様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 ２９ 日現在

機関番号：１７２０１
研究種目：基盤研究(C)（一般）
研究期間：2012～2014
課題番号：２４５００８４

研究課題名（和文）複数の安全性レベルを提供する通信のための複数経路統合

研究課題名（英文）Multipath integration for providing secure communication with multi-level

研究代表者
堀　良彰（Hori, Yoshiaki）

佐賀大学・全学教育機構・教授

研究者番号：９０２６４１２６

交付決定額（研究期間全体）：（直接経費）　　4,100,000円

研究成果の概要（和文）：Perfect Secure Message Transmission (PSMT) の一種であるHuman PSMT を例に、無線通信路によって構成された複数経路を用いた情報伝達方式の設計を行った。無線通信路における特性パラメタである廃棄率を変化させた場合に必要となる通信量について計算機シミュレーションを実施して評価を行った。攻撃者モデルとして能動的攻撃者および受動的攻撃者を仮定して、安全性を確保するために必要なトラヒック量について明らかにした。PSMT をSoftware Defined Network (SDN) 上に適用するための検討を行った。

研究成果の概要（英文）：We design a secure communication system with two or more paths between a sender and a receiver by using Human PSMT, which is one kind of Perfect Secure Message Transmission (PSMT) protocols, on a multi-hop wireless network. We evaluate relationship between an amount of traffic and packet loss by using computer simulations. We also discuss to design PSMT scheme on Software Defined Network (SDN).

研究分野：情報工学

キーワード：セキュア・ネットワーク　高信頼性ネットワーク　暗号・認証等　情報通信工学

１．研究開始当初の背景
送信者から受信者へのメッセージ転送において事前に鍵共有を前提としない無条件の安全性を提供する手段として，1990 年代初めより，Perfectly Secure Message Transmission (PSMT) の理論的研究が行われている．Dolev らの先駆的研究は，複数経路を利用し，共有秘密鍵を用いずに，秘密分散法による耐盗聴性と耐改ざん性を完全に保証するメッセージ伝送手法を提案している．さらに，実用面への要求から，耐盗聴性を損なわず対改竄性を譲る代わりに PSMT より少ない通信資源実現する Almost Secure Message Transmission (ASMT)が研究されている．通信路を仮想化した上で確率的に安全性を保証するプロトコルの理論的研究がなされている．また，性能面に重きをおいたセキュアな転送手法の研究がすすめられている．これら理論的な研究は進められているにもかかわらず，これらを現実的な手法で実ネットワークに適用した研究は見当たらない．一方，単一ネットワークにおいて複数の経路を構築し，機密性を有する転送方式の実現はアドホックネットワークにおける非連結マルチパス転送に秘密分散を適用した研究は 2000 年代中ごろから開始されているが，前述の PSMT のような理論的に強固な安全性の裏付けは不十分である．

２．研究の目的
本研究では，安全性レベル可変な通信を実現する複数ネットワーク経路の統合による通信方式を実現するため次の点を明らかにする．
（１）提供する安全性のレベルと必要な通信資源との関係について整理する．完全秘匿性ならびに信頼性（耐改竄性）を実現する PSMT およびそれらの派生方式と通信パラメタと，それらの安全性および必要な通信資源を評価する．
（２）複数レベルの安全性を実現するために必要な時間・空間を共有しない複数経路の構築手法について検討する．

３．研究の方法
安全性レベル可変な通信を実現する複数ネットワーク経路の時間・空間統合を実現するための通信方式を設計するため，複数レベルの安全性提供時に必要となる通信資源の評価，時間・空間を共有しない複数経路の構築について研究する．

４．研究成果
[1]複数レベルの安全性提供時に必要となる通信資源の評価
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し，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．
[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．本研究では 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 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．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した．

[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 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 ≧ 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評価した．

[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．

[通信アルゴリズム]

通信のフローチャートを図 1, 2, 3 に示す．

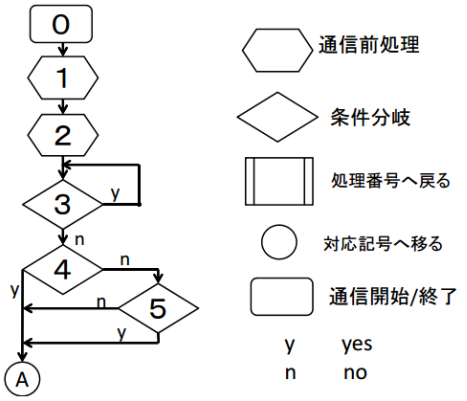

図 1 フローチャート 1

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．よって次の式が成り立つ

n′ ≧ 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．

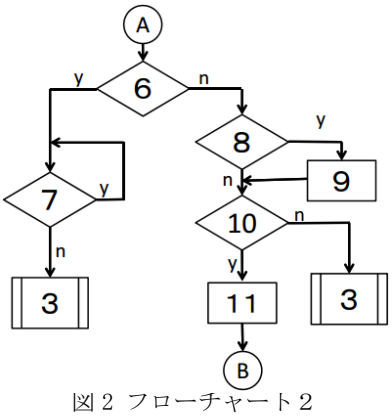

図 2 フローチャート 2

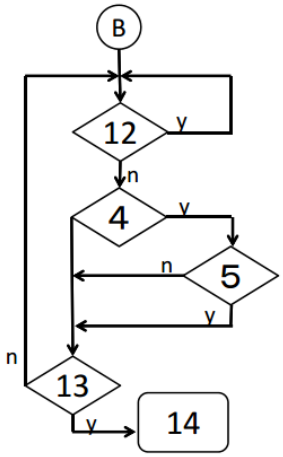

図 3 フローチャート 3

[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次の様になっている．

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．

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表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．

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表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

[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４に示す．

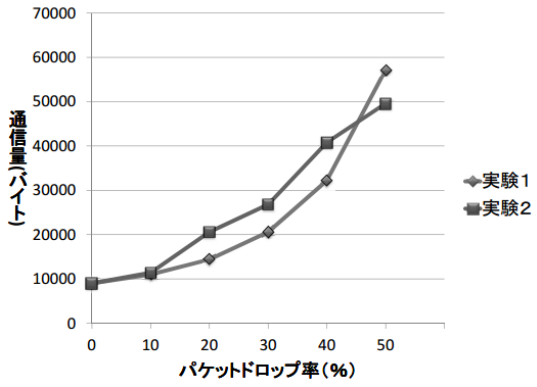

図４ 攻撃者の種類とパケットロスによる通信量の変化

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．

[2]複数パスの構築手法について

本手法では，複数パスの構築が必要であるが，次世代ネットワーク基盤として有望とされている Software Defined Network では OpenFlow や NETCONF プロトコルを用いてスイッチ上に仮想パスを構築することができることに着目し，複数パス構築の手法について

検討を行った.

５．主な発表論文等
（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　１件）
① Wataru Tsuda, Yoshiaki Hori, Kouichi Sakurai, Performance Evaluation of Information Theoretic Secure Multi-channel Transmission on Multihop Wirelss Network, Proc. of the 2013 8th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA 2013), Vol.1, pp. 570- 574, DOI:10.1109/BWCCA.2013.99 (2013)

〔学会発表〕（計　２件）
① 津田航，堀良彰，櫻井幸一，″情報理論的安全性に基づく通信方式の設計と評価″，火の国情報シンポジウム 2013，2013 年 3 月 14 日～2013 年 3 月 15 日，熊本市

② 堀良彰，松本晋一，山内一将，梶原直也，川本淳平，櫻井幸一，″SDN セキュリティ研究動向 －現状と課題－″，2015 年暗号と情報セキュリティシンポジウム（SCIS 2015），2015 年 1 月 20 日～2015 年 1 月 23 日，北九州市

６．研究組織
(1)研究代表者
堀　良彰（HORI YOSHIAKI）
佐賀大学・全学教育機構・教授
　研究者番号：90264126

(2)研究分担者
櫻井　幸一（SAKURAI KOUICHI）
九州大学・大学院システム情報科学研究院・教授
　研究者番号：60264066

西出　隆志（NISHIDE TAKASHI）
筑波大学・システム情報工学研究系・准教授
　研究者番号：70570985