2007－CSEC－39 (3)
2007／12／14

不正アクセス防御システムのハードウエア実装

菊池 一平*, 佐藤 友暁**, 深瀬 政秋*
*弘前大学大学院理工学研究科
**弘前大学総合情報処理センター

あらまし 不正アクセスやコンピュータウイルスへの対策として IDS(Intrusion Detection System)や IPS (Intrusion Prevention System)の導入による監視や防御を行っている。IDS と IPS は NIDS (Network-based IDS) / NIPS (Network-based IPS) と HIDS (Host-based IDS) / HIPS (Host-based IPS)に分類され、それぞれに問題を有する。本論文では、従来の IDS と IPS の問題点を解消することを目的として開発を行っている H-HIPS(Hardware-based HIPS)のネットワークへ接続するために必要な機能の開発と H-HIPS において不可欠な DoS (Denial of Service)攻撃防御機能の実装について述べる。

Hardware Implementation of Intrusion Prevention System

Kazuhira Kikuchi*, Tomoaki Sato**, and Masa-aki Fukase*
* Graduate School of Science and Technology, Hirosaki University
** Computer and Network Systems Center, Hirosaki University

Abstract As solution against unauthorized computer access and computer virus, IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) are used and execute those monitor and defense. They are classified into NIDS (Network-based IDS) / NIPS (Network-based IPS) and HIDS (Host-based IDS) / HIPS (Host-based IPS) and have problems, respectively. To solve these problems, we have developed H-HIPS (Hardware-based HIPS). In this paper, we describe development of function to connect H-HIPS with network and hardware implementation of DoS (Denial of Service) attack detecting function is essential for H-HIPS.

1 はじめに

コンピュータネットワークを安全・安心に使う上では、IDS (Intrusion Detection System)や IPS (Intrusion Prevention System)による不正アクセスやコンピュータウイルスの監視や防御が不可欠である。IDS と IPS の実態はソフトウエアで、ネットワークベース IDS (Network-based IDS : NIDS)および IPS (Network-based IPS : NIPS)、ホストベース IDS (Host-based IDS : HIDS)および IPS (Host-based IPS : HIPS)に分類される[1]。

NIDS は専用の高性能コンピュータを用いてネットワーク上を流れるパケットを詳細に解析し、不正アクセスをリアルタイムで監視する。NIDS の稼動には高価な高性能計算機を必要とする。しかし、ネットワークを流れるパケット量が多い場合、現在の計算機の処理能力上、すべてのパケットを解析することは不可能である。さらに１台の NIDS では監視対象に限界があるため，複数台の設置が不可欠である。完全に監視するにはすべてのネットワークノードへNIDSを設置する必要がある。

HIDS はファイル改ざんの有無、設定情報、プロセスの状態を監視する。HIDS はホストに HIDS ソフトウエアをインストールして使用するため、NIDS よりも設置が容易である。しかし、リアルタイムに不正アクセスを検知することはできない。パケットの監視機能を搭載した HIDS も一部にあるが、CPU パワーをなるべく消費させないことが不可欠である。このため HIDS は NIDS のように詳細なパケットレベルで解析できない。HIPS においても HIDS と同じ問題を有する。

IDS が攻撃や不正アクセスを検出するだけなのに対し、IPS はこれらをリアルタイムに検出し、パケットを遮断することで防御する。特に NIPS においては正常なパケットを遮断する事を防ぐために，IDS 以上にパケットの詳細な解析と厳密な設定が必要である。このため IDS 以上に高性能な計算機を必要とし、また設定が非常に困難である問題がある。

我々は，従来の IDS と IPS の問題点を解消することを目的として、再構成可能なハードウエアである FPGA (Field programmable gate array)を使用して H-HIPS(Hardware-based HIPS)の開発を行ってきた[2]-[5]。レジスタを使用せずにパイプライン処理が可能であるウェーブパイプライン手法[6]を導入することで、高速かつ低消費電力で動作させることが可能である[7]。

公衆無線 LAN や大学内のネットワーク等は不正アクセスやコンピュータウイルスが多発している[8]。このようなネットワーク環境出はバッテリで駆動するノート PC を使用することが多い

ため，低消費電力動作は非常に重要である。現在FPGA を使用した IDS や IPS は，我々以外にも[9]-[12]が進められている。しかしバッテリで駆動するモバイルコンピュータを前提とした低消費電力化については考慮されていない。

本論文では，不正アクセス防御システムのハードウエア実装について述べる。これまで、H-HIPS において実現されていない。実際にネットワークに接続するための機能を実装する。また、不正アクセスを防御する上で不可欠な DoS (Denial of Service)攻撃防御機能の実装と評価について述べる。

2 不正アクセス検知・防御システムの問題点

不正アクセスやコンピュータウイルスの脅威はインターネット側のみならず、イントラネット等の内部ネットワークにおいても発生する。この問題を解決するためには高価である NIDS を複数用意しなくてはならないという問題がある。NIDS の問題点を下記に挙げる。

NIDS の問題点
・検知を対象としたネットワーク以外で発生する不正アクセス検知が不可能
・パケット量が過大である場合取りこぼしがある
・専用高性能計算機が必要であるため、費用の点から複数台の設置が難しい
・検知のみで防御は行わないため、不正アクセスの対応には常に人的リソースを要する

HIDS は守ることが必要なコンピュータへ IDS ソフトウエアをインストールし、スタティックに改ざんされたファイル、設定情報、プロセスを解析することで不正アクセスを監視する。しかし、HIDS は NIDS と同等レベルでリアルタイムにパケットを解析することは不可能であり、現状の HIDS の処理においても少なからず計算機に負荷を与える。また、HIDS はパケットレベルの解析機能の一部は実現されているが、本格的にパケットレベルの解析処理を行うことは計算機の処理能力上不可能である。これら HIDS の問題点を下記に挙げる。

HIDS の問題点
・リアルタイム検知が不可能
・CPU リソースを消費する
・検知のみで防御は行わないため、不正アクセスの対応には常に人的リソースを要する

IDS (Intrusion Detection System)に防御機能を加えられた IPS (Intrusion Protection System)は、IDS に比べると不正アクセスに対して投入する人的リソースが少なく済むため企業も多く取り入れている[13]。一般的に IPS はネットワークベースであり、実際のネットワークのパケットを制御するため攻撃以外の通信に与える影響を無くす必要がある。このため NIDS 以上に高性能なパケット解析エンジンを要する。NIPS の問題点を下記に挙げる。

NIPS の問題点
・検知を対象としたネットワーク以外で発生する不正アクセス検知が不可能
・専用高性能計算機が必要であるため、費用の点から設置台数が限られる
・ネットワーク上のパケットデータを直接操作するためルール設定が非常に難しい

3 提案システム

これらの諸問題を解決する方法として我々は H-HIPS を提案してきた。H-HIPS は従来の HIDS では不可能だった詳細なパケットレベルでの不正アクセス、コンピュータウイルス、ワームを解析、防御をハードウエアによって実現することを目的としている。ハードウエアには書き換えや更新が容易に可能である FPGA を用いる。これによって今後新たな不正アクセスやコンピュータウイルス、ワームが出現したとしても、それらの防御回路を追加することで柔軟に対処できる。またモバイル化に不可欠な低消費電力化に対処するためにウェーブパイプライン手法を導入する[14],[15]。

従来の IDS,IPS との比較を表 1 にまとめる。H-HIPS のハードウエア構成を図 1 に示す。イーサネットや無線 LAN のネットワークカード上に FPGA を搭載する。FPGA にはイーサネットコントローラなど各周辺回路を制御する Nios2 プロセッサとパケット解析、防御を行う IPL (Intrusion Protection Logic)部で構成されている。100 万ゲートクラスの FPGA の価格が 20US $ 程度であるため、従来の NIC と比べて大幅に価格が高くなることは無い。

ハードウエア構成

Altera 社の Nios development Board Cyclone edition を使用する。開発環境を表 2 に示す。Cyclone は、動作速度は他の FPGA より低速であるが、低価格であり低消費電力で動作する。

表 1　IDS,IPS と H-HIPS

Item	Software			Logic
	Host-based IDS	*Network - Based IDS*	*IPS*	*Host-based IPL*
Installation place	Computer on user side	Network node	Network node	Computer on user side
Input data	File and action in computer	Packet in network	Packet in network	Packet which inputs and outputs computer
Costs	Software	Exclusive use and High performance computer, Software	Exclusive use and High performance computer, Software	FPGA Chip Netlist
Detection time	Unreal-time	Real-time	Real-time	Real-time
CPU load on user side	Yes	No	No	No
Processingcapacity	Non-correspondence of high - load processing	Limit by amount of packet	Limit by amount of packet	High ability
Detect of internal attack	Possible	Impossible	Impossible	Possible
Protect	Impossible	Impossible	Possible	Possible

表 2　開発環境

Platform	Microsoft Windows 2000
Microprocessor	Intel Pentium 4 (3GHz)
Main Memory	1 Gbyte
CAD	Altera QuartusII
FPGA	Cyclone EP1C20F400C7
Tool	Nios development board

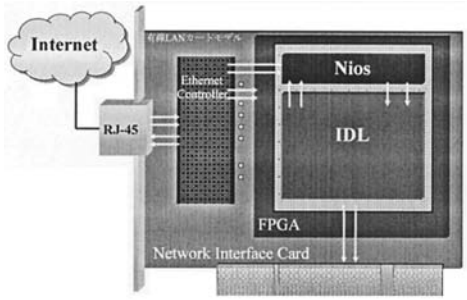


図 1　H-HIPS ハードウエア構成

次に FPGA 上の構成を図 1 で示す。H-HIPS は大きく分けて通信制御部と不正アクセス検出部で構成される。通信制御部にはソフトコアの Nios2 プロセッサが配置され、イーサネットコントローラなどの各ペリフェラルの制御を行う。Nios2プロセッサはALTERA社が提供する柔軟性の高い 32bitRISC ソフトコアプロセッサである。ソフトであるため簡単にコンフィグレーションが可能であり、様々な組み込み開発企業に採用されている。本研究でもこのプロセッサを組み込むことで様々なペリフェラルや自作回路を容易に統合することが可能となっている。

本研究では Nios II にペリフェラルとしてメモリ、イーサネットコントローラ、フラッシュメモリ、そして各不正アクセス検知回路を組み込む。IPL は各不正アクセス検出回路と防御回路を有している。

不正アクセスの大まかな処理の流れを説明する。ネットワークからのパケットデータを Nios II プロセッサによって各不正アクセス検知に必要なデータ部を抽出する。抽出されたチェックデータ部は Fire Wall ユニットを通り各不正アクセス検知ユニットへ送られる。この時 Fire Wall ユニットではパケットフィルタリングが行われ、予め排除リストに登録されている IP アドレスやポート番号のパケットデータは破棄される。Packet Memory には各不正アクセス検知ユニットが検査している間一時的にパケットデータが保管される。各不正アクセス検知ユニットにより正常通信と判定された場合プロテクションユニットは Packet Memory に保管されたパケットデータをホストコンピュータへ送信する。また、不正アクセスが検出された場合は Nios II プロセッサへ検出通知シグナルを送り該当パケットを破棄するこ

とで防御を実現する。これが H-HIPS の不正アクセス防御の大まかな流れである。

FPGA 上はソフトコアの Nios II プロセッサと各不正アクセスの検知、防御機能を備えた IPL で構成される。FPGA 上のブロックを図 2 で示す。

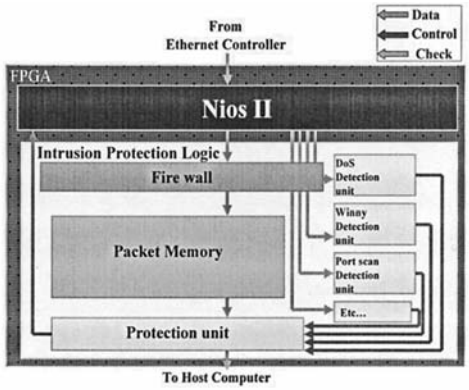


図 2　FPGA 内のブロック構成

ソフトウエア構成

本研究では不正アクセスを防御するにあたってネットワーク上を流れるパケットデータをモニタリングする必要がある。モニタリングのためネットワーク機能を構築した。Nios II にペリフェラルとしてイーサネットコントローラを組み込み、TCP/IP を使用するためプロトコルスタック、OS を実装した。プロトコルスタックにはフリーソフトの Light weight IP、OS には商業アプリケーションとして採用実績がある μC/OS-II を使用した。ネットワークモニタリングに使用するダンププログラムはあらかじめ ALTERA 社が提供するサンプルプログラムを改良し作成した。このダンププログラムによってパケットごとの送信元の IP アドレス、データ長を抽出することが可能となる。

IPL

IPL は通信パケット中で不正アクセスや攻撃の可能性を検査し、それらを検知した場合、防御を実行する。IPL 内には様々な不正アクセス検知や攻撃に個別に検知するユニットによって構成されている。これらの検知ユニットは H-HIPS を実装するコンピュータの用途に合わせて容易にカスタマイズすることが可能である。従来の IPS では基本的に複数台のコンピュータを対象に検知、防御を行うため各コンピュータに基づく多くのルールを適用しなくてはならない。そのためルールが複雑化し検知、防御の誤検知を助長する恐れがある。H-HIPS は個別に実装するため各コンピュータに最適なカスタマイズが可能である。これはルールを単純化し、誤検知を減らすことにつながる。

DoS 攻撃検知ユニット

DoS 攻撃は大量のパケットデータをサーバに送信することでサーバに過剰な負荷を与え、サービス不能状態にする攻撃である。攻撃の方法はコンピュータウイルスによる攻撃や、ボットによる攻撃、DoS ツールによる攻撃など様々なものが挙げられる。いずれかの攻撃手法をとってもサーバへ大きな負荷をかけてサービスの妨害を行う。ウイルス対策ソフトなどを筆頭にソフトウエアによる様々な防御対策が研究されているが、ソフトウエアで防御するということは攻撃パケットデータ自体をコンピュータにロードして検知、防御処理を行うことからリソースの浪費やしまう。ロードしたデータにウイルスなど未知の脅威がある場合感染してしまう恐れがある。H-HIPS ではコンピュータにロードする前に防御を行うため、脅威を未然に回避することができる。

DoS 攻撃検知アルゴリズム

Dos 攻撃検知に当たって送信元 IP アドレスとデータ長(Data Length)の統計を正確に把握する必要があることから DoS 攻撃検知ユニットは IP アドレスとデータ長を検査対象とした。また、DoS 攻撃の特徴として突発的に負荷をかけることから単位時間当たりの受信データ合計から DoS 攻撃を検知する。そのため、DoS 攻撃検知ユニットを配置したネットワークにおける Dos 攻撃を検査する最適な時間の閾値とデータ合計の閾値を設定する必要がある。Dos 攻撃検知フローチャートを図 3 に示す。

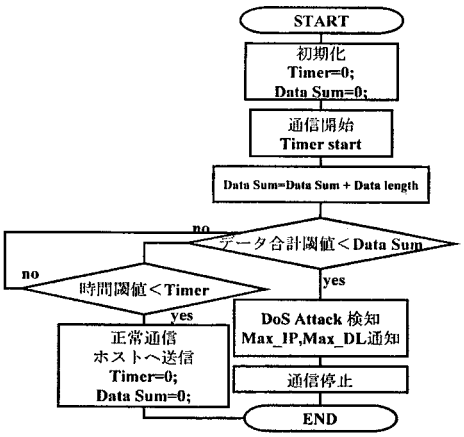


図 3　DoS 攻撃検知フローチャート

DoS 攻撃検知ユニットの設計

DoS 攻撃検知ユニットの内部構成を図 4 に示す。DoS 攻撃検知ユニットは大きく分けてパケットの統計データを計算する Logging unit と攻撃であるかどうかを判断する Detecting unit から構成されている。入力データは CLK,RESET,IP Address, Data Length となっており、IP Address, Data Length は Nios II プロセッサ上で動くダンププログラムによって抽出され Avalon バスを介して入力される。

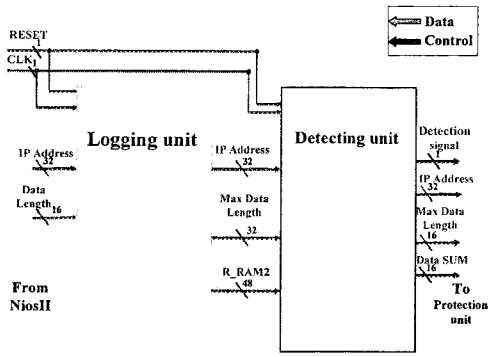


図４　DoS 攻撃検知ユニット構成

Logging unit

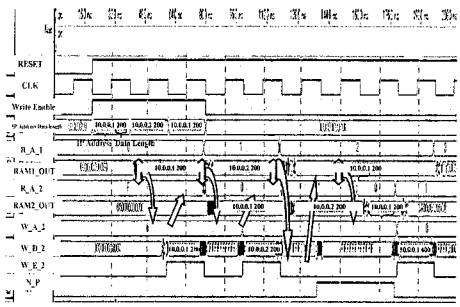
Logging unit は，RAM1，Address Controller(A_C), RAM2 によって構成される。NiosII からの IP アドレス、Data Length は順次 RAM1 に格納される。RAM1 はデータ幅が 6 バイト、16 ワードとなっており各パケットの IP アドレス(4 バイト)とデータ長(2 バイト)で 1 ワードを占める。A_C は RAM1 に格納された IP アドレスと RAM2 内の IP アドレスと比較し、重複が見つからなかった場合はそのまま RAM2 へ格納し、見つかった場合は RAM 2 内で該当する IP アドレスのデータ長どうしを加算する。このように各アドレスからの各データ長合計を示す統計データは RAM2 へ格納されていく。

Detecting unit

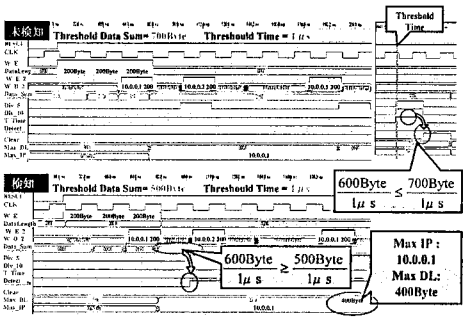
Detecting unit は Threshould_Timer ，Data_SUM, Max_IP_C, Detect から構成され Dos 攻撃と判断する閾値時間、閾値データ合計が設定されている。設定された時間閾値、データ長閾値と Log unit からのパケットデータ統計を比較し DoS 攻撃の判定を行う。判定結果は Protection unit に通達される。

4 DoS 攻撃検知ユニット のシミュレーション

DoS 攻撃検知ユニットは出力データが多いため Logging unit と Detecting unit 別々にシミュレーションを行った。入力データは 3 パケットで、計 600 バイトを入力する。この入力データが Log unit において RAM2 にパケット統計データが正常に格納されることを確認する。Detecting では時間閾値を 1μ秒とし、データ合計閾値を 500 バイトと 700 バイトの二通りに設定し、攻撃検知時と未検知時のシミュレーションを行った。各ユニットの結果を図５に示す。次に実際に FPGA に書き込みロジックアナライザによる検証を行う。ロジックアナライザのプローブ本数に対応させるため、IP アドレスを示す信号は 4bit に省略する。検証結果を図６に示す。シミュレーション結果と同様の結果が正しいことが確認できる。動作周波数は 56.8MH z を確認した。現状では 48bit のワ

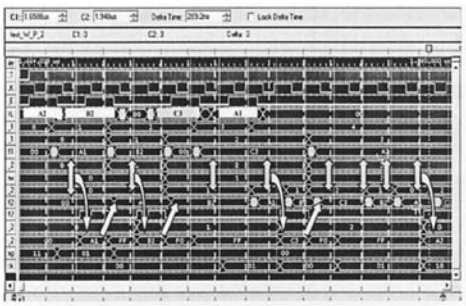


(a) Logging unit

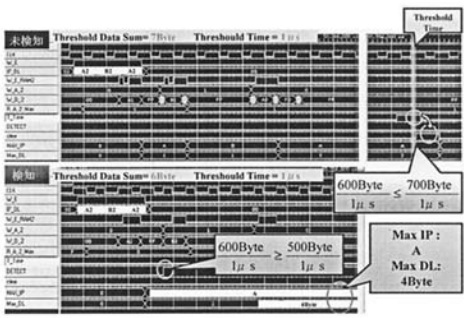


(b) Detecting unit

図５　シミュレーション結果



(a) Logging unit



(b)Detecting unit

図６　実機検証結果

ード幅で設計してあるため、本ユニットは2.6Gbpsに対応できることが示されている。

5 まとめ

本論文ではハードウエアによるパケット解析と防御機能を有するH-HIPSについて述べた。ネットワーク機能を実現するためのハード・ソフトウエア設計、DoS攻撃検知ユニットの設計、機能シミュレーション、実機検証を行った。DoS攻撃検知ユニットはシミュレーション、実機検証結果より正常に動作することを確認した。動作周波数は56.8MHzであるため2.6Gbpsに対応できる。これはクライアントが使用するIPSとしては十分な性能である。今後の課題として実際のネットワーク上での実験、評価、他の不正アクセス検知ユニットの開発と評価が挙げられる。

謝辞

本研究の一部は文部科学省科学研究費補助金（若手研究(B)，19700050）による実施である。

参考文献

[1] Stephen Northcutt and Judy Novak, "Network Intrusion Detection, 2nd Edition," New Riders Publishing, 2001.
[2] Tomoaki Sato and Masa-aki Fukase, "Reconfigurable Hardware Implementation of Host-Based IDS," Proc. of the 9th Asia-Pacific Conference on Communication, Vol. 2, pp. 849-853, 2003.
[3] Tomoaki Sato, Daisuke Miyamori, Rena Sakuma, and Masa-aki Fukase, "Power-Consumption Aware Intrusion Detection Logic for WLAN," SCI2005. Vol. III, pp. 409-414, 2005.
[4] Tomoaki Sato, Rena Sakuma, Daisuke Miyamori, and Masa-aki Fukase, "Hardware Security-Embedded Wireless LAN Processor," Proc. of ECTI-CON 2005, Vol. II, pp. 839-842, Pattaya, Cholburi, THAILAND, May 2005.
[5] Tomoaki Sato, Kazuhira Kikuchi and Masa-aki Fukase, "Port-Scan Detection Unit for H-HIPS," Proc. of CCCT2007, Vol. II, pp. 250-255, 2007.
[6] F. Klass and M. J. Flynn, "COMPARATIVE STUDIES OF PIPELINED CIRCUITS," Stanford University Technical Report, No. CSL-TR-93-579, July 1993.
[7] M. Fukase, T. Sato, R. Egawa, and T. Nakamura, "A Wave-Pipelined Biprocessor Achieving Remarkable Compatibility between Low Power and High Speed," Proc. of 10th NASA Symposium on VLSI Design, pp. 8.3.1-8.3.8, 2002.
[8] 佐藤友暁, 深瀬政秋, "学内無線 LAN における不正アクセス・コンピュータウイルス問題のハード的解決手段の開発," 学術情報処理研究, No. 9, pp. 15-26, 2005.
[9] Gregg Judge, "FPGA Architecture Ups Intrusion Detection Performance," http://www.commsdesign.com/design_corner/showArticle.jhtml?articleID=16502099, Sep., 2003.
[10] Shaomeng Li, Jim Torresen, Oddvar Soraasen, "Exploiting Reconfigurable Hardware for Network Security," Proceedings of the 11th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, pp. 292-293, 2003.
[11] Young H. Cho and William H. Mangione-Smith, "Deep Packet Filter with Dedicated Logic and Read Only Memories," Proc. the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines, "pp. 125-134, 2004.
[12] Jan Korenek and Petr Kobiersky, "Intrusion Detection System Intended for Multigigabit Networks," Proc. of IEEE Design and Diagnostics of Electronic Circuits and Systems, pp. 1-4, 2007.
[13] 小倉秀敏,"IPS(不正侵入防御システム)を知る" http://www.atmarkit.co.jp/fsecurity/special/59ips/ips01.html,March,2005.
[14] Tomoaki Sato, Rena Sakuma, Daisuke Miyamori, and Masa-aki Fukase, "High-Speed and Low-Power LFSR by Wave-Pipelining," Proc. of CCCT, Vol. III, pp. 396-401, 2004.
[15] Tomoaki Sato, Rena Sakuma, Daisuke Miyamori, and Masa-aki Fukase,"Performance Analysis of Wave-Pipelined LFSR," Proc. of IEEE ISCIT 2004, vol. 2, pp. 694 - 699, 2004.