2007－CSEC－39（12）
2007／12／14

インターネットのエッジノードにおける受信トラフィックを媒体とするステガノグラフィの可能性

†塩田明弘 †遠山 毅 ‡井上大介 ‡吉岡克成 ‡衛藤将史 ‡中尾康二 †松本 勉

† 横浜国立大学大学院環境情報研究院
〒240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7
‡ 独立行政法人 情報通信研究機構 情報通信セキュリティ研究センター
〒184-8795 東京都小金井市貫井北町 4-2-1
†Email: {shiota, toyama}@mlab.jks.ynu.ac.jp, tsutomu@ynu.ac.jp
‡{dai, katsunari_yoshioka, eto, ko-nakao}@nict.go.jp

あらまし インターネットのトラフィックを媒体とする既存のステガノグラフィは，送・受信者間の1対1通信を前提としていたが，これを多対多の通信に拡張した新たなステガノグラフィの可能性を検討する．その一実現手法として，ネットワーク観測システムのセンサ（エッジノード）に定常的に届くマルウェアの不正なトラフィックをカバーデータとしたステゴシステムを提案し，実装および評価を行った．

Considerations on Steganography Using Traffic Received at Edge Nodes in the Internet

†Akihiro Shiota †Tsuyoshi Toyama ‡Daisuke Inoue ‡Katsunari Yoshioka ‡Masashi Eto
‡Koji Nakao †Tsutomu Matsumoto

†Graduate School of Environment and Information Sciences, Yokohama National University
79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan
‡National Institute of Information and Communications Technology
4-2-1 Nukui-kitamachi, Koganei, Tokyo, 184-8795, Japan
†Email: {shiota, toyama}@mlab.jks.ynu.ac.jp, tsutomu@ynu.ac.jp
‡{dai, katsunari_yoshioka, eto, ko-nakao}@nict.go.jp

Abstract We address a new scenario of steganography using Internet traffic in which multiple senders and receivers are considered unlike the previous studies with a single sender and a receiver. In this report, we propose, implement, and evaluate a new steganographic system using malware's malicious traffic (e.g. scans) which is constantly observed by sensors of network monitoring system.

1. はじめに

ステガノグラフィは真に伝えたい情報を別の媒体に埋込んで伝送し，通信当事者以外に対し通信の存在そのものを秘匿する技術である．情報を埋込む媒体（カバーメディア）には，静止画像，動画像，音声，テキストをはじめとして様々なメディアが利用される．ステガノグラフィの手法には，通信プロトコルをカバーメディアとするものもあり，その多くはインターネットを流れるパケットが内包する冗長性を利用して情報を埋込んでいる[1][2][3]．これら既存の手法は，送信者と受信者が1対1（互いに1つのIPアドレス）で通信することを前提に設計されている．本稿では，ステガノグラフィを行う送信者と受信者の双方が，複数の制御可能なIPアドレスを保有しているという新たな設定を導入し，多対多（多数のIPアドレス同士）の通信を前提としたステガノグラフィの可能性を検討する．

単一のエンティティが，複数のIPアドレスを保有することは，インターネットのセキュリティインシデント

対策を行うネットワーク観測システム[4][5][6]においては自然な設定である．一般にネットワーク観測システムは，インターネットの終端にセンサ（エッジノード）を分散配置し，各センサで複数のIPアドレスを観測する．センサはマルウェアに感染した多数のホストが送出する不正なトラフィックや，送信元IPアドレスが詐称されたDoS攻撃への返信であるBackscatter等を定常的に受信することとなる．

ここで，マルウェアによる不正なトラフィックとは，脆弱なホストを探査するためのスキャンパケットや，ホストの脆弱性をつくエクスプロイトコードを含むパケット，コネクションの確立なしにマルウェア本体を送りつけるパケット，マルウェアによるDoS攻撃やDDoS攻撃のパケットと定義する．

本稿では，多対多の通信が可能な環境下でのステガノグラフィの一手法として，送信者がマルウェアの不正なトラフィックをカバーメディアとして情報を埋込み，受信者が複数のIPアドレスを観測するエッジノードとして動作して，受信トラフィックから情報を抽出するステゴシステムを提案し，実装および評価を行う．

本稿の構成は次のとおりである．2節ではエッジノードにおける受信トラフィックへの埋込手法を提案し，これを用いたステゴシステムを3節において提案して4節で評価する．5節では今後の課題を述べ6節でまとめを行う．

2. エッジノードにおける受信トラフィックを利用した埋込手法の提案

本節では，エッジノードにおける受信トラフィックを利用した埋込手法を提案する．2.1節で提案手法の概要を述べ，2.2節でStego keyについて述べる．2.3節で1パケットあたりの埋込可能情報量について述べる．

2.1 提案手法の概要

エッジノードにおける受信トラフィックを利用した埋込手法を提案する．提案手法では，複数のIPアドレスのエッジノードで観測された受信トラフィック中の埋込可能なパケットヘッダ内の送信元IPアドレスフィールドと宛先IPアドレスフィールドの値を，あらかじめ送受信者間で共有しておいたStego keyを参照し，埋込情報に対応する値に書換える事で埋込む．この時，埋込まないパケットはトラフィック中から削除し，埋込を行ったパケットのトラフィック中の時系列は保持したまま送信する．Stego keyは，送受信者が使用できるIPアドレスの対とビット列を対応させたものである．

既存の手法で想定する送受信者は，1対1で通信することを前提に設計されているため，送信元IPアドレスフィールドと宛先IPアドレスフィールドには埋込めない．一方，提案手法では，埋込媒体として利用するエッジノードにおける受信トラフィックは複数のIPアドレスから複数のIPアドレスへの通信を記録したものである．そのため，トラフィックの送信元IPアドレスフィールドと宛先IPアドレスフィールドを変更しても通信が成り立つことから，送受信者が複数のIPアドレスを持つ環境下でのカバーメディアとして利用できる．

2.2 Stego key

提案手法では，埋込情報の埋込と抽出において，送受信者で事前に共有しておいたStego keyを使用する．送信者がm個の，受信者がn個のIPアドレスを使用できるとすると，IPアドレスの対の数はt=m･n通り存在する．これらに$\lfloor \log_2 m \cdot n \rfloor$[bit]のビット列をそれぞれ1個または2個割当てる方法のそれぞれをStegokeyの中でもEmbedding keyとする．表1に，m=3，n=4としたときのEmbedding keyの一例を示す．

表1 m=3，n=4のEmbedding keyの例

	n_1	n_2	n_3	n_4
m_1	000	001	010	011
m_2	100	101	110	111
m_3	000	001	010	011

提案手法におけるEmbedding keyの総数を見積もる．t（=s+2u）個のものがあり，これらは第1の種類のもの1個，…，第sの種類のもの1個，第s+1の種類のもの2個，…，第s+uの種類のもの2個からなるとするとき，これらの重複順列の総数は，

$$\frac{t!}{(1!)^s (2!)^u} = \frac{t!}{2^u}$$

である．記号p(t)で$\lfloor \log_2 t \rfloor$[bit]のビット列の総数，すなわちt以下の最大の2のベキ乗$p(t) = 2^{\lfloor \log_2 t \rfloor}$を表すことにすると，Embedding keyの場合，p(t)と上記のsとuとは

$$p(t) = s + u, \quad u = t - p(t)$$

という関係にある．すなわち，p(t)個のビット列のうちのどのu個を2個ずつ割当てるかは，

$$\binom{p(t)}{t-p(t)}$$

通りだけある．このようにして，t 個のアドレス対に $\lfloor \log_2 t \rfloor$[bit]からなるビット列をそれぞれ 1 個または 2 個割当てる方法（Embedding key）の総数が

$$q(t)=\binom{p(t)}{t-p(t)}\frac{t!}{2^{t-p(t)}}$$

であることが判る．なおtが2のベキ乗の場合はt=p(t)であることからq(t)=t!である．

したがって，送信者，受信者が利用できるIPアドレスの個数がそれぞれm，nであるとき，Embedding keyの個数はq(m･n)であるといえる．特にmもnも2のベキ乗の場合，Embedding keyの個数は(m･n)!である．

2.3 1パケットあたりの埋込可能情報量

提案手法では，送信者がm個のIPアドレス，受信者がn個のIPアドレスを使用できる場合，1パケットあたり$\lfloor \log_2 m \cdot n \rfloor$[bit]の情報を埋込める．例えば，m=256，n=256の時は1パケットあたり2[byte]埋込める．また，提案手法はIPv4を前提として検討しているが，IPv6ではIPアドレスの総数が大幅に増加する．そのため1パケットあたりの埋込可能情報量が送受信者のIPアドレスの対の数に比例する提案手法では，より多くの埋込可能情報量が確保できると同時に，個人で提案手法を利用することも現実的なシナリオとなることが予想される．

3. 提案手法を用いたステゴシステム

本節では，3節で提案した埋込手法を用いたステゴシステムを検討する．3.1節で通信モデルを述べ，3.2節で想定する攻撃者について述べる．最後に3.3節で想定する攻撃への対策を述べる．

3.1 提案するステゴシステムの通信モデル

提案手法を用いたステゴシステムについて検討する．本システムにおいて，送信者と受信者は複数のIPアドレスを持ち，それぞれを複数のノードに割当てる．送信者は自身の持つノードから自由にパケットを送信でき，受信者は自身の持つノードに届く全パケットを観測できる．

本システムは情報の埋込（embedding），伝送（transmitting），抽出（extracting）の3つのプロセスからなる．通信モデルを図1に示す．

図1でCはカバートラフィック（Cover Traffic），Eは埋込情報（Embedded Data），Sはステゴトラフィック（Stego Traffic），Nはノイズトラフィック（Noise Traffic）である．カバートラフィックはエッジノードで観測されたトラフィックであり，ステゴトラフィックは送信者から送信される，埋込情報が埋込まれたトラフィックである．また，ノイズトラフィックは，第三者から受信者に届くトラフィックである．Stego keyは2.2節で説明した埋込情報を指定するためのEmbedding keyに加え，情報の埋込まれたパケットと埋込まれていないパケットを判別するためにMACを計算するための鍵Detecting keyを合わせたものである．この時，MACはパケットヘッダの特定のフィールドの値を利用して計算する．

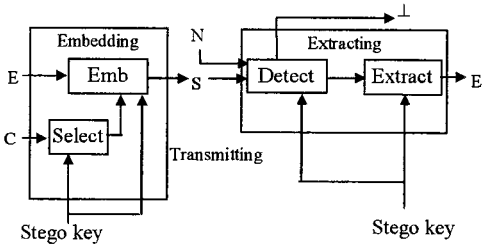

図1 提案するステゴシステムの通信モデル

送信者は，Embeddingで，カバートラフィックから埋込可能なパケットを選び出す（Select）．その後，それらのパケットの送信元IPアドレスと宛先IPアドレスのフィールドの値を，Embedding keyを用い，埋込情報のビット列に対応したIPアドレスの対に書換える．さらに，埋込情報が埋込まれたパケットと埋込まれていないパケットを判別するための情報をDetecting keyを用いて生成し，既存のパケットを用いるステガノグラフィ手法で提案されてきたフィールドにその値を埋込み，ステゴトラフィックを生成する（Emb）．最後に，ステゴトラフィックを受信者に対し送信する．

受信者は，Extractingで，Detecting keyを用い，受信したトラフィックの中から，ステゴトラフィックとノイズトラフィックを判別し，ノイズトラフィックを破棄する（Detect）．その後，Embedding keyを用い，ステゴトラフィックから埋込情報を抽出する（Extract）．

3.2 想定する攻撃者

提案システムでは，以下のような攻撃を想定する．攻撃者の目標は，観測しているトラフィックを解析することで，情報が埋込まれているステゴトラフィックと，埋込まれていないノンステゴトラフィックを正しく判別することである．攻撃者は，受信者に届く全てのトラフィックを観測し，3.1 節で述べた，ネットワーク観測システムに届くことが多いとされるトラフィックの知識を元に，ステゴトラフィックの特定を行う．具体的な攻撃として以下の Attack1 から Attack4 を想定する．

Attack1 攻撃者は，通常観測できないトラフィックをステゴトラフィックと判断する．

Attack2 攻撃者は，観測したトラフィックの送信元アドレスに接続し，接続先が，観測されたトラフィックを発生させるホストかそうでないかを観察する．本稿では特に，Backscatter（SYN/ACK）のパケットの送信元がサービスを行うホストでない場合，ステゴトラフィックと判断する．

Attack3 攻撃者は，パケットのヘッダの値や送信のタイミング等を観察する．この時，ある特定のパケットと比べて，送信元 IP アドレスと宛先 IP アドレスが異なるが，タイムアウトによる再送パケットの特徴を持つパケットが観測できたとき，ステゴトラフィックと判断する．

Attack4 攻撃者は，ある単位時間の間に観測したトラフィック中のパケットにおけるヘッダの値を観察する．この時，異なるホストからのパケット間の関連性から，それらのパケットが元々一つのホストから送られたパケットの系列であると判断できれば，ステゴトラフィックと判断する．

3.3 想定する攻撃への対策

3.2 節で挙げた攻撃 Attack1 から Attack4 に耐性を持たせる手法を提案する．具体的には，カバートラフィックから，攻撃者の解析する手がかりを与えないトラフィックにのみ埋込むことで，攻撃に耐性を持たせる．Attack1 から Attack4 に耐性を持たせるための条件をそれぞれ Pattern 1 から Pattern4 とし，以下にまとめる．

Pattern1 観測されたトラフィックのパケットを埋込可能とする．

Pattern2 Pattern1 で埋込可能としたトラフィックの中で，SYN/ACK パケットを埋込不可能とする．

Pattern3 Pattern2 で埋込可能としたトラフィックの中で，タイムアウトによる再送パケットを埋込不可能とする．

Pattern4 Pattern3 で埋込可能としたパケットの中で，ある時間内で，観測システムに複数回パケットを送ったホストからのパケットを埋込不可能とする．

4. 実験による性能評価と考察

本節では，提案システムについて，実際にネットワーク観測システムで観測されたトラフィックをカバーデータとして用いて計測した結果を示す．4.1 節で実験環境について述べ，4.2 節で埋込可能情報量について計測した結果を示す．4.3 節で送信者からのパケットの割合について示し，最後に 4.4 節で考察を行う．

4.1 実験環境

本稿では，送信者と受信者が，ともに/24 のアドレスブロックを利用可能な環境を想定し，実験を行った．このとき，3.3 節の式より，1 パケットあたりの埋込可能情報量は $\lfloor \log_2 256 \cdot 256 \rfloor = 16[\text{bit}] = 2[\text{byte}]$ である．

カバートラフィックとして，24 時間の間に/24 のアドレスブロックを持つネットワーク観測システムで観測されたトラフィックを用いた．埋込情報は一度 AES 暗号の OFB モードで暗号化した．これは埋込情報の bit の偏りを無くすためである．

Detecting key を 128bit 長の鍵とし，HMAC-SHA1 を用い，計算した値の上位 32bit をシーケンス番号フィールドに埋込んだ．ハッシュ関数に入力する情報は，IP ヘッダの識別子，送信元 IP アドレス，宛先 IP アドレス，TCP ヘッダの送信元ポート番号，宛先ポート番号の各フィールドの値と，受信者への命令を表す値を 1byte の配列に入力して用いた．受信者への命令には，通信開始，通信継続，通信終了の 3 種類があり，それぞれ，1，0，2 の 3 つの値で表される．

4.2 埋込可能情報量

24 時間のトラフィックを 1 時間毎に分割し，3.3 節の Pattern1 から Pattern4 を適用した場合の 1 時間あたりの埋込可能情報量を計測した．この結果を図 2 に示す．各時間帯での埋込可能情報量は，1 時間あたりの埋込可能なパケット数に，4.1 で求めた 1 パケットあたりの埋込可能情報量をかけて算出した．

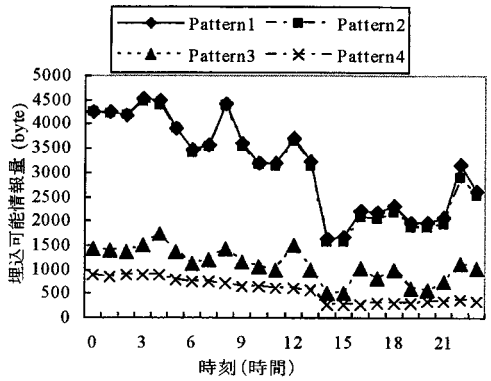

図2　1時間当たりの埋込可能情報量

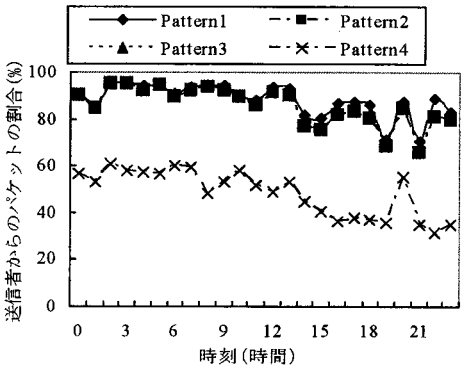

図3　1時間当たりのパケット総数に対する送信パケットの割合

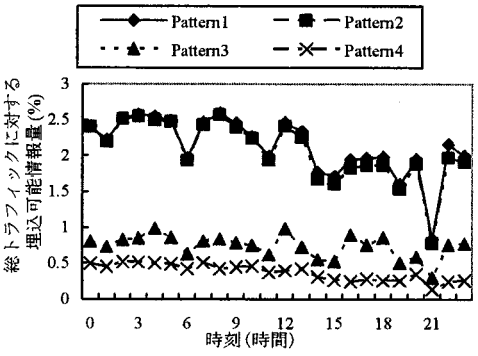

図4　1時間当たりの総トラフィックサイズに対する埋込可能情報量の割合

4.3　送信者からのパケットの割合

提案するステゴシステムを用いて通信を行う時,受信者にはステゴトラフィック以外にもノイズトラフィックが届いている.この受信者が受け取るトラフィック中の送信者のパケットの割合を調べた.本稿では,ノイズトラフィックはネットワーク観測システムで通常観測できるようなトラフィックであると考え,ノイズトラフィックの代わりにカバートラフィックを用いた.カバートラフィック中の埋込可能なパケットの割合を,3.3節のPattern1~4をそれぞれ適用した場合において計測した.トラフィック中の送信者からのパケットの割合 T_P は,以下の式で求めた.結果を図3に示す.

$$T_P = \frac{\text{送信したパケット数} \times 100}{\text{カバートラフィックの 総パケット数}} [\%]$$

また,総トラフィックサイズに対する埋込可能情報量の割合 T_S 以下の式で求めた.結果を図4に示す.

$$T_S = \frac{\text{埋込可能情報量} \times 100}{\text{総トラフィックサイズ}} [\%]$$

4.4　考察

図2から,Patternを適用して埋込不可能なパケットの条件を増やすことで,埋込可能情報量が減少することがわかった.特に,Pattern3を適用した場合,Pattern2を適用した場合と比較して,埋込可能情報量が約1/3になっている.これは,Windowsでの接続要求の際のタイムアウト再送の回数が規定値で2に設定されていることと関係があると考えられる.図3から,Pattern3を適用した場合,Pattern1やPattern2の場合と同じ程度のパケットを送っていることがわかるが,図4から,Pattern3を適用した場合の埋込可能情報量は,Pattern1やPattern2と比較し,大きく減少していることがわかる.これは,Pattern3を適用することで,Pattern2まで埋込めていた再送パケットに埋込めなくなるが,再送パケットを再現することから,送信するパケットの数が変わらないためである.これにより,あるパケットの系列の一部のパケットにしか情報を埋込まない場合も,パケットの系列を模擬する必要があるために埋込んでないパケットを送ることから,通信の効率が落ちることがわかる.

5. 今後の課題

本節では今後の課題について検討する．5.1 節では埋込可能情報量，5.2 節では安全性について検討する．5.3 節ではその他のカバーメディアの可能性を検討する．

5.1 埋込可能情報量

本稿で送信者は自身の保有する IP アドレスを用いて埋込みを行うが，送信元 IP アドレスをスプーフすれば，より多くの情報が埋込める．ただし，スプーフしたアドレスがパケットを送信しないようなホストである場合，ステゴトラフィックと判断される可能性も考えられる．提案手法にパケットの冗長性を利用した既存の埋込手法を併用すれば，1 パケットあたりの埋込可能情報量は増加する．その場合の安全性も今後の検討課題といえる．

さらに，提案手法で埋込を検討した TCP パケット以外の，UDP パケットや ICMP パケットへの埋込を検討することで，カバートラフィック中の埋込可能なパケット数は増加する．特に UDP パケットに関しては，SQLSlammer のように UDP パケットを頻繁に送信するマルウェアがあり，埋込可能なパケットの大幅な増加が見込める．ただし，これらの異なるプロトコルを利用する際には，受信者が正しく抽出できるようにするための判別情報を埋込むフィールドを検討する必要がある．また，書換えるフィールドを見直す事によって，埋込可能となるパケットについても検討する必要がある．

5.2 安全性

本稿で検討したステゴシステムにおいては，一般的なネットワーク観測システムで観測できるトラフィックに関する知識を持つ攻撃者を想定し，安全性を検討した．しかし，特定のネットワーク観測システムに届くトラフィック関してさらに詳しい知識を持つ攻撃者には埋込が検出される可能性がある．例えば，特定のマルウェアやアプリケーションに関する知識を持つ攻撃者の場合，埋込により生じた不自然なトラフィックを検出できる可能性がある．また，ネットワーク観測システムの持つアドレスによって観測できるトラフィックの局所性や，時刻による周期性の違いが解析の手がかりとなりうる．さらには，受信者に届くトラフィックに，送信者によるステゴトラフィックが加わることで，トラフィック中の送信元アドレスに偏りが生じたり，流量が増加したりする．以上のような強い攻撃者に対して耐性を持つシステムの検討が，安全性に関する今後の課題である．

5.3 その他のカバーメディアの可能性について

提案システムでは実際にネットワーク観測システムで観測されたトラフィックをカバーメディアとして用いているが，ネットワーク観測システムに届くトラフィックに含まれるパケットを送信者自身が作成し，カバーメディアとして用いる手法が考えられる．一例として，送信者がマルウェアのプログラムを用い，マルウェアが出力するトラフィックをカバーメディアとして用いる方法が考えられる．ただし，そのマルウェアによるトラフィックが受信者側で多く観測されるようなものである必要があり，安全性についても検討する必要がある．

6. まとめ

エッジノードにおける受信トラフィックを利用した埋込手法を提案し，提案する埋込手法を用いたステゴシステムについても提案を行った．また，提案するステゴシステムの性能評価として，実際にネットワーク観測システムで観測されたトラフィックをカバーデータとして用いて埋込可能情報量を計測した．さらに，埋込可能情報量を増やす手法，安全性，カバーメディアの可能性について検討した．

参考文献

[1] K. Ahsan, D. Kundur, “Practical Data Hiding in TCP/IP,” ACM Workshop on Multimedia Security, 2002.

[2] S. J. Murdoch, S. Lewis, “Embedding Covert Channels into TCP/IP,” 7th Information Hiding Workshop, 2005.

[3] 松本勉，井上大介，鈴木雅貴，“通信におけるインフォメーションハイディング，” IPSJ Magazine, Vol.44, No.3, pp 254 - 259, 2003.

[4] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, D. Watson, “The Internet Motion Sensor: A Distributed Blackhole Monitoring System,” The 12th Annual Network and Distributed System Security Symposium, 2005.

[5] D. Moore, “Network Telescopes: Tracking Denial-of-Service Attacks and Internet Worms around the Globe,” 17th Large Installation Systems Administration Conference, USENIX, 2003.

[6] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, K. Rikitake, “nicter: An Incident Analysis System using Correlation between Network Monitoring and Malware Analysis,” The 1st Joint Workshop on Information Security, pp.363-377, 2006.