氏名（本籍）	わかば　よういち 若葉　陽一（広島県）
学位の種類	博士（情報工学）
学位記番号	甲第106号
学位授与年月日	平成26年3月24日
学位授与の要件	広島市立大学大学院学則第36条第2項及び広島市立大学学位規程第3条第2項の規定による
学位論文題目	ネットワーク侵入検知のためのパターン非依存正規表現マッチングハードウェアに関する研究
論文審査委員	主査　教授　若林真一
	副査　教授　井上智生
	副査　教授　弘中哲夫
	副査　准教授　永山忍

論文内容の要旨

インターネットの普及に伴い、コンピュータウィルス等の脅威も増加している。その対策の１つとしてネットワーク侵入検知システム（NIDS）がある。NIDS はネットワークセキュリティの向上のため、ネットワーク上を流れる通信パケットを監視するシステムである。NIDS はコンピュータウィルスを正規表現で定義したパターン（ウィルスパターン）と通信パケットに対する正規表現マッチングを行うことで、ウィルスの検知を行う。ここで、正規表現とは文字列の集合を１つの文字列で表現する方法であり、正規表現マッチングとは、正規表現を用いて記述されたパターンと一致する部分文字列をテキスト中から検索する操作である。

現在のネットワーク環境下におけるNIDSの正規表現マッチングにおいて、以下の要件を全て満たすことが望ましい。（要件1）高速ネットワーク（ギガビットイーサネット）上でリアルタイムなウィルス検知ができる、（要件2）どんなウィルスパターンでも扱うことができる、（要件3）多数のウィルスパターンをコンパクトな回路で扱ことができる、（要件4）新しいウィルスに素早く対応するため、パターン更新を瞬時に行うことができる。

ソフトウェアによる正規表現マッチングでは（要件1）を満たす事が難しいため、様々な正規表現マッチングハードウェアが提案されている。既存のハードウェアは大きく分けてパターン依存型とパターン非依存型に分類される。パターン依存型は与えられたパターンに特化した回路構成を持ち、高速かつコンパクトな回路規模で正規表現マッチングを実現できる。しかしパターンが更新される度に回路を再設計する必要があり、パターン更新に時間がかかる。パターン非依存型は任意のパターンに対応できる回路構成を持ち、パターンの更新を瞬時に行えるという利点を持つ。しかし、任意の正規表現を扱うマッチングハードウェアは非現実的な回路規模と性能となるため、扱う正規表現を制限したマッチングハードウェアが提案されている。

本論文では、上述の全ての要件を満たす正規表現マッチングハードウェアを実現するために、(1)シストリックアルゴリズムと非決定性有限オートマトン（NFA）を組み合せた新しいマッチングハードウェア、(2)FPGAの部分再構成機能に基づく回路面積の削減手法、(3)拡張正規表現に対するマッチング手法、を提案する。本論文の成果により、NIDSにおいてパフォーマンスの低下を招くことなくウィルス検知が可能となり、ネットワークのセキュリティが向上することが期待される。

本論文では４章で、任意の正規表現を扱うことができるパターン非依存正規表現マッチングハードウェアを提案する。既存のパターン非依存正規表現マッチングハードウェアのほとんどは、回路構造の制約からマッチング可能な正規表現が制限されている。そのため、パターン更新時に検知可能なウィルスが制限される。また任意の正規表現を扱うことができる既存のパターン非依存正規表現マッチングハードウェアは、複雑な回路構造を持つため実用的な回路規模ではない。そこで、本論文では単純な回路構造を持つシストリックアルゴリズムに基づくハードウェアと任意の正規表現を扱うことができるNFA に基づくハードウェアの利点を活かしながら組み合わせることで、任意の正規表現パターンに対応可能であり、しかも回路規模がコンパクトなパターン非依存正規表現マッチングハードウェアを提案する。提案ハードウェアは文字列遷移双対位置オートマトンに基づいている。文字列遷移双対位置オートマトンにおける文字列に対するマッチングはシストリックアルゴリズムに基づくハードウェアで実現し、状態遷移はNFAに基づくハードウェアで実現される。実験的評価から、任意の正規表現を扱うことができる既存のパターン非依存ハードウェアと比べ実用的な回路規模でマッチングを実現できることを示す。

４章で提案するハードウェアは任意の正規表現を扱うことができ、回路規模は実用的ではあるが、やはり大きい。そこで５章において、任意の正規表現を扱うことができかつ瞬時にパターン更新が可能であるという特長を保ちつつ、回路面積を削減する手法を提案する。提案手法では、FPGAの部分再構成機能を用いて与えられた正規表現パターンに合わせた回路構成を瞬時に生成する。提案手法では、正規表現の異なる部分クラスを扱う部分回路が複数個あらかじめ用意されている。正規表現パターンが与えられた時、そのパターンに適したコンパクトなマッチングハードウェアが部分回路の組み合わせにより自動生成され、部分再構成によってFPGA上に実装される。提案手法はパターン更新時に長い時間を要する回路の再設計を必要としない為、高速にパターンを更新でき、かつ与えられたパターンに特化した回路を生成できる。実験的評価から、提案手法は４章で示すハードウェアと比べ、63%の回路面積を削減できる事を示す。

NIDSのパターン記述においては、ユニオン等の基本演算子だけでなく量指定子等の様々な演算子を導入した拡張正規表現もよく用いられる。拡張正規表現を用いると、パターンをより簡潔に記述することができるだけでなく、正規表現では表せないパターンを記述することもできる。そこで、６章において、拡張正規表現に対するハードウェアマッチング手法を提案する。拡張正規表現の中で、量指定子やクラス文字に対するハードウェアマッチング手法は既に提案されているが、先読み演算や後方参照に対するマッチング手法は提案されていない。そこで、これらの演算子に対するハードウェアマッチング手法を提案する。先読み演算に対しては、４章で提案したパターン非依存正規表現マッチングハードウ

ェアに前処理回路を導入する。前処理回路はテキストの末尾から先頭に検索を行うことで先読み演算のマッチングを行う。また高スループットを達成するために、スタックメモリを用いた新しいバッファ機構を提案する。後方参照に対しては、４章で提案したマッチングハードウェアを使った前処理手法を提案する。この手法はバックトラックに基づいたマッチングアルゴリズムによる検索において、不必要な検索を可能な限り削減する。それによって高速な後方参照に対するマッチングを実現する。実験的評価から、これらの演算子をハードウェアで効率的に扱える事を示す。

論文審査の結果の要旨

平成26年2月13日午前10時40分から正午まで博士学位論文発表会（公聴会）を開催した。申請者が論文内容について説明を行い、その後、論文内容に関する質疑応答および議論を行った。発表会終了後の正午から午後0時20分まで審査委員会を開催し、論文の合否に関する審議を行った。

ネットワーク侵入検知システム（NIDS）はネットワークセキュリティの向上のため、ネットワーク上を流れる通信パケットを監視するシステムである。NIDSはコンピュータウィルスを正規表現で定義したパターン（ウィルスパターン）と通信パケットに対する正規表現マッチングを行うことで、ウィルスの検知を行う。NIDSにおける正規表現マッチングは従来、ソフトウェアによって実装されることが一般的であったが、近年、検索対象のパケットの伝送速度とパターン数が著しく増加しており、正規表現マッチングに要する時間の短縮が求められている。博士学位論文は伝送速度1Gbps以上の高速ネットワークを対象とするNIDSに対する新しいマッチングハードウェアの構成手法を提案することで、ネットワークセキュリティの向上に貢献することを目的としている。

本論文にまとめられている主な成果は、国内ジャーナル論文（フルペーパ）1編、国際会議3編（うち2編はショートペーパ）、国際ワークショップ2編（以上、すべて査読付き）として公表されている。

発表会においては、申請者から博士論文研究の内容が的確に説明され、質疑応答も適切だった。聴講者や審査委員の質疑から発して、今後の研究課題も含めた議論も活発に行われた。また、英語による論文執筆、国際会議発表の実績もあることから、申請者は十分な外国語能力を有すると判断された。以上より、申請者は博士（情報工学）を取得するのに十分な専門知識と資格を有しているものと認め、審査委員会は試験（諮問）を合格と判定した。