科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月　 ２ 日現在

機関番号：１１１０１
研究種目：若手研究(B)
研究期間：2011～2013
課題番号：２３７０００６８

研究課題名（和文）多重化データバスを有する再構成可能なホストベースＩＰＳプロセッサチップの開発

研究課題名（英文）Development of the Reconfigurable Host-Based IPS Processor with the Multiplexed Data Bus

研究代表者
佐藤　友暁（Sato, Tomoaki）

弘前大学・総合情報処理センター・准教授

研究者番号：００３３６９９２

交付決定額（研究期間全体）：（直接経費）　　3,400,000円、（間接経費）　　1,020,000円

研究成果の概要（和文）：スマートフォンやバッテリで稼働するノートパソコン上で稼働可能な高検知精度IPSプロセッサは，MACユニット，再構成可能な検知ユニットとファイアウォールユニットおよびCPUで構成される。これらのユニット間はパケットフレーム単位で大量のデータの転送が必要なバスが不可欠である。したがって大量の配線が必要となる。本研究では高効率なパケット転送を可能にすることを目的として，ウェーブ化技術を使用した多重化バスは開発される。多重化バスは評価され，その結果多重化動作が可能であることを明らかにする。さらに，IPSプロセッサに必要なCPUの性能評価や無線LANの暗号強度の強化を行う。

研究成果の概要（英文）：The Reconfigurable Host-Based IPS Processor is developed for a highly accurate detection of unauthorized computer access in a smartphone or a personal computer with battery operation. The processor is composed of MAC Unit, Firewall Logic Unit with LUTs for Intrusion Prevention and a CPU. Each unit is connected with a bus to carry Ethernet frames. That is, a huge number of wiring is required. In this study, a multiplexed bus is developed by using wave-pipeline technique aiming at a highly effective packet forwarding. The bus is evaluated, and the multiplexing operation of the bus is confirmed. In addition, the performance of the CPU needed in the processor is evaluated and cipher strength of the wireless LAN in the processor is strengthened.

研究分野：総合領域

科研費の分科・細目：計算機システム・ネットワーク

キーワード：ネットワークセキュリティ技術　不正侵入防御システム

１．研究開始当初の背景

不正アクセスやコンピュータウイルスによる情報漏えいや情報改ざんは今日の重要な問題になっています。これらの問題に対し，IDS (Intrusion Detection System)や IPS による監視と被害防止が不可欠です。このような，不正アクセスやコンピュータウイルスを防ぐために，IDS (Intrusion Detection System)や IPS(Intrusion Prevention System)による監視と被害防止が不可欠です。さらに，これらの IDS や IPS で実行される処理として，ホストベースと呼ばれるスマートフォンやバッテリで稼働するノートパソコン上において，詳細なパケットレベルの解析が必要です。

２．研究の目的

本研究の目的は，多様なネットワーク環境下で使用されるスマートフォンやモバイル PC (Personal Computer)においても適用可能であり，省スペース・低消費電力で動作するホストベース IPS プロセッサを実現することです。本研究では，この目的を実現するために，CPU，MAC，ファイアウォールユニット間のデータ転送を高速かつ高効率で行うために重要なバスの開発，これを制御するための CPU の開発，さらに IPS プロセッサの実現に不可欠なユニットの開発を行うことです。

３．研究の方法

本研究で開発を進めている H-HIPS (Hardware- and Host-based IPS) は FPGA と同様の再構成可能なロジックセルを有し，H-HIPS 向けに最適化された MIPS CORE を搭載した IPS プロセッサで構成される。IPS プロセッサは，イーサネット MAC，検知ユニット，制御用の MIPS CORE 間をイーサネットフレームの単位によるバス幅で接続する必要がある。このバスの構成は図２に示される。このイーサネットフレームは 1，518bytes であるため，膨大な配線が必要になる。

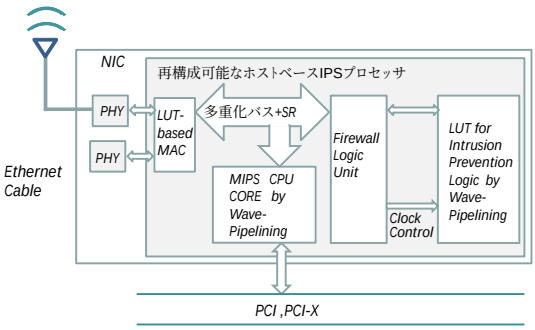

図１ H-HIPS

本研究では，ウェーブ化による多重化バスを開発し，ゲートレベルシミュレーションによって多重化動作が可能であることを示し，配線の削減が可能であることを明らかにする。

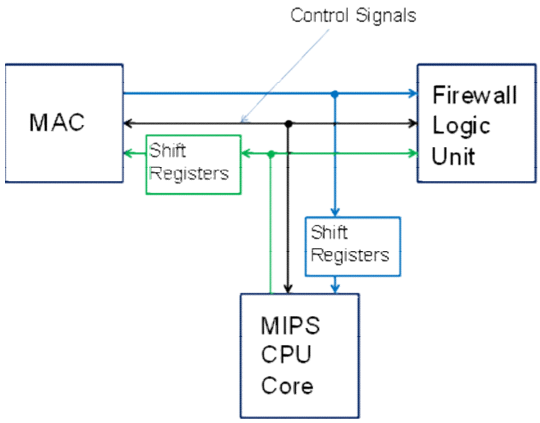

図２　バス構成

図３が二つの信号線を多重化し１本の線で信号を運ぶための多重化回路，図４は一本の線から２つの信号線に信号を分離するための分離回路である。

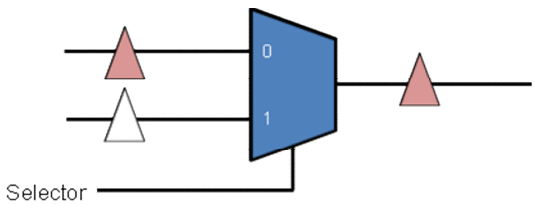

図３　多重化回路

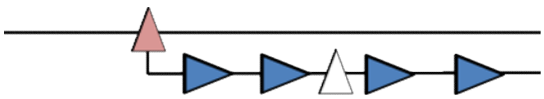

図４　分離回路

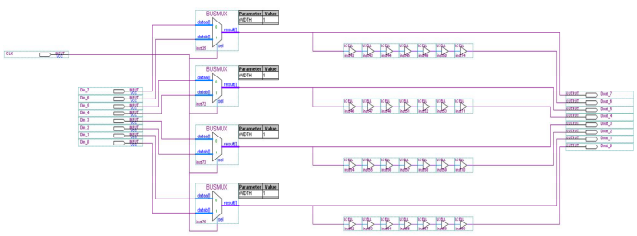

図５　FPGA を使用した多重化回路

図３と図４を FPGA 上に実装する。この成果は次章に示される。実装の際に使用した CAD は Altera 社の Quartus II である。また FPGA は，Altera 社の Cyclone EP1C3T100C6 を使用した。

次に多重化バスを使用して，IPS プロセッサ内の各ユニットを制御するための CPU の開発を行う。この CPU はネットワークルータ等のネットワーク機器で使用されている MIPS アーキテクチャを使用する。この CPU はバッテリで駆動することが前提であるため，スマートフォンで使用される CPU よりもさらに低消費電力で動作することが求められる。

一方，1Gbps 以上の高速なスループットでの処理も求められます。例えば，4K TV において医療用の動画を表示する場合は，1Gbps をさらに超えるスループットが必要となります。そこで本研究では表１に示すパケットサイズを使用し，MIPS32 4K を使用し，MIPS32 4K 上で動作するアセンブリプログラムを作成した。このプログラムを使用しパケットの処理能力を調査する。

表１　パケットフレーム

Type of Ethernet flame	**Flame size**	**Processing time in MAC Unit**	**Number of operations in 32-bit**	**Number of operations in 64-bit**
Minimum size flame	65 Bytes	520 ns	17	9
Standard size flame	1519 Bytes	12152 ns	380	190
Jumbo flame (3000KB)	3019 Bytes	24142 ns	755	378
Maximum jumbo flame	16000 Bytes	128000 ns	4000	2000

H-HIPS は，有線 LAN やモバイル通信のみならず，無線 LAN にも対応する。無線 LAN は，容易に盗聴が可能であるため，暗号が使用されている。この暗号方式として，特に日本の公衆無線 LAN で WEP が広く使用されている。しかし WEP は，容易に暗号を解読できる問題がある。このため本研究者らは WEP と互換性を有し暗号強度を強化したアルゴリズムを開発している。本研究ではこのアルゴリズムを再構成可能なデバイスである FPGA 上に実装する。

４．研究成果

図５の回路の多重化動作をゲートレベルシミュレーションで動作可能であることを明らかにした。図６はゲートレベルシミュレーションの結果である。この結果より多重化動作が確認され，正しく動作することが明らかになった。

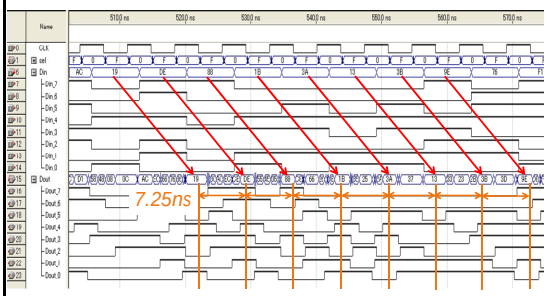

図６　FPGA を使用した多重化回路

表２　多重化バスのためのシフトレジスタ

	Conventional	Waved (17 cells)	Waved (18 cells)	Waved (19 cells)
Clock rate (GHz)	2.0	2.0	2.0	2.0
Throughput (Gbps)	64.0	115.2	115.2	128.0
Delay time (ns)	**2.50**	**2.41**	**2.61**	2.68
No. of stages	5	9	9	10
Area (μm^2)	**7670.48**	7328.56	**7638.22**	**7947.88**
No. of cells	238	544	576	608
Total power (mW)	1.69	0.95	0.97	0.98
Leakage Power (nW)	10.47	9.70	9.9	10.15

表３　CPU 処理時間

Frequency of the CPU	**Minimum size flame (ns)**	**Standard size flame (ns)**	**Jumbo flame of 3000 KB (ns)**	**Maximum jumbo flame (ns)**
500MHz	760.0	15280.0	30280.0	160080.0
800MHz	380.0	7640.0	15140.0	80040.0
1GHz	237.5	4775.0	9462.5	50025.0
1.2GHz	190.0	3820.0	7570.0	40020.0
1.5GHz	158.3	3183.3	6308.3	33350.0
2.0GHz	126.7	2546.7	5046.7	26680.0
3.0GHz	95.0	1910.0	3785.0	20010.0
4.0GHz	63.3	1273.3	2523.3	13340.0

表２において，多重化バスのタイミング調整に必要なシフトレジスタの性能を示す。Conventional は通常のシフトレジスタを使用したレジスタ，残りはウェーブパイプライン方式で実現されたシフトレジスタである。ウェーブパイプライン方式のシフトレジスタは多重化動作が可能である。

この結果より，ウェーブ方式は遅延時間で比較した場合，通常のものよりも消費電力と面積が若干小さくなる。ウェーブ方式のスループットについては約 1.8 倍に高速化されることが明らかになった。

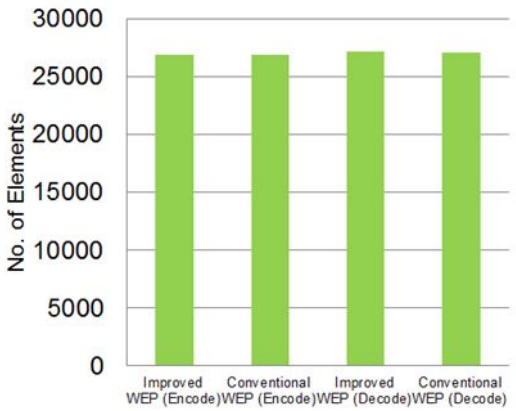

図７　エレメント数

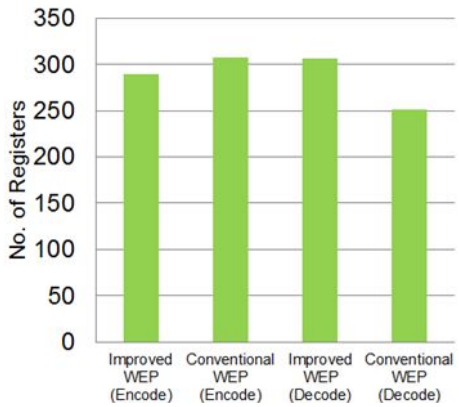

図８　レジスタ数

図７は，WEP 回路のエレメント数を示し，図８はレジスタ数を示す。この結果より，通常型の WEP 回路とエレメント数はほぼ同数であることが明らかになった。また，レジスタ数は通常方式よりも 55 個増加することが明らかになった。

レジスタ数が 55 個程度の増加は，リソースおよび消費電力の観点ではシステム全体への影響は限定される。その一方で，改良型 WEP は暗号強度が強化され，スループットも同一である。

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　９件）

① Tomoaki Sato, Phichet Moungnoul, and Masa-aki Fukase, "Delay Time Analysis of Reconfigurable Firewall Unit," Proc. of the 4th International Multi-Conference on Engineering and Technological Innovation, Vol. II, pp. 109-114, 2011.**査読有**

② Tomoaki Sato, Phichet Moungnoul, and Masa-aki Fukase, “Throughput Evaluation of Improved WEP Processing on a Mobile Processor,” Proceeding of 1st International Symposium on Technology for Sustainability, pp. 325-328, 2012. **査読有**

③ **佐藤友暁，今田智也，モングノウル　ピシェット，深瀬　政秋**, “**改良型** WEP **アルゴリズムのハードウエア実装**,” **信学技報**, Vol. 112 No. 78, pp. 1-5, 2012. **査読無**

④ Tomoaki Sato, Phichet Moungnoul, and Masa-aki Fukase, "Packet Filtering Circuits for Smart Phones," Proc. of The 16th World Multi-Conference on Systemics, Cybernetics and Informatics, Vol. II, pp. 5-9, 2012. **査読有**

⑤ Tomoaki Sato, Phichet Moungnoul, Masa-aki Fukase, "Delay Time Analysis of Reconfigurable Firewall Unit," Journal of Systemics, Cybernetics and Informatics, vol. 10, no. 5, pp. 80-84, 2012. **査読有**

⑥ Tomoaki Sato, Phichet Moungnoul and Masa-aki Fukase, "Multiplexed Bus for Mobile Communications and an IPS," Proceedings of The 2013 International Electrical Engineering Congress (iEECON2013), pp. 257-260, 2013. **招待論文**

⑦ Tomoaki Sato and Phichet Moungnoul, “Hardware Amount Evaluation of the Improved WEP on an FPGA,” Proc. of ECTI-CON 2013, pp. 1760.1-1760.6, 2013. **査読有**

⑧ Tomoaki Sato, Sorawat Chivapreecha, Phichet Moungnoul and kohji Higuchi, "Evaluations of Waved-Shift Registers for Multiplexed Bus," Proceedings of The 2014 International Electrical Engineering Congress (iEECON2014), pp. 109.1-109.4, 2014. **査読有**

⑨ Tomoaki Sato, Phichet Moungnoul, Sorawat Chivapreecha and Kohji Higuchi, "Performance Estimates of an Embedded CPU for High-Speed Packet Processing," Proc. of ECTI-CON 2014, pp.1298.1-1298-5, 2014. **査読有**

〔学会発表〕（計　２件）

① Tomoaki Sato, "Reconfigurable Circuits for Secure Mobile Computing," 2011 International Symposium on Multimedia and Communication Technology (ISMAC 2011), Sapporo, Japan, Sept. 2, 2013. **招待講演**
② Tomoaki Sato, "Digital Circuit Design and Network Security in the Digital TV Era," International Conference on Digital Broadcasting, Bangkok, Thailand, Jul. 27, 2013. **招待講演**

〔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
佐藤　友暁（SATO TOMOAKI）
弘前大学・総合情報処理センター・准教授
研究者番号：00336992

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：