様式 C-19

科学研究費補助金研究成果報告書

平成２３年　６月　１５日現在

機関番号：25403
研究種目：基盤研究（C）
研究期間：2008～2010
課題番号：20500075
研究課題名（和文）　効率的なサービス不能攻撃対策の研究

研究課題名（英文）　Efficient Countermeasures against DoS Attacks

研究代表者
双紙　正和　　（SOSHI　MASAKAZU）
広島市立大学・情報科学研究科・准教授
研究者番号：00293142

研究成果の概要（和文）：インターネットにおいては，DoS 攻撃がセキュリティにおける大きな脅威となっている．この攻撃においては，攻撃者が発信アドレスを偽装するため，その対処が極めて困難である．そこで本研究課題では，DoS 攻撃対策として，IP トレースバック方式を研究した．具体的には，効率が良い IP トレースバック方式の提案およびトレースバック方式の理論的なモデル化およびそれに基づく評価等の研究を行った．

研究成果の概要（英文）：DoS attacks have been serious threat to the Internet security these years.　Therefore we studied efficient countermeasures against such DoS attacks, especially focused on IP traceback schemes.　In this study we proposed efficient IP traceback schemes and conducted theoretical analysis of them.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,000,000	300,000	1,300,000
２００９年度	1,300,000	390,000	1,690,000
２０１０年度	1,100,000	330,000	1,430,000
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：基盤研究
科研費の分科・細目：C
キーワード：セキュリティ，サービス不能攻撃，トレースバック，モデル，理論的解析，実装，ネットワーク，シミュレーション

１．研究開始当初の背景

近年，インターネットにおいては，サービス不能（Denial of Service, DoS）攻撃がセキュリティにおける大きな脅威となっている．DoS 攻撃とは，悪意を持った攻撃者が，攻撃対象のサイトに向けて大量のパケットやメールを一斉に送信するなどして，そのサイトを使用不能に陥れる攻撃である．このような DoS 攻撃の対策としては，攻撃パケットの発信源を求めることが有効に思える．しかしながら，通常 DoS 攻撃では発信アドレスが偽造されるため，その発信源を特定することは極めて困難である．そこで，近年 IP トレースバックと呼ばれる技術が盛んに研究されるようになってきた．IP トレースバックとは，攻撃対象ノードあるいはネットワーク上のルータが，攻撃者の位置またはそれまでの経路を特定するための技術である．残念ながら，従来の IP トレースバック方式には課題が多く，未だに決定的な方法は存在しない．さらに，多くの方式は実装を主眼とするもので，理論的な観点からは未だ十分な解析・評価はなされていない．

そこで，本研究課題では，IP トレースバッ

ク方式，中でも特に，カウンタを用いた IP トレースバック方式，改良 FIT トレースバック方式，およびキャッシュに基づく DoS 攻撃対策を中心に研究開発を行っていく．

２．研究の目的

IP トレースバック方式は，(a) 確率的マーキング方式，(b) ダイジェスト方式に大きく分類できる．(a) の確率的マーキング方式とは，攻撃者の位置を特定するために，そのパケットに確率的に何らかの情報を埋め込む方式である．この方式は，マーキングによる性能低下，トレースバックの際の非効率性等，様々な問題点を抱えている．

一方で，上記(b)のダイジェスト方式とは，パケットのダイジェストデータを，通過ルータなどが記録しておき，そのデータを各ルータが照らし合わせて発信源を特定する方式である．ダイジェスト方式は，ルータに極めて大きな負荷がかかる．

そこで近年，双方の利点を同時に生かせるような，ハイブリッド方式と呼ばれる IP トレースバック方式が研究されるようになってきた．本研究で研究開発を行う方式は，基本的にこのハイブリッド方式に属する．そして，本研究課題では，効率の良い IP トレースバック方式を提案するとともに，今までの研究では不十分であった理論的解析を詳細に行うことを目的とする．

３．研究の方法

効率の良いトレースバック方式の確立のため，さまざまな効率のよい認証方式について研究する．さらに，トレースバック時のスペース効率を改善するため，既存の space-time encoding 方式を改良する．これは，もともと，確率的パケットマーキング方式を対象として，Muthuprasanna らによって提案された方式である．このアルゴリズムを改良し，また，もとの研究ではなされていなかった，理論的な性能解析を行う．

さらに，カウンタを用いた IP トレースバック方式の研究開発を行う．この方式は，それぞれのパケットにサンプリングカウンタを用意し，攻撃経路全体でサンプリング相関を高めるというものである．さらに，改良 FIT トレースバック方式およびキャッシュに基づく DoS 攻撃対策の研究開発を行う．より具体的には，履歴ベースの DoS 攻撃対策方式である．今まで受信したパケットの履歴に基づき，フィルタリング等適切な対策を行う．

４．研究成果

まず，カウンタに基づく IP トレースバックを提案した．この方式では，DoS 攻撃が起きた際，各ルータがある確率 p に従い，Bloom filter （ある要素がある集合に属しているかどうかを効率よく判定するための確率的データ構造）を利用して，中継パケットのダイジェスト情報を自らに保存する．その後，これらのダイジェスト情報を利用して攻撃者までの経路を特定する．この際，攻撃経路における（攻撃対象から見て）上流のルータを効率よく特定できなければならない．このための基本的なアイディアは下記のとおりである．まず，各パケットのある領域（Identification field 等）を，カウンタとして用いる．そして，各ルータが確率 p によりダイジェストを取る毎に，そのパケットのカウンタを 1 増やしていく．したがって，パケットにおけるカウンタの値は，経路上のルータによってそのパケットのダイジェストが記録された回数を意味する．すなわち，カウンタの値が大きいパケットほど，経路上に情報を残していることになり，トレースバックの際に重要となるパケットとなることを意味している．そこで，確率 p を，カウンタの値が大きいほど高い値とし，カウンタ値が小さいほど低い確率となるように，可変のものとして確率的サンプリングを行えばよい．この提案方式の理論的・実験的な解析評価を行い，いずれにおいても，従来研究よりも良い性能であることを確認した．

さらに本研究課題では，FIT 法の改良を行った．FIT (Fast Internet Traceback) は，Yaar らによって提案されたトレースバック手法である．既存の Savage らによるトレースバック手法の問題点であった，パケットに書き込む情報の容量が大きいという問題と，アルゴリズムを実装していないルータ(レガシールータ)を無視しているという問題を解消するなど，優れた特徴を持つ．その一方で，(i) TTL (Time To Live) フィールドを上書きすることによって，比較的長時間 TTL が 0 にならなくなり，TTL のセマンティクスが損なわれる，(ii) マーキングしたルータ間の距離の計算の効率が悪い，(iii) TTL の値の更新ついての理論的解析がなされていない，といった欠点を持つ．これらの問題を解決するために，以下のような改良を行った．具体的には，TTL のリセット値を 2 通り行えるようにし，適切な初期化を行えるようにした．さらにその結果として，TTL の適切なセマンティクスを保持できるようにした．この結果，FIT 法よりも効率の良いトレースバックを実現できた．

最後に，履歴に基づく DoS 攻撃対策として，フィルタリング手法の研究開発を行った．より具体的には以下のとおりである．フィルタリング方式として有名なものに Pi 方式があるが，Pi 方式は，TTL の偽造やマーキング値偽造に対してアドホックな対策しかしていない．そこで我々は，シンプルで効率がよく，

かつ，上記の偽造に対してより耐性を持つ方式を提案し，さらに，より長い経路を経由する DDoS 攻撃にも対応できるよう，ルータのメモリを用いる方式を提案した．また，提案方式のマーキング特性に対する理論的な解析を行い，さらに，実験的な評価も行った．以上の結果より，ここでの二つの提案フィルタリング方式いずれも Pi 方式よりも偽造に耐性を持つ方式であることを示した．

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 6 件）

1. A. Miyaji and K. Mizosoe, “Revisited (Hyper)-Elliptic Curve Scalar Multiplication with a Fixed Point”, IPSJ Journal, 査読有, 49, 9, 2008, 2975-2988
2. A. Miyaji, “Generalized Scalar Multiplication Secure against SPA, DPA, and RPA”, IEICE Trans., Fundamentals, 査読有, E91-A, 10, 2008, 2833-2842
3. K. Emura, A. Miyaji and K. Omote, “A Dynamic Attribute-Based Group Signature Scheme and its Application in an Anonymous Survey for the Collection of Attribute Statistics”, IPSJ Journal, 査読有, 50, 2009, 1968-1983
4. K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length”, IJACT, 査読有, 2, 2010, 46-59
5. A. Miyaji and M. Sukegawa, “New Analysis Based on Correlations of RC4 PRGA with Nonzero-Bit Differences”, IEICE Trans., Fundamentals.,査読有, E93-A, 2010, 1066-1077
6. G. Hanaoka, S. Hirose, A. Miyaji, K. Miyazaki, B. Santoso, and P. Yang, “Sequential Bitwise Sanitizable Signature Schemes”, IEICE Trans., Fundamentals, 査読有, E94-A, 2011, 392-404

〔学会発表〕（計 33 件）

1. A. Miyaji, K. Emura, A. Nomura, K. Omote, and M. Soshi, “A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length”, ISPEC 2009, LNCS, 査読有, 5451, Springer-Verlag, 2009, 13-23
2. K. Emura, A. Miyaji and K. Omote, “A Dynamic Attribute-Based Group Signature Scheme and its Application in an Anonymous Survey for the Collection of Attribute Statistics”, 査読有, AReS, 2009, 487-492
3. K. Emura, A. Miyaji and K. Omote, “A Certificate Revocable Anonymous Authentication Scheme with Designated Verifier”, 査読有, RIBC 2009, 769-773
4. A. Miyaji, S. Zrelli, Y. Shinoda, and T. Ernst, “Security and Access Control for Vehicular Communications Networking and Communications”, 査読有, WIMOB ’08, 2008, 561-566
5. A. Miyaji, K. Omote and K. Kato, “Simple Certificateless Signature with Smart Cards”, 査読有, SECUBIQ’08, 2008
6. A. Miyaji, A. Waseda, T. Takagi, and M. Soshi, “Quantum Secret Sharing between Multiparty and Multiparty against the Attack with Single Photons or EPR-pair”, 査読有, Proceedings of ISITA 2008
7. 高原加誉子，双紙正和，効率の良い space-time encoding を利用した IP トレースバックの検討，Computer Security Symposium 2008 (CSS 2008)，査読無
8. K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, “A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length”, 査読有, ISPEC 2009, LNCS, Springer-Verlag, 5451, 2009, 13-23
9. S. Hirasawa and A. Miyaji, “Elliptic curves with a pre-determined embedding degree”, ISIT 2009, 査読有, 2009, 2391-2395
10. A. Miyaji and M. Sukegawa, “New Correlations of RC4 PRGA Using Nonzero-Bit Differences”, ACISP 2009, LNCS, Springer-Verlag, 査読有, 5594, 2009, 134-152
11. K. Emura, A. Miyaji and K. Omote, “A Ciphertext-Policy Attribute-Based Encryption Scheme with Strong Recipient Anonymity”, IWSEC 2009, 査読有, 2009, 49-63
12. K. Emura, A. Miyaji and K. Omote, “A Selectable k-Times Relaxed Anonymous Authentication Scheme”, WISA 2009, LNCS, Springer-Verlag, 査読有, 5932, 2009, 281-295
13. 双紙正和，ワイヤレスセンサネットワークにおけるグループ鍵分配プロトコルの考察，CSEC-48，査読無，2010

14. 村上大樹，双紙正和，ワイヤレスセンサネットワークのためのグループ鍵分配プロトコルの提案，暗号と情報セキュリティシンポジウム，査読無，SCIS2010，3C3-3，2010
15. 村上大樹，双紙正和，ワイヤレスセンサネットワークにおける柔軟な鍵共有プロトコルの検討，電気・情報関連学会中国支部第 60 回連合大会，査読無，2009，367-368
16. J. Chen and A. Miyaji，“A New Class of RC4 Colliding Key Pairs With Greater Hamming Distance”，ISPEC 2010，LNCS，Springer-Verlag，査読有，6047，2010，30-44
17. J. Chen and A. Miyaji，“Generalized RC4 Key Collisions and Hash Collisions”，SCN 2010，LNCS，Springer-Verlag，査読有，6280，2010，73-87
18. R. Goundar，M. Joye，and A. Miyaji，“Co-Z Addition Formulae and Binary Ladders on Elliptic Curves”，CHES 2010，LNCS，Springer-Verlag，査読有，6225，2010，65-79
19. K. Emura，A. Miyaji，and K. Omote，“An Anonymous Designated Verifier Signature Scheme with Revocation: How to Protect a Company's Reputation”，ProvSec 2010，LNCS，Springer-Verlag，査読有，6402，2010，184-198
20. K. Emura，A. Miyaji，and K. Omote，“A Timed-Release Proxy Re-Encryption Scheme and its Application to Fairly-Opened Multicast Communication”，ProvSec 2010，LNCS，Springer-Verlag，査読有，6402，2010，200-213
21. H. Ito，A. Miyaji，and K. Omote，“RPoK: A Strongly Resilient Polynomial-based Random Key Pre-distribution Scheme for Multi-phase Wireless Sensor Networks”，IEEE GLOBECOM 2010，査読有，2010，1-5
22. K. Emura，A. Miyaji，and K. Omote，“An Identity-based Proxy Re-Encryption Scheme with Source Hiding Property，and its Application to a Mailing-list System”，EuroPKI 2010，LNCS，査読有，2010
23. A. Miyaji，M. Shahriar Rahman，and M. Soshi，“Hidden Credential Retrieval Without Random Oracles”，WISA 2010，LNCS，Springer-Verlag，査読有，6513，2010，160-174
24. A. Miyaji and K. Omote，“Efficient and Optimally Secure In-Network Aggregation in Wireless Sensor Networks”，WISA 2010，LNCS，Springer-Verlag，査読有，6513，2010，135-149
25. K. Emura，A. Miyaji，and M. Shahriar Rahman，“Efficient Privacy-Preserving Data Mining in Malicious Model，ADMA 2010，LNCS，Springer-Verlag，査読有，6440，2010，429-440
26. A. Miyaji and M. Shahriar Rahman，“Privacy-Preserving Data Mining in Presence of Covert Adversaries”，ADMA 2010，LNCS，Springer-Verlag，査読有，6440，2010，370-382
27. J. Chen and A. Miyaji，“A New Practical Key Recovery Attack on the Stream Cipher RC4 under Related-Key Model，Inscrypt 2010，LNCS，査読有，2010
28. Y. Desmedt and A. Miyaji，“Redesigning Group Key Exchange Protocol based on Bilinear Pairing Suitable for Various Environments”，Inscrypt 2010，LNCS，査読有，6584，2011，236-254
29. 唐沢智之，双紙正和，宮地充子，カウンタを用いた IP トレースバック方式の評価，IPSJ SIG Tech. Rep.，査読無，2011-CSEC
30. 双紙正和，ハッシュ連鎖による単純な認証法とセンサーネットワークへの応用，CSS 2010，査読無，CSS2010-ID1-3，2010，85-90
31. 三吉雄大，双紙正和，ワイヤレスセンサネットワークにおけるグループ鍵配送プロトコルの検討，CSS 2010，査読無，CSS2010-ID1-2，2010，79-84
32. 双紙正和，新しいハッシュ連鎖の構成による単純な認証方式とその応用，信学技報，査読無，ICSS2010-44，2010，1-5
33. 三吉雄大，双紙正和，ワイヤレスセンサネットワークにおける効率的なグループ鍵配送プロトコル，信学技報，査読無，ICSS2010-44，2010，7-10

〔図書〕（計　件）
〔産業財産権〕
○出願状況（計　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計◇件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
双紙正和　　(SOSHI MASAKAZU)
広島市立大学・情報科学研究科・准教授
研究者番号：00293142

(2)研究分担者
宮地充子　　(MIYAJI ATSUKO)
北陸先端科学技術大学院大学・
情報科学研究科・教授
研究者番号：10313701

(3)連携研究者
(　　)

研究者番号：