

プレフィックス展開と比較回路の併用による アクセス制御リストの効率的な管理

黄 恵聖†, 山本 耕次‡, 阿多 信吾§
井上 一成‡, 村田 正幸†

大阪大学 大学院情報科学研究科†
株式会社ルネサステクノロジ‡
大阪市立大学 大学院工学研究科§

Outline

- 研究背景
- 用語説明
 - アクセス制御リスト (Access Control List)
 - TCAM (Ternary Content Addressable Memory)
 - プレフィックス展開 (Prefix Expansion)
- 関連研究および研究目的
- 研究内容
 - 比較判定回路 (Range Matching Device)
 - TCAM デバイスの制御 (RMD 格納 + PE-MIN)
- 提案方式の評価
- まとめ

07.12.13

IN 研究会

2

研究背景

- 高速なパケット分類のために使用されている TCAM の問題点
 - 消費電力, チップの面積, LSI通信のコスト (I/O)
- TCAM に格納する, アクセス制御リスト (Access Control List; ACL) フィールドの中, ポート番号の範囲表現問題
 - TCAM 容量の消費量増加

07.12.13

IN 研究会

3

用語説明

- ルータで, セキュアなネットワークを確保するためアクセス制御リスト (Access Control List; ACL) を持つ必要がある
- 高速に ACL を検索するために, 連想メモリ (Ternary Content Addressable Memory; TCAM) を使用する
- 格納される ACL の行数を減らすために, プレフィックス展開 (Prefix Expansion; PE) 方法を使用する

07.12.13

IN 研究会

4

アクセス制御リスト (ACL)

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
access-list 102 deny tcp any range 137 139 any
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo
access-list 191 permit udp any any range 16384 16483
```

- セキュアなネットワークを確保するために, ルータが持つリスト
- 送受信 IP アドレス, 送受信ポート番号, プロトコル番号の組み合わせで構成

07.12.13

IN 研究会

5

Ternary CAM

- 格納された内容を検索し, 入力データの位置や内容を返す記憶デバイス
- 各ビットには 0, 1, 任意の値 * を格納可能
- 問題点: SRAM に比べ, 多いチップの配線による高い消費電力

- **高速な検索可能**
 - IP アドレスの最長プレフィックスマッチに有利
 - TCAM の構造は簡単で, 理解が容易
 - ベンダーごとに異なるパケット分類に対して, 標準化された TCAM が利用可能

07.12.13

IN 研究会

6

プレフィックス展開

```

1***** 32768 - 65535
01***** 16384 - 32767
001***** 8192 - 16383
0001***** 4096 - 8191
00001***** 2048 - 4095
000001***** 1024 - 2047
  
```

- ポート範囲 1024 - 65535 に対し、
 - フル展開: 64512 行
 - プレフィックス展開: 6 行
- 2ⁱ の単位で範囲を記述することが可能
- ワーストケース: 16385 - 65534 の場合 29 行

07.12.13 IN 研究会 7


関連研究

- ソフトウェアが中心となった処理
 - 範囲のエンコード (ビットマッピング情報が必要)
 - 重複プレフィックスの消去
- ハードウェア関連研究
 - 外部の装置を利用
 - 複数の TCAM を利用 (TCAM 自体の変更は回避する研究が多数)

07.12.13 IN 研究会 8

研究目的

- TCAM 内部のデバイス搭載による I/O ピンと TCAM セルの節約
- プレフィックス展開の最適化による範囲展開のワーストケースが減少



比較判定回路と最適なプレフィックス展開の併用による TCAM 消費量削減

07.12.13 IN 研究会 9

比較判定回路 (Range Matching Device, RMD)

Conventional TCAM					Bits added for RMD			
SRC IP (32)	DST IP (32)	SRC Port (16)	DST Port (16)	Prot (8)	1	*	*	*
*	*	*	*	*	1	*	*	*
*	*	*	*	*	*	1	*	*
*	*	*	*	*	*	*	1	*
*	*	*	*	*	*	*	*	1

HIT

Port Range From~To in RMD :
 Search Key : 2436 →

Port Range From~To

Search Key

RMD

TCAM

- 既存の TCAM に、範囲を記憶する RMD 用のビットを用意

07.12.13 IN 研究会 10

RMD の論理回路

<入力>

送/受信ポート

- FROM
- TO

<大小比較機>

検索キーが FROM~TO の範囲内か判断

<結果>

出力

- 送信元/宛先を区別し、範囲の下限と上限を格納しておく
- 検索時は大小比較機を通じ、ポートの範囲内にあるか判断

07.12.13 IN 研究会 11

プレフィックス展開の拡張

範囲 5000-6000 に対するプレフィックス展開

- PE-OR: 従来のプレフィックス展開

- PE-Exclusive: +完全包含範囲 - 不要部分

07.12.13 IN 研究会 12

プレフィックス展開の最適化

5000: 1001110001000
 5120: 1010000000000
 6000: 1011101110000

14992-5119 5120 5120-6143
 24992-4999 6000 6016-6143

- $5120 - 5000 = 120 = 128 - 8 = 64 + 32 + 16 + 8$
- $6000 - 5120 = 880 = 1024 - 128 - 16 = 1024 - 256 + 128 - 16$
 $= 1024 - 256 + 64 + 32 + 16$
 $= 512 + 256 + 128 - 16 = 512 + 256 + 64 + 32 + 16$

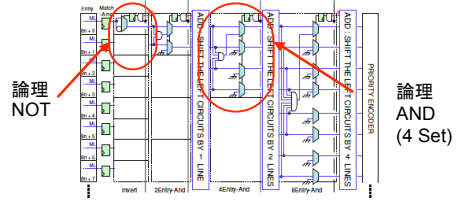
- PE-MIN: 総当たりにより、もっともエントリが少なくなるよう最適化されたプレフィックス展開を求める
- 本研究では PE-OR と PE-MIN を使用して評価

07.12.13

IN 研究会

13

TCAM + 論理 NOT/AND 追加回路



- PE-Exclusive や PE-MIN の結果を格納するために、既存の TCAM に論理ゲートを追加
- 行数の無駄を最少にするために ADD 部分が発生

07.12.13

IN 研究会

14

TCAM デバイス制御

- RMD への格納ポリシー
 - RMD に格納する範囲の順位決定
- プレフィックス展開の最適化 (PE-MIN)
 - RMD に格納されなかった範囲の表現

07.12.13

IN 研究会

15

RMD格納ポリシー

- Weight = (プレフィックス展開後の行数 - 1) x (その範囲を参照している ACL 数)
- 同一な Weight を持つ場合、(PE-MIN) x (# of ranges) 順で RMD に格納

Range	PE-MIN lines	# of Ranges	PE-MIN x # of Ranges	Weight
2326 - 2837	8	16	128	112
6970 - 6999	4	18	72	54
5555 - 6555	10	6	60	54
5555 - 5587	5	11	55	44
3230 - 3253	4	14	56	42

07.12.13

IN 研究会

16

提案方式の評価

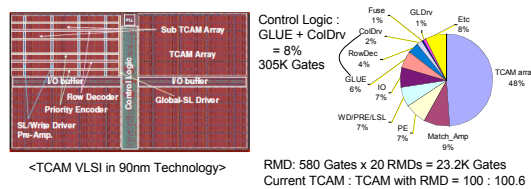
- RMD 搭載のシリコンオーバーヘッド
- RMD によるエントリ削減効果
 - RMD を使用し、RMD に格納しきれなかった範囲については PE-MIN で TCAM に格納
- ACL 格納部分の変更効果

07.12.13

IN 研究会

17

シリコンオーバーヘッドの検証

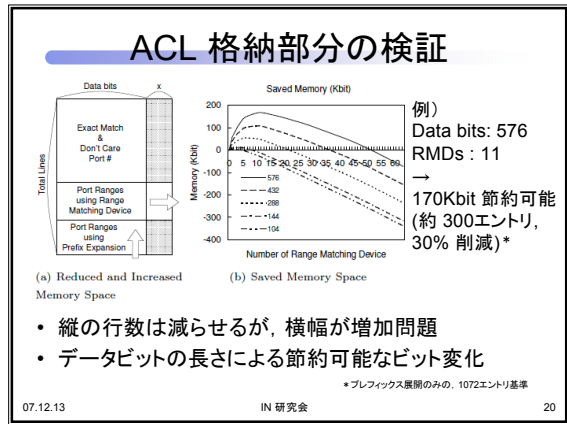
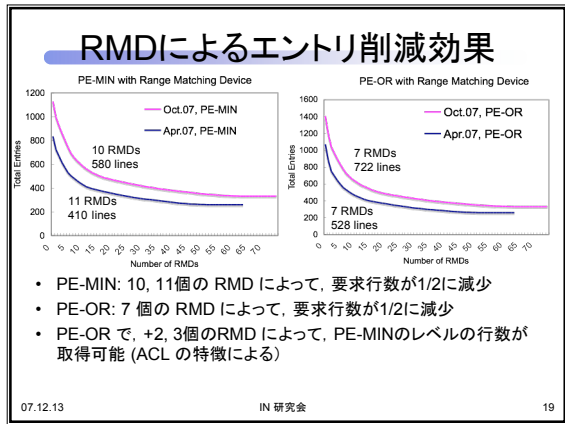


- 既存の TCAM に、RMD を 20個搭載した場合、シリコンオーバーヘッドは 0.6% 増加

07.12.13

IN 研究会

18



- ### まとめ
- 範囲比較デバイスと最適プレフィックス展開を併用した新しい TCAM を提案
 - 実運用 ACL を使用した評価
 - 今後の課題
 - 多様な実運用 ACL についての評価を通じた、提案方式の汎用性提示
 - 提案した改良 TCAM をネットワークプロセッサに搭載し、評価
- 07.12.13 IN 研究会 21

ご清聴ありがとうございます。

07.12.13 IN 研究会 22