75.43 - Introducción a los Sistemas Distribuidos

Gigabit Rate Packet Pattern-Matching Using TCAM

Guido Movia - 102896

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.385.6912&rep=rep1&type=pdf

Motivación

- ¿Cómo prevenir la propagación de virus en la red?.
- Sistemas de detección de intrusos.
- Esquemas basados en la cooperación del usuario final.
- Tiempo de reacción lento.
- ¿Es posible utilizar esquemas que soportan velocidades de gigatibts?.
- Esquemas basados en la red.

Definición del problema

- Reportar todos los patrones contenidos en un paquete.
- Tipos de patrones.
  - Patrones simples
    - Deterministas.
    - No deterministas
      - Alfabetos.
      - Comodines.
  - Patrones compuestos
    - Negación
    - Correlacionados

Soluciones alternativas

Esquemas basados en software:

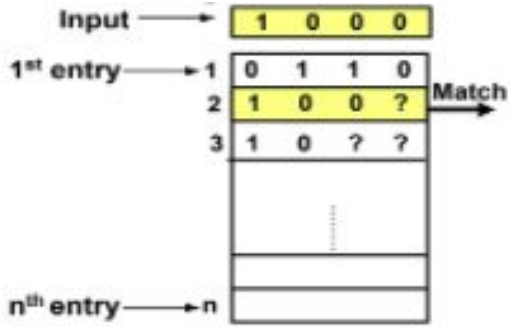
- Algoritmo de Knuth-Morris-Pratt (KMP).
- Algoritmo de Boyer-Moore.
- Algoritmo de Aho-Corasick.
- Algoritmo de Commentz-Walter.

Esquemas basados en hardware:

- Solución vía FPGA.
- Solucion via filtro bloom.

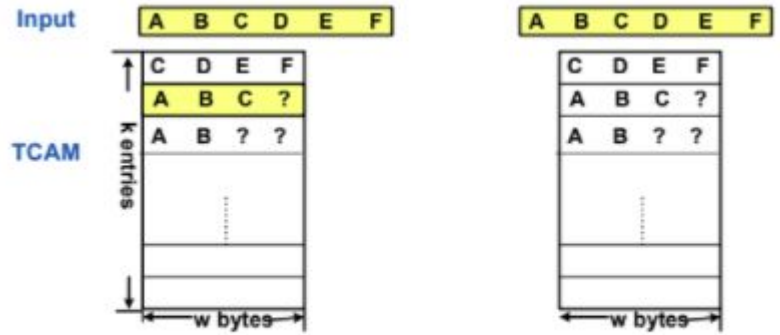
Memoria direccionable de contenido ternario (TCAM)

- Recibe un contenido en vez de una dirección de memoria.
- Reporta la primer entrada coincidente.
- Tasa de acceso y tasa de procesamiento constante.
- Tres estados: 0, 1 y “?” (no importa).
- Utilizada por los routers para la búsqueda de prefijos IP.



Coincidencia de patrones múltiples con TCAM

- Solución para patrones simples deterministas con n <= w
  - Tabla de patrones simples



3.a First Position 3.b Second Position

Figure 3. Scanning Process.

Coincidencia de patrones múltiples con TCAM

- Solución para patrones simples deterministas con n > w
  - Tabla de patrones largos
  - Tabla de patrones simples, prefijos, sufijos
  - Tabla de patrones combinados
  - Tabla de aciertos parciales (PHL)
  - Tabla de matcheo

Table 1. Long Pattern Examples.

Pattern Index	Pattern Contents	Prefix Patterns	Suffix Patterns
1	ABCDABCD	ABCD	ABCD
2	DEFGABCDL	DEFG	ABCDL
3	DEFGDEF	DEFG	DEF
4	DEF	-	-

Table 2. Patterns in the TCAM.

TCAM Index	Content
1	ABCD
2	DEFG
3	BCDL
4	GDEF
5	DEF?

Table 3. Combined Pattern Table.

Index (Content)	Simple Pattern Index	Prefix Index	Suffix Index
1(ABCD)	-1	1	1
2(DEFG)	4(DEF)	2	-1
3(BCDL)	-1	-1	2
4(GDEF)	-1	-1	3
5(DEF ?)	4(DEF)	-1	-1

Table 4. Partial Hit List.

Compressed Index	Position
1	1

Table 5. Matching Table.

Prefix Index	Suffix Index	Distance	Matched Long Pattern Index
1(ABCD)	1(ABCD)	4	1(ABCDABCD)
2(DEFG)	1(ABCD)	4	3*(DEGFABCD)
2(DEFG)	3(GDEF)	3	3(DEGFDEF)
3(DEGFABCD)	1(ABCD)	4	1(ABCDABCD)
3(DEGFABCD)	2(BCDL)	1	2(DEFDABCDL)

Coincidencia de patrones múltiples con TCAM

- Ejemplo de búsqueda de patrones en la cadena “DEFGABCDL”.

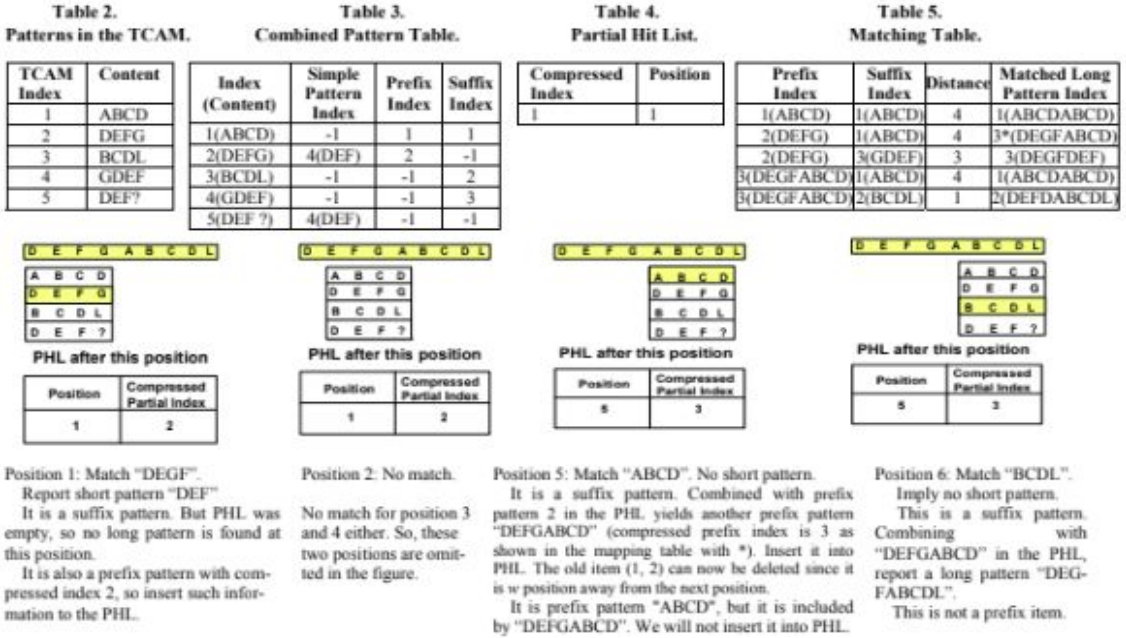


Table 2. Patterns in the TCAM.

TCAM Index	Content
1	ABCD
2	DEFG
3	BCDL
4	GDEF
5	DEF?

Table 3. Combined Pattern Table.

Index (Content)	Simple Pattern Index	Prefix Index	Suffix Index
1(ABCD)	-1	1	1
2(DEFG)	4(DEF)	2	-1
3(BCDL)	-1	-1	2
4(GDEF)	-1	-1	3
5(DEF ?)	4(DEF)	-1	-1

Table 4. Partial Hit List.

Compressed Index	Position
1	1

Table 5. Matching Table.

Prefix Index	Suffix Index	Distance	Matched Long Pattern Index
1(ABCD)	1(ABCD)	4	1(ABCDABCD)
2(DEFG)	1(ABCD)	4	3*(DEGFABCD)
2(DEFG)	3(GDEF)	3	3(DEGFDEF)
3(DEGFABCD)	1(ABCD)	4	1(ABCDABCD)
3(DEGFABCD)	2(BCDL)	1	2(DEFDABCDL)

Position 1: Match “DEGF”.
Report short pattern “DEF”
It is a suffix pattern. But PHL was empty, so no long pattern is found at this position.
It is also a prefix pattern with compressed index 2, so insert such information to the PHL.

Position 2: No match.
No match for position 3 and 4 either. So, these two positions are omitted in the figure.

Position 5: Match “ABCD”. No short pattern.
It is a suffix pattern. Combined with prefix pattern 2 in the PHL yields another prefix pattern “DEFGABCD” (compressed prefix index is 3 as shown in the mapping table with *). Insert it into PHL. The old item (1, 2) can now be deleted since it is *w* position away from the next position.
It is prefix pattern “ABCD”, but it is included by “DEFGABCD”. We will not insert it into PHL.

Position 6: Match “BCDL”.
Imply no short pattern.
This is a suffix pattern. Combining with “DEFGABCD” in the PHL, report a long pattern “DEGFABCDL”.
This is not a prefix item.

Figure 4. An Example of Matching Long Patterns in an Input String “DEFGABCDL”.

Análisis del esquema propuesto

- Impacto del ancho de la TCAM (w) en el esquema.
  - Capacidad de las tablas.
  - Probabilidad de aciertos.
- Impacto de las búsquedas de memoria en la tasa de exploración del sistema.
  - TCAM.
  - SRAM.
  - 2 Gbps

TCAM Size	Matching Table Size	TCAM Hit Rate	PHL Size
$w * \sum \lceil m_i / w \rceil$	$w * (\sum_i (\lceil m_i / w \rceil - 1))^2$	$\frac{\sum_i (\lceil m_i / w \rceil - 1)}{(2^8)^w}$	$w * \frac{\sum_i (\lceil m_i / w \rceil - 1)}{(2^8)^w}$

Simulación de resultados con ClamAV

- Patrones simples.
- Conjunto de seguimiento de paquetes.
  - MIT DARPA.
  - Berkeley.
- TCAM
  - w = 128 bytes
  - Size = 240 KB

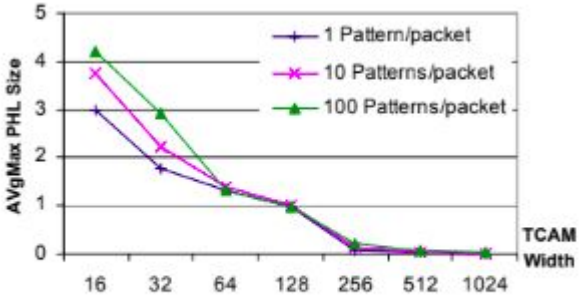


Figure 10. *AvgMax* PHL Size.

TCAM Width	MIT Dump			Berkeley Dump		
	Avg	*AvgMax*	*Max*	*Avg*	*AvgMax*	*Max*
4	0.042	0.27	4	0.03	0.48	4
8	4.8e-6	5.6e-4	8	1.e-6	1.9e-5	7
16	0	0	0	4.3e-7	5.8e-6	3
32	0	0	0	0	0	0
64	0	0	0	0	0	0
128	0	0	0	0	0	0

Table 6. PHL Size for ClamAV Signature Set.

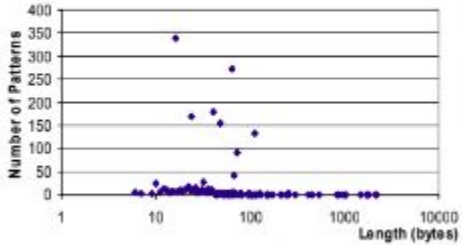


Figure 7. Distribution of Pattern Length

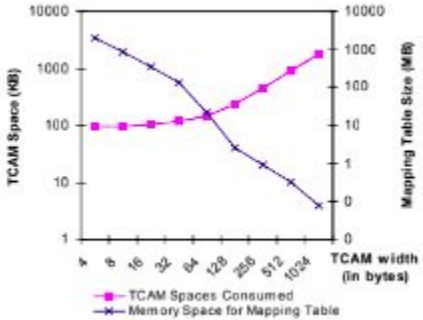


Figure 8. Impact of TCAM Width

Simulación de resultados con SNORT

- Patrones simples y compuesto
- Conjunto de seguimiento de paquetes.
  - MIT DARPA.
  - Berkeley.
- TCAM
  - w = 128 bytes
  - Size = 295 KB

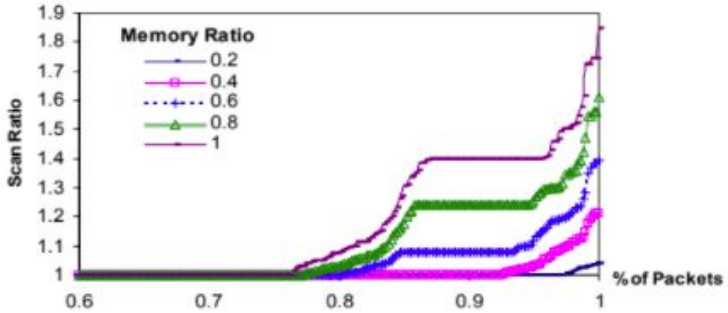


Figure 12. Effects of Memory Ratio on Scan Rate

Table 7. PHL Size for SNORT Signature Set

Window Size	MIT Dump			Berkeley Dump		
	Avg	AvgMax	Max	Avg	AvgMax	Max
20	0.5523	2.7683	8	0.4702	1.5765	12
40	0.9881	3.5376	14	0.6500	1.8661	18
60	1.3151	3.9960	14	0.7313	1.9652	23
80	1.5491	4.2158	16	0.7587	2.0373	24
100	1.6867	4.3485	18	0.7661	2.0740	25
120	1.7725	4.4475	18	0.7669	2.0768	25
140	1.8308	4.5722	19	0.7669	2.0768	25
160	1.8800	4.6643	19	0.7669	2.0768	25
180	1.9244	4.7386	19	0.7669	2.0768	25
200	1.9662	4.8079	20	0.7669	2.0768	25

Conclusión

- Mecanismo de protección de la red.
- Escanea miles de patrones de forma simultánea.
- Alta velocidad.
- Capacidad de aceleración a tasas de varios gigabits.