要 旨

二段 AC アルゴリズムの
自己タイミング型パイプライン実装

永尾 徹

将来のユビキタスネットワーク上の携帯通信機器は，様々なネットワークに接続し得るため，いわゆるウィルスなどの悪意ある攻撃を受けやすい．そのため，組込み機器向けのセキュリティ機能を持つ組込みパーソナルゲートウェイ (EPG) が必要である．我々の研究室では，省電力データ駆動型ネットワークプロセッサ (DDNP) を用いたセキュリティ機能の効果的な LSI 実現法を検討している．その一環として，本研究では，性能を支配するシグネチャマッチングエンジンを自己タイミング型パイプライン (STP) を用いて実装する．

ペイロード全体から悪意ある攻撃を発見するシグネチャマッチングのために，古典的な AC アルゴリズムの冗長性を減らし，シグネチャマッチングを高速化する二段 AC アルゴリズムが提案されている．二段 AC アルゴリズムは，状態遷移の深さにより区切られた，上段と下段の二つの FSM で実装される．STP は，DDNP と親和性が高いため，シグネチャマッチングエンジンの実装において，DDNP との同期をとるためのインタフェースなどを必要とせず，回路の簡単化による省面積化や高スループットが期待できる．提案回路は TSMC 社の 0.18μm CMOS 6LM ライブラリを用いて設計した．論理合成・配置配線には，それぞれ Cadence 社の Build Gates・Silicon Ensemble を用いた．結果，メモリ容量 21.3KB，回路面積 2.07mm^2，一文字当たりのメモリ消費量 48.6B/char，面積利用率 2200char/mm^2，及びスループット 1.24Gbps となり，IEEE 802.11n などの無線通信方式に十分対応できる．

キーワード　二段 AC アルゴリズム，自己タイミング型パイプライン，組込みパーソナルゲートウェイ，シグネチャマッチング

Abstract

Self-Timed Pipeline Implementation of Two-Layered AC Algorithm

Toru Nagao

A self–timed pipeline(STP) implementation of the two-layered AC algorithm(TLAC) is studied in this dissertation. This implementation aims to realize the signature matching engine (SME) of our embedded personal gateway(EPG) which can provide both gateway and security functions for mobile devices in ubiquitous network.

The EPG is implemented on the data–driven network processor(DDNP), in which a flexible asynchronous circuit called STP is adopted because of its low power consumption and high flexibility. In EPG, each SME employs a signature matching algorithm called TLAC algorithm and works as an internal accelerator independently. The STP implementation of the TLAC algorithm is adopted, because a relatively large interface and overflow detection circuits between the SME and other modules are necessary if the SME is realized by a synchronous circuit.

The ASIC implementation of the proposed solution is realized based on the 0.18μm–CMOS standard library of TSMC. The results shows that an SME accepting a signature set of 4682 characters at the cost of 21.3 KB SRAM,is customized into 2.07 mm^2 area and processes at 1.24 Gbps throughput. The results shows a excellent area efficiency and satisfactory requirements of the SME on EPG.

key words Two–Layered AC algorithm, Self–Timed Pipeline, Embedded personal gateway, signature matching