原著論文

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

佐藤　友暁　　深瀬　政秋

弘前大学総合情報処理センター
〒036-8561 弘前市文京町３

Hardware Approach for Unauthorized Computer Access and Computer Virus in Wireless Campus LAN

Tomoaki Sato and Masa-aki Fukase

Computer and Network Systems Center, Hirosaki University
Bunkyo-cho 3, Hirosaki, 036-8561, Japan

概要

学内に設置された無線 LAN のアクセスポイントを通して，学生が所有するノートパソコンを学内 LAN やインターネットに接続する機会が増えてきている。このようなネットワーク環境においては，従来以上に不正アクセス，コンピュータウイルス，ワームの対策を強化することが必要である。しかし，ソフトウェアによる従来の不正アクセス検知システム(Intrusion Detection System :IDS)では，十分な対応が難しい。この問題に対処するため，本論文では従来のソフトウェア IDS と同等な機能を有し低消費電力で動作するハードウェアの開発について述べる。また，学内 LAN への実装を提案する。

Abstract

There are so many opportunities in todays campus life that students connect their laptop computers to campus LAN and Internet via access points. It is really indispensable for such network environment to more strengthen the detection of unauthorized computer access, computer virus, worm etc. However, conventional IDS- (Intrusion Detection System) installed software system does not always cover this affair. In order to solve this issue, we have developed an IDS-implemented hardware that operates with low-power consumption. Its application for wireless campus LAN is also described.

Keywords: 学内 LAN，無線 LAN，低消費電力化，不正アクセス，コンピュータウイルス, IDS

１．　はじめに

コンピュータとネットワークの高性能化，低価格化が進んだ結果，学生は自前のノートパソコンを学内に携帯し，学内ではイーサネットの接続口を継続的に充実してきた。さらに，これまでの有線 LAN を補完すべくアクセスポイントを随所に設置し，学内無線 LAN 環境を整えつつある [1]。このようなネットワーク環境を利用し，学生所有の携帯型ノートパソコンを使用した情報教育が拡がりを見せている[2]。このような教育体制は，学生側と大学側の双方に多くの利点をもたらす反面，ウイルスや不正アクセス等が容易に学内 LAN に持ち込まれるようになり，従来以上の対策が必要となる。

従来の学内有線 LAN に対しては，不正アクセスを検知するために IDS が導入されてきた。IDS の実態はソフトウェアで，ネットワークベース IDS (Network-based IDS :NIDS)とホストベース IDS (Host-based IDS :HIDS)に分類される[3]。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ため，設置には限りがある。しかも，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。更に，監視対象としているネットワーク以外で発生する不正アクセスの検知は不可能である。一方，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 はホストにインストールして使用するため，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ため，ネットワークベース IDS と比べて監視内容は不完全である。一方，ハードウェア的な手段による IDS としては，FPGA (Field programmable gate array)によるギガビットネットワークを対象とした NIDS がある[4]。しかし，消費電力については考慮されていないため，無線 LAN で発生する不正アクセス，コンピュータウイルス，ワーム問題へは対処できていない。

我々は，無線 LAN をより安全かつ安定した運用を可能にすることを目的として，従来の IDS の問題点を解消するハードウェアベースの HIDS である H-HIDS (Hardware-based HIDS)の開発を行ってきた [5]。H-HIDS は再構成可能なハードウェアである FPGA によるロジックベースの IDS である。H-HIDS は，詳細なパケットレベルの解析機能をホストベースかつ低消費電力で実現する。本論文では，H-HIDS の開発，及び H-HIDS を用いて教育用携帯型ノートパソコンを不正アクセス，コンピュータウイルス・ワームから防御する手法について提案する。H-HIDS の特徴である低消費電力動作について示し，H-HIDS を学内 LAN に適用することで従来の問題点を解消可能であることを述べる。

２．　学内 LAN の現状

2.1 IDS の問題点

IDS は不正なアクセスの検知を行うシステムである。HIDS は，守ることが必要なコンピュータへ IDS ソフトウェ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から不可能である。従来の IDS の問題点を整理すると下記の通りである。

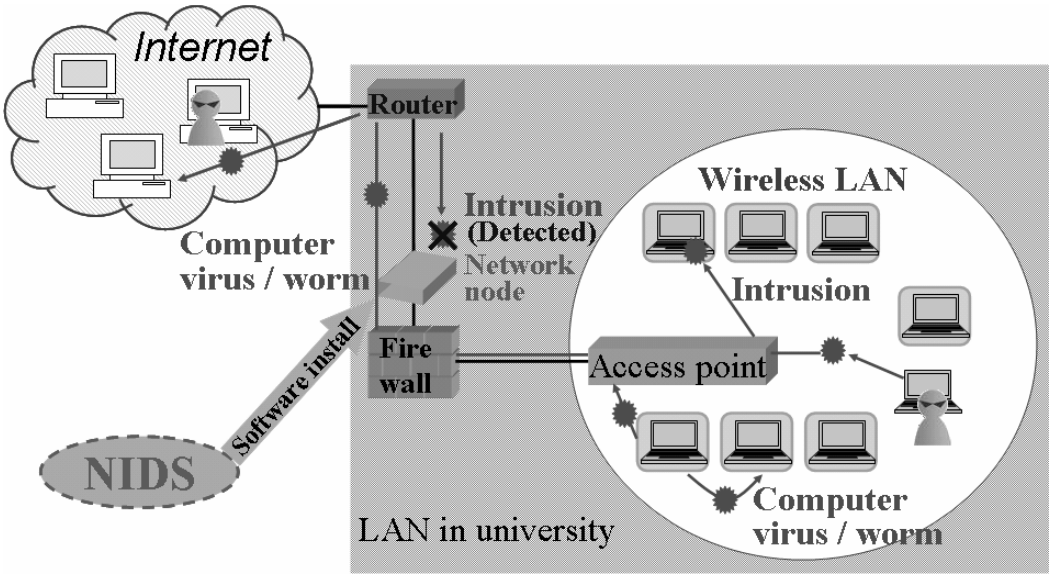


図-１　大学内で発生する不正アクセス，コンピュータウイルス，ワームの侵入経路

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

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，費用の点から設置台数が限られる。

不正アクセスの検出率の向上や，正常なアクセスに対する誤動作を防ぐための効果的な検出方式の開発は，IDS 研究の重要な課題である。ホストベース IDS の例では，[6]のように多変量解析を用いた研究が行われている。効果的な検出手法は，攻撃の検知がより正確になる一方，計算機への負荷が高まることが予想される。また，ネットワーク IDS の例では，大容量ネットワークになるほどパケット量が増大すると，すべてのパケットの処理が IDS の処理能力の限界から不可能である。例えば[7]のように，トラフィックパターンによる検出の研究が行われている。しかし，正確な検出を行うにはすべてのパケットを詳細に解析する必要がある。

２．２　不正アクセス，コンピュータウイルス，ワーム

多くの大学において，無線 LAN のアクセスポイントの設置やイーサネットケーブルの接続口を設置し，学生自身が所有するノートパソコン等をインターネットへ接続できる環境の構築が進められている。さらに学生自身が所有するノートパソコンを用いた講義，実習などもおこなわれている。これらの接続に使用するノートパソコンは，学生自身が管理しているため，パソコンの管理が不完全な状態であることが多い。実際に，２００３年の夏に発生した W32/MSBlaster ワームによって，大学内の LAN が麻痺することが発生している。

図-１に大学内において発生する不正アクセス，コンピュータウイルス，ワームの侵入経路を示す。学生が所有するノートパソコン等は，大学内に設置してある IDS，ファイヤーウォール，メールのフィルタリング等で外部から侵入する不正アクセス，ウイルス，ワームから守られているが，次の理由からこれらが機能しない場合がある。

表-１　ソフトウェア IDS と IDL

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

- 学外でインターネットに接続した際に感染したコンピュータの学内 LAN への接続
- 学外メールサーバを経由したメールの受信
- 不正アクセスを学生自身が実行

コンピュータウイルスやワームは，ウイルス対策ソフトウェアの導入によって感染から守ることが可能であるが，多くの学生がウイルスのパターンファイルの更新を怠っている。このためウイルス対策ソフトウェアが機能しないことが多い。一部のウイルス対策ソフトウェアにおいては，集中してパターンファイルの更新を管理する機能を持つものがあるが，各種 OS や機種の接続が考えられる大学においては，このようなソフトウェアを一律に導入することはできない。

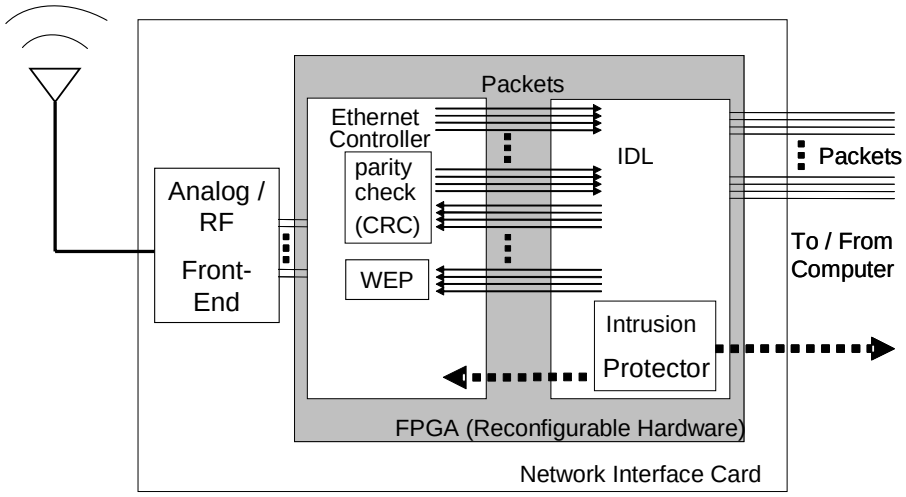
３．　H-HIDS

H-HIDS は，従来のソフトウェアによる HIDS が実現不可能である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，ワームを解析する機能の実現を目的に研究されている[8]。FPGA を使用するため，これから新たに出現する不正アクセス，コンピュータウイルス，ワームへも検知するための回路を追加することで対応が可能である。従来のソフトウェアによる IDS との比較を表-1 にまとめる。

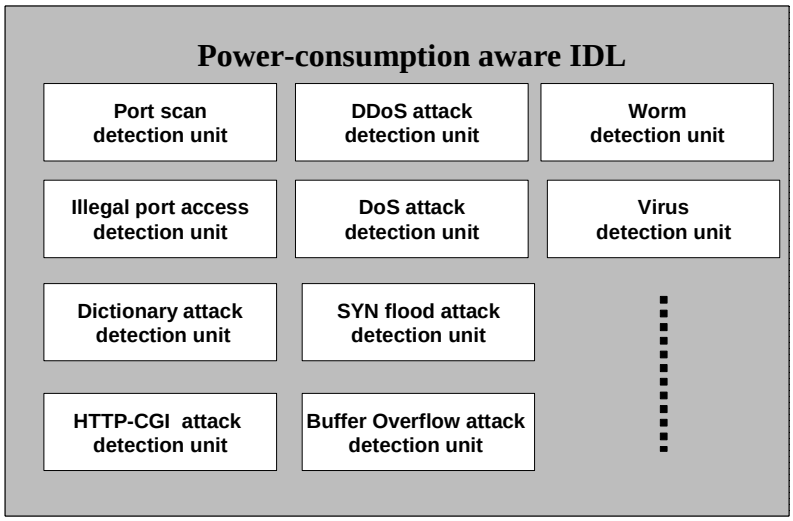
無線 LAN 向けの H-HIDS のハードウェアの構成を図２に示す [9]-[10]。無線 LAN のネットワークカード上に FPGA を搭載している。その FPGA では，従来のイーサネットコントローラ部と実際にパケットの解析をおこなう IDL (Intrusion Detection Logic)部で構成されている。H-HIDS では，３層以上をハードウェアで処理する必要がある。従来ソフトウェアによって処理がおこなわれる CRC (Cyclic Redundancy Check)回路や無線 LAN では，従来の有線 LAN と異なり暗号化が不可欠なため，無線 LAN において標準的な暗号方式である WEP (Wired Equivalent Privacy)が搭載されている。100 万ゲートクラスの FPGA の価格が 20US$程度[11]であるため，従来の無線 LAN の NIC と比べて大幅に価格が高くなることは無い。

H-HIDS によってパケットレベルの詳細な解析が可能になり，次の利点が生まれる。

- LAN 内部で発生する不正アクセス，コンピュータウイルス，ワームをリアルタイムで検知することが可能である。
- NIDS よりも検知を対象とするパケット規模が小さくなることで，パケットの取りこぼしが無くなる。



(a)



(b)

図-2 ハードウェア構造 (a) H-HIDS 全体　(b) IDL の構成

加えて，専用ハードウェアにおいてロジックレベルで直接処理をおこなうため，並列処理やパイプライン処理によって複数の検知機能を同時に高速に処理することが可能である。

３．１　運用

我々は FPGA を用いて H-HIDS の開発をおこなっている。ネットリストが書き込まれた FPGA はカスタム LSI として動作する。ネットリストとは回路素子と結線の情報をテキストデータとして出力されたものである。従って，従来の不正アクセスの検知とパケットの解析アルゴリズムに対応するソフトウェアはネットリストに対応する。検知と解析のアルゴリズムをハードウェア化しそのネットリストを FPGA へ書き込むことで,専用ハードウェアとして直接パケットの解析や不正アクセスの検知が可能になる。図-3 に示すように，ネットリストは，IDS をサービスする会社のサーバに置かれ，IDS ユーザは，インターネットを通じてネットリストをダウンロードする。それを H-HIDS 上の FPGA にダウンロードする。運用手順は従来のウイルス対策ソフトウェアと同じである。

ポートレベルの監視，制御はユーザによって使用するアプリケーションが異なるため，パソコンのユーザ

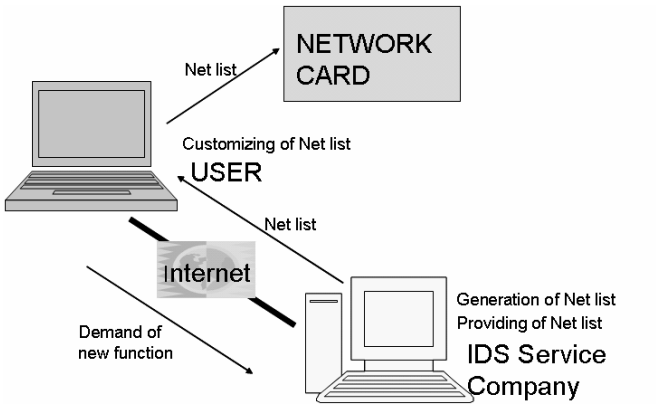


図-3 運用方法

自身が設定することが不可欠である。このような設定情報は，ユーザ数分のネットリストが必要となるため，IDS をサービスする会社のサーバ上で用意することは非現実的である。解決策としてユーザ自身がネットリストをカスタマイズできるツールの開発もおこなう。

３．２　実現した機能

我々がすでに設計した機能は不正なポートへのアクセス検知である。権限のないポートアクセスの制御は，従来のオペレーティングシステムに搭載されている機能であるが，同時に CPU のリソースが消費される。加えて古いオペレーティングシステムには搭載されていないため，使用用途が十分であっても，一世代前のコンピュータは，そのようなオペレーティングシステムの使用は動作が遅く，買い替えが要求される。これらの問題を解決するために，我々は H-HIDS で権限のないポートへのアクセスを検出と防御する機能を実現させている。この機能によって，MS-Blaster の蔓延と LAN 内部のトラフィックの増大を防ぐことが可能である。

図-4 は，WWW (World Wide Web)へのアクセスの例による不正なポートのアクセスの監視部分を示す。また図-5 に TCP/IP プロトコルのパケット形式を示す。WWW へのアクセスは HTTP ポートである 80 番を使用する。WWW サーバへのリクエストパケットは，図-5 の Destination PORT number を監視することで，許可されたものかどうかを判断することができる。逆に WWW サーバから送られる情報は，図-5 の Source PORT

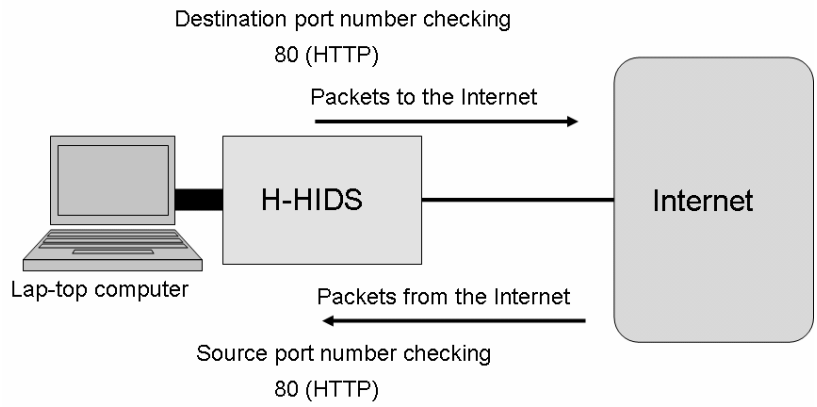


図-4 ノートパソコンにおける不正ポートアクセスの監視部分

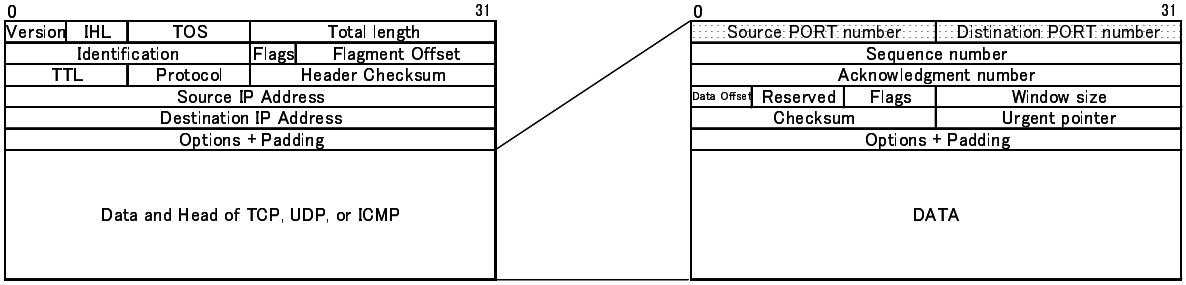


図-5 TCP/IP プロトコルにおけるパケット形式

表-2　ポート番号

Function	Port number
FTP	21
TELNET	23
SMTP	25
DNS	53
HTTP	80
POP	110

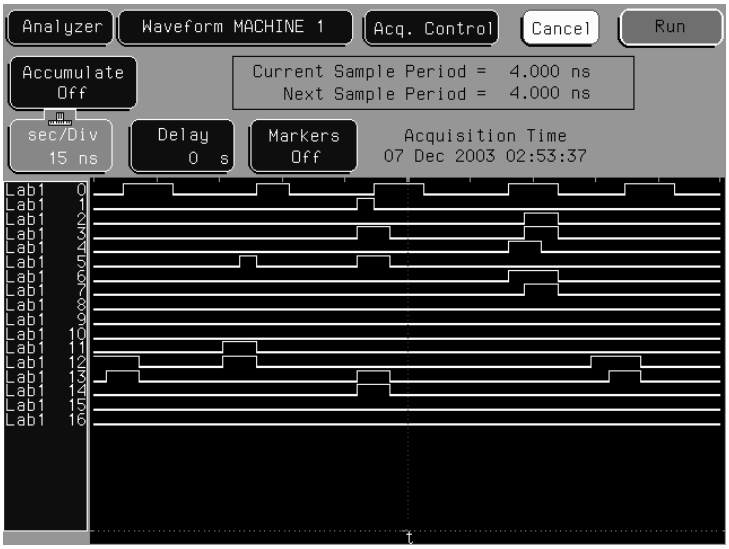


図-6 測定結果(100 MHz 動作)

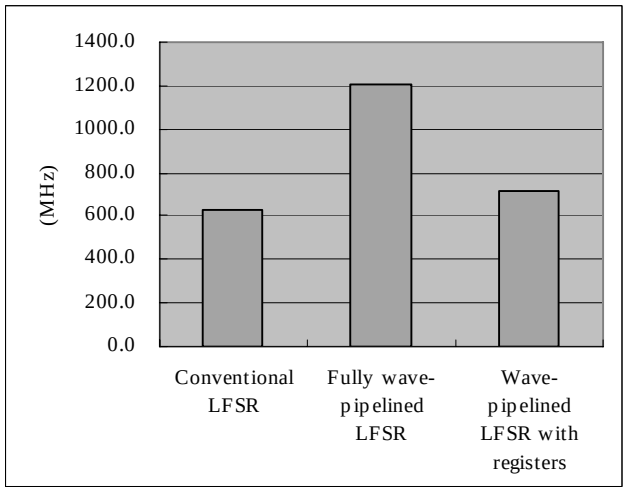
number を監視することで判断できる。

この機能を実際に Altera 社の MAX700 へ回路を書き込み検証した。表-2 のポートを許可するポートとし，それ以外のポートへのアクセスがあった場合に不正を検出するものである。ロジックアナライザを用いて実際に動作する信号を測定した結果を図-6 に示す。その結果 100MHz においても正しく動作を行うことが示された。イーサネットフレームは 12,208bits であり，FPGA 内部ではフレーム単位で処理が可能であるため，10-Gbit イーサネットにも対応可能である。現在は不正アクセスの半数を占めるポートスキャンを検地する回路の開発を行っている。

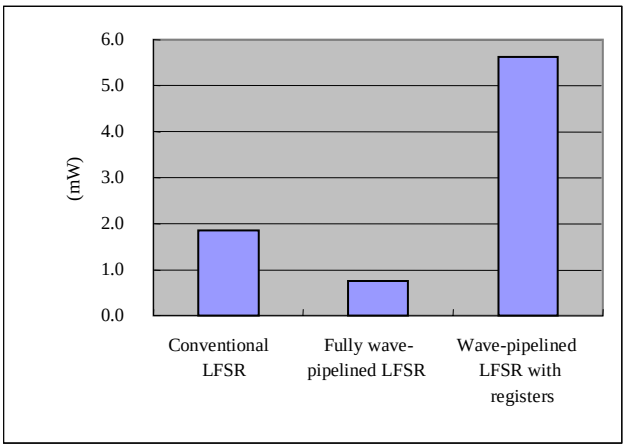
３．３　低消費電力化

無線 LAN 環境下においては，バッテリの駆動によるパソコンの使用が考えられる。とくに公衆無線 LAN においては，バッテリでの使用が前提となる。このため低消費電力化の技術が必須である。トランジスタレベルの設計が不可能な FPGA において低消費電力動作が必要である場合，低消費電力で動作する FPGA デバイスを選択するのが一般的で，この場合回路全体の動作速度を犠牲にする必要がある。我々はレジスタを使用せずにパイプライン動作が可能であるウェーブパイプライン手法を開発した[12],[13]。この手法を，多数のレジスタを必要とする CRC と WEP 処理に適用することで速度を犠牲にせずに低消費電力化を達成させる。レジスタは常にクロックが入力されるため，消費電力を増大させる原因となる[14]。

ウェーブパイプライン手法を用いるプロセッサは，商用ベースではサン・マイクロシステムズの Ultra SPARC III の SRAM の制御といった単純な構造の回路[15]，研究レベルでは加算回路[16]，乗算回路[17]といった単機能な回路で，最近になってようやく多機能回路であるスーパースカラプロセッシングユニット[18]が実現されたのみである。これらはすべて組み合わせ論理回路であり，CRC と WEP を処理で必要となる順序回



(a)



(b)

図-7 ウェーブパイプライン方式 LFSR と従来方式 LFSR の性能比較
(a) 動作速度　(b) 消費電力

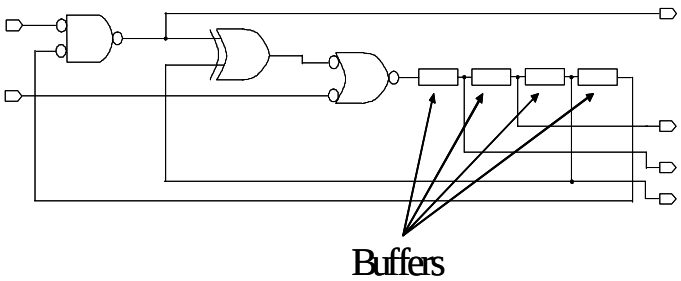


図-8. 4-bit fully wave-pipelined LFSR 回路

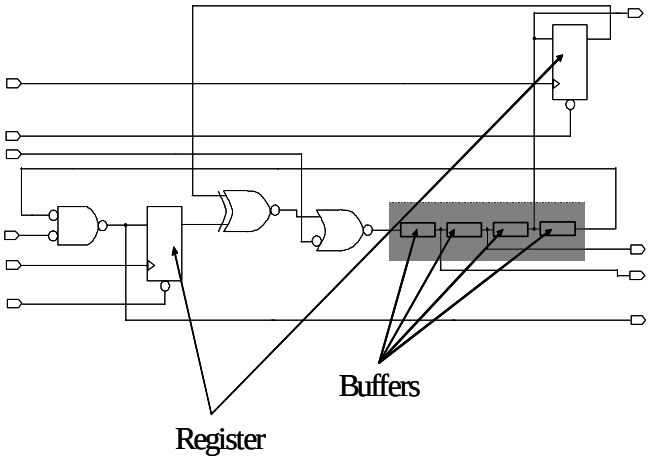


図-9 4-bit wave-pipelined LFSR with registers 回路

路は実現されていなかった。

このため我々は，CRC と WEP をウェーブパイプライン手法で処理することを目指して，CRC と WEP を構成する最小単位の LFSR (Linear Feedback Shift Register)回路のウェーブパイプライン化を行った[19],[20]。0.35 C-MOS (Complementary Metal Oxide Semiconductor)テクノロジを使用し, CAD によるシミュレーションによって従来方式の LFSR と比較評価し，その結果を図-7 に示す。図-8 の Fully wave-pipelined LFSR はレジスタを全く使用しないもの，図-9 の Wave-pipelined LFSR with registers はタイミング調整のために, LFSR 回路の両端に 2 つレジスタを使用したものである。ここでは, C-MOS を使用して評価を行っているが，ウェーブパイプライン手法は，ロジックレベルの設計が可能であるため FPGA への適用が可能である。FPGA 回路の場合タイミング調整が C-MOS と比較して厳密に行うことが困難である。このため回路の両端に 2 つレジスタを使用した Wave-pipelined LFSR with registers を適用する必要があると考えられる。

評価結果は, Fully wave-pipelined LFSR は従来方式の LFSR 回路よりを速度，消費電力の両面で優れていることが示されている。Wave-pipelined LFSR with registers は従来手法の LFSR よりも電力を消費する結果となった。しかし，ここで評価を行った LFSR は 1bit と小規模なものである。従来方式の CRC や WEP は，24 から 32 ビットのレジスタを必要とする大規模な回路である。その際も wave-pipelined LFSR with registers 回路においては，2 つのレジスタのみで動作可能である。このため Wave-pipelined LFSR with registers 回路を CRC や WEP に適用した際は, Fully wave-pipelined LFSR 回路の結果より，従来方式の CRC や WEP 回路よりも消費電力が大幅に削減できると考えられる。今後は，このウェーブパイプライン化 LFSR 回路の規模を拡大し, CRC や WEP 回路のウェーブパイプライン化を達成させる。

４．　H-HIDS の学内無線 LAN における適用

H-HIDS を導入することで，大学内のような特殊な環境においても，不正アクセスのかなりの部分を防ぐことが可能である。改善点は次のとおりである。

- オペレーティングシステムに依存しないため，オペレーティングシステムの混在する環境においても適用可能である。さらに旧来のオペレーティングシステムが導入されている機種にも適用可能である。
- 従来のソフトウェアによる HIDS と異なりパケットによる解析を主とするため，問題となる行為を直ちに防ぐことが可能である。

- 受信パケットだけでなく，送信パケットの解析も可能なため，別のルートでウイルス等に感染した場合でも，被害の拡大を防ぐことができる。
- 他のウィルス対策ソフトウェアと併用が可能である。

W32/MSBlaster ワームとその派生のワームは通常使用しないポート番号を使用して感染を繰り返すため，現時点で実現している不正なポートの機能のみでも十分対応可能である。

さらに，ウイルス対策ソフトウェアにおいても，CPU 資源をかなり消費するために，ウイルス対策ソフトウェアを動作させないで使用する例が見られる。しかし H-HIDS は CPU 資源を消費しないため，このような例も大幅に減少すると考えられる。

５．　まとめ

本論文は，ハードウェアによるパケット解析機能を有する HIDS である H-HIDS について述べた。H-HIDS は，低消費電力で動作が可能で大学内の無線 LAN 環境における問題点の大部分を解消可能である。H-HIDS の実装に使用した FPGA は US$20 以下で導入コストが安価である。また CPU リソースを消費しないこともユーザにとって大きなメリットである。今後は，H-HIDS の機能を更に充実し，より実用的な研究開発を進める。

参考文献

[1] 右田雅裕，杉谷賢一，入口紀男，喜多敏博，中野裕司，松葉龍一，武藏泰雄，辻一隆，島本勝，木田健，平英雄，太田泰史，宇佐川毅，秋山秀典，“全学無線 LAN システムによるユビキタス環境の構築，” 学術情報処理研究, No.8, pp. 17-24, 2004.

[2] 佐藤和洋，“ノート PC 活用教育情報環境の仕様策定とその活用事例報告，” 社会情報，Vol. 13, No. 1, pp. 29-64, 2003.

[3] Stephen Northcutt and Judy Novak, “Network Intrusion Detection, 2nd ed. ,” New Riders Publishing, 2001.

[4] Gregg Judge, “FPGA Architecture Ups Intrusion Detection Performance,” http://www.commsdesign.com/design_corner/showArticle.jhtml?articleID=16502099, Sep., 2003.

[5] 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.

[6] 浅香緑，女部田武史，井上直，岡澤俊士，後藤滋樹, “不正侵入の痕跡と判別分析によるリモートアタックの検出法，” 信学論, Vol. J85-B, No.1, pp. 60-74, 2002.

[7] 武井洋介，太田耕平，加藤寧，根元義章, “トラヒックパターンを用いた不正アクセス検出及び追跡方式，” 信学論, Vol.J84-B No.8 pp.1464-1473, 2001.

[8] Tomoaki Sato, Daisuke Miyamori, Rena Sakuma, and Masa-aki Fukase,“Unauthorized Port Access Detection in the H-HIDS,” Proc. of SCI2004, Vol. II, pp. 389-394,2004.

[9] 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.

[10] 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.

[11] EDN Japan, http://www.ednjapan.com/l_news/2003/04/15spartan3.html, 2003.

[12] W. P. Burleson, M. Ciesielski, F. Klass, and W. Liu, “Wave-Pipelining: A Tutorial and Research Survey,” IEEE Trans. on Very Large Scale Integration (VLSI) Systems, Vol. 6, No. 3, pp. 464-474, Sept. 1998.

[13] F. Klass and M. J. Flynn, “COMPARATIVE STUDIES OF PIPELINED CIRCUITS,” Stanford University Technical Report, No. CSL-TR-93-579, July 1993.

[14] 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, Mar. 2002.

[15] Tim Horel and Gary Lauterbach, “UltraSPARC-III: Designing Third-Generation 64-Bit Performance,” IEEE Micro, Vol. 19, No. 3, pp. 73-85, 1999.

[16] W. Liu et al., “A 250-MHz wave pipelined adder in 2-um CMOS,” IEEE J. Solid-State Circuits, vol. 29, no. 9, pp. 1117-1128, 1994.

[17] F. Klass et al., “Fast multiplication in VLSI using wave-pipelining,”　J. VLSI Signal Processing, 1994.

[18] M. Fukase, T. Sato, R. Egawa, and T. Nakamura, “Breakthrough of Superscalar Processors by Multifunctional Wave-Pipelines,” Proc. of 9th NASA Symposium on VLSI Design, pp. 6.3.1-6.3.17, Nov. 2000.

[19] 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.

[20] Tomoaki Sato, Rena Sakuma, Daisuke Miyamori, and Masa-aki Fukase,“Performance Analysis of Wave-Pipelined LFSR,” Proc. of ISCIT 2004, pp. 694-699, 2004. .