)ブロックの値から r を生成し，r と送りたい暗号文 Ms を組み合わせた暗号文 V を作成し，ブラックリスト B' をまとめる．
(12)ブラックリストと暗号文 V を受信者へブロードキャストした結果，過半数以上のパケットが経路上で失われる．
(13)受信者へ届いたパケットのうち，t 個以上のパケットが同じ値である．
(14)ブロック B からブラックリストに登録されたブロック B' を除いたブロック B" から，r の値と推定する．送信者より受け取った値 V と r を用いて Ms を得る．

5.4 実験結果

HPSMT を用いた，パケットロスを考慮した無線マルチホップネットワーク上における通信のシミュレーション結果について述べる．
実験結果に用いられる記号については以下の様になっている．
D:パケットドロップ率（%）を表す．
times：計測回数（回目）を表す．
実験結果の表は通信成功までに必要となった通信量を表しており，単位はバイトである．

5.4.1 実験１：盗聴を行う攻撃者を想定した通信

攻撃者が盗聴のみを行う場合の実験結果を図 1 に示す．パケットドロップ率が 40 %以上になると、通信が成功するまでに必要となる通信量が非常に増えている事がわかる．

5.4.2 実験２：改ざんを行う攻撃者を想定した通信

攻撃者が潜んでいる経路を通るパケットに対して常に改ざんを行う場合の通信量は図 2 の様になっている．実験 1 と比較すると，パケットドロップ率 50 %の場合を除き、通信量が増加している事がわかる．

表 1 盗聴を行う攻撃者を想定した通信量

D \ times	1	2	3	4	5	平均
5	9000	9000	12000	9000	9000	9600
10	12000	13000	12000	9000	9000	11000
20	19000	13000	12000	12000	16000	14400
30	26000	13000	25000	13000	26000	20600
40	45000	13000	65000	13000	25000	32200
50	66000	68000	52000	47000	53000	57200

表 2 改ざんを行う攻撃者を想定した通信量

D \ times	1	2	3	4	5	平均
5	11000	9000	9000	9000	15000	10600
10	11000	9000	9000	9000	19000	11400
20	25000	25000	9000	12000	32000	20600
30	53000	26000	16000	12000	27000	26800
40	54000	34000	49000	22000	45000	40800
50	50000	36000	58000	39000	65000	49600

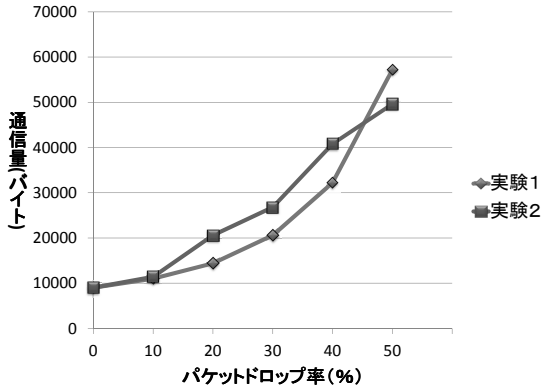

図 8 攻撃者の種類とパケットロスによる通信量の変化

5.5 考察

上記二つの実験によって明らかとなった，通信が成功するまでに必要となった通信量の平均の結果を図 8 に示す．複数の非連結経路と秘密分散を用いずに 1 つのパケットを送る通常の通信と比較した場合，パケットロスの割合と攻撃者の種類に依存して通信量は約 10 倍から 60 倍に増加する事が明らかとなった．

実験 1 と実験 2 の結果を比較すると，改ざんを行う攻撃者と盗聴を行う攻撃者の違いによって通信量が異なることが明らかとなり，一部の例外を除き，盗聴を行う攻撃者の場合は通信量が少なくなった．パケットドロップ率が 50 %のとき，盗聴を行う攻撃者の場合の通信量は改ざんの攻撃者を仮定した場合よりも大きくなっている．これは攻撃者の影響よりも，パケットロスの確率の影響の方が大きい為だと考えられる．よって，さらに実験回数を増やすことで，盗聴を想定した通信量の平均値は改ざんの場合よりも

少なくなると考えられる．また，本実験においてはパケットロスが起きた後に到達するパケットはバッファに一時保存せず破棄し，パケットロスにより失われたパケットから再送を行った．パケットロスが発生した場合でも，その後届いたパケットに対してバッファに一時保存をする事で，通信量をより少なくする事が可能である．さらに，本実験において，2-round 目にブロードキャストする際，攻撃者が潜んでいると思われる経路の特定を行わず，すべての経路に再送を行った為，通信が失敗する確率が大きくなり，余計な通信量が増えている．経路が増えた場合でも攻撃者の特定が可能ならば，さらに通信量は少なくする事が可能となる．

また，本実験では，(n,b,t)-verifiers set system を使用したが，(n,b,t',t)-verifiers set system を利用する事によって，パケットロス耐性をつける事が可能となる．具体的には，攻撃者の数を t と仮定したとき，ブロックを構成する経路群の数 b に依存して，ある程度のパケットロスが発生した場合も通信が可能となる．しかしながら，ブロックを構成する経路群を増やすためには，通信に用いる経路の総本数を増やす必要があり，通信量が増加してしまう．よって，想定する攻撃者の数，パケットロス耐性，パケットドロップ率の 3 つを考慮した最適値を見つけだす事ができれば，改ざんを行う攻撃者の存在を想定した，パケットロスが起こりうるネットワーク上の通信に対して，通信量をさらに減らせる可能性がある．パケットロス耐性をつける場合とそうでない場合について，どちらが通信量をより少なくする事ができるかについては今後検討を行う必要がある．

6. おわりに

6.1 結論

今回の結果は，HPSMT の攻撃者の数と経路の数が最少の結果であるので，経路の数を増やすことで、攻撃者の種類とパケットドロップ率の差による通信量の違いはより明確になると思われる．しかしながら，想定する攻撃者の数が 1 人だと十分に安全であるとは言えないため，経路を増やす必要がある．想定する攻撃者の数が 2，3，4，5 と増えるにつれて必要となる最低限の通信量は,35 倍，147 倍，639 倍と著しく増加する事となる．よって，使用用途に関しては限られるが，送る情報が小さく，通信量のコストがある程度大きくなっても問題がないならば，十分に有用だと言える．

6.2 今後の課題

今後の課題として，以下の５つが挙げられる．

(1) 一時的なデータの保存する記憶領域をとりいれることによって，通信量の削減を行う．
(2) 攻撃者が改ざん攻撃を行う場合，攻撃者の潜む経路を特定する事で 2-round 目のブロードキャストの改良を行い，通信量の削減を行う．
(3) 経路を増やした場合のシミュレーションを行い，通信量の比較を行う．
(4) 経路構築についてのシミュレーションを行い，必要となる通信量を明らかにする．
(5) パケットロス耐性をつける場合とつけない場合に関する通信量の比較を行う．

謝辞 本研究の一部は（財）電気通信普及財団の研究助成，および，JSPS 科研費 24500084 の助成を受けたものである

参考文献

[1] Dolev, D., Dwork, C., Waarts, O., Yung, M.: Perfectly Secure Message Transmission. Journal of the ACM 40(1), pp.17-47,1993
[2] Shannon.C. E, Communication Theory of Secrecy Systems *Bell Systems Technical Journal, Vol. 28* pp. 656-715,1948
[3] Erotokritou,S and Desmedt,Y:Human Perfectly Secure Message Transmission Protocols and Their Applications Visconti and R. De Prisco (Eds.): SCN 2012, LNCS 7485, Springer-Verlag Berlin Heidelberg, pp. 540-558,2012
[4] Desmedt,Y.,Kurosawa,K.: How to Break a Practical MIX and Design a New One. In: Preneel,B. (ed.) EUROCRYPT 2000. LNCS,vol. 1807,pp. 277-287. Springer, Heidelberg, 2000
[5] Kurosawa,K.,Suzuki,K.: Truly Efficient 2-Round Perfectly Secure Message Transmission Scheme. In: Smart,N. (ed.) EUROCRYPT 2008. LNCS,vol. 4965, pp. 324-340. Springer,Heidelberg, 2008
[6] Yang,Q.,Desmedt,Y.: General Perfectly Secure Message Transmission Using Linear Codes. In: Abe,M. (ed.) ASIACRYPT 2010. LNCS,vol. 6477,pp. 448-465. Springer,Heidelberg, 2010
[7] Desmedt,Y.,Erotokritou,S.,Safavi-Naini,R.: Simple and Communication Complexity Efficient Almost Secure and Perfectly Secure Message Transmission Schemes. In: Bernstein,D.J.,Lange,T. (eds.) AFRICACRYPT 2010. LNCS, vol. 6055,pp. 166-183. Springer,Heidelberg, 2010
[8] Rees, R., Stinson, D.R., Wei, R., Rees, G.H.J.V.: An Application of Covering Designs: Determining the Maximum Consistent Set of Shares in a Threshold Scheme. Ars Comb. 53, pp.225-237,1999
[9] Stavrou Eliana, Andreas Pitsillides: A survey on secure multipath routing protocols in WSNs *University of Cyprus, Computer Networks,54(13),pp2215-2238,2010*
[10] Lou.W, W. Liu, and Fang.Y. :SPREAD : Enhancing data condentiality in mobile ad hoc networks, *Proc. IEEE INFOCOM, Hong Kong, China, Mar. 2004* pp. 2404-2413
[11] Marti.S,.Giuli.T,Lai.K and .Baker.M, “Mitigating routing misbehavior in mobile ad hoc networks,” MobiCom’00,Boston,MA, USA,August,2000
[12] Zhang.Y,Lee.W and Huang.Y, “Intrusion detection techniques for mobile wireless networks,” ACM Wireless Networks Journal,Vol. 9, No. 5,Sep,2003
[13] 銭飛 著:NS2 によるネットワークシミュレーション 発行 森北出版株式会社
[14] http://seculab.cis.ibaraki.ac.jp/ kurosawa/class/ CANS(kaoru).pdf