김일성종합대학학보
(자연과학)
주체104(2015)년 제61권 제12호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 61 No. 12 JUCHE104(2015).

FPGA에 기초한 Snort패턴정합체계의 연구

허철만, 박성호

콤퓨터망침입검출체계(NIDS)는 콤퓨터망보안체계에서 중요한 부분으로 되고있다. 콤퓨터망에서 공격자들이 자동공격도구를 비롯한 여러가지 도구와 방법들을 리용하고있으므로 보안사고는 나날이 급속히 늘어나고있다.[1] 그리고 콤퓨터망통과량이 콤퓨터체계의 성능을 초과하므로 NIDS에 병목현상을 일으키고있다.[2] 한편 현재 리용되고있는 NIDS는 100M망에 적당하다. 그러나 최근시기에 1G망이 널리 리용되고 10G망도 개발되고있으므로 콤퓨터망통과량과 NIDS처리속도사이의 불일치가 존재한다. 따라서 콤퓨터망보안체계의 성능을 개선하기 위한 장치적방법에 대한 여러가지 연구가 진행되고있다.

론문에서는 NIDS에서의 패턴정합을 위한 장치적인 방법 즉 XOR하쉬방법과 이것을 리용한 Snort패턴정합체계를 제안하였다.

1. XOR하쉬방법

Snort는 경량급의 NIDS로서 프로그람적인 방법으로 콤퓨터망의 파케트를 잡고 해석하며 침입행위를 검출한다. Snort침입검출체계에서 계산량이 제일 많이 요구되는 부분은 content에 있는 패턴을 정합하는 부분이며 이것은 전체 계산량의 60%이상을 차지한다. 그런데 쏘프트웨어적인 패턴정합산법은 보안체계가 요구하는 속도를 보장할수 없다. 따라서 우리는 장치적인 XOR하쉬방법에 의한 패턴정합방법을 제기한다.

하쉬방법에서 하쉬함수의 선택은 체계의 성능에 매우 큰 영향을 준다. 장치적실현에 적당한 하쉬함수(XOR하쉬함수)는 다음과 같다.

$$h_i(X)=d_{i0}\cdot x_0 \oplus d_{i1}\cdot x_1 \oplus d_{i2}\cdot x_2 \oplus \cdots \oplus d_{i\ n-1}\cdot x_{n-1}$$

여기서 d_{ij}는 우연수값들이다. $n$bit문자렬 $x_0, x_1, \cdots, x_{n-1}$은 열쇠값이다.

이때 하쉬처리는 d_{ij}와 x_j의 비트적인 론리적과 배타적론리합에 의하여 진행된다. 이것은 x_j의 비트값과 패턴에서의 위치에 의하여 결정된다.

식 (1)을 XOR하쉬함수라고 부른다.

이러한 XOR하쉬함수를 적용한 방법의 우점은 장치적으로 쉽게 실현된다는것이다.

XOR하쉬법을 리용한 체계는 크게 자료의 수집, 자료에 대한 16B 패턴정합처리, 결과처리로 이루어지며 그 과정은 그림과 같다.

그림에서 자료수집과 결과처리모듈은 쏘프트웨어적인 방법으로 처리되며 패턴정합의 기능만이 FPGA에 의하여 처리된다.

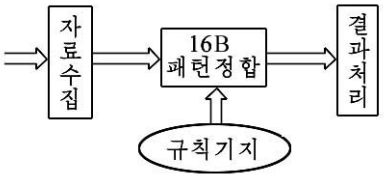

그림. 체계의 동작흐름

2. 패턴정합체계의 실현

XOR하쉬방법을 리용하여 패턴정합체계실현과정은 다음과 같다.

① 배타적론리합연산을 리용하여 주소를 계산한다.

② 얻어진 주소를 리용하여 패턴을 얻는다.

③ 입력문자렬을 패턴과 비교하고 정합결과를 출력한다.

XOR하쉬방법은 하쉬함수에 관하여 복잡한 계산을 포함한다. 그러므로 이 부분은 주문제작IP를 가지고 실현한다.

한편 패턴정합에 대한 모든 조작이 FPGA에 기초하여 실현된다면 많은 자원이 소비되고 정합속도가 떨어진다. 따라서 16B보다 큰 패턴은 PC에서 처리하게 설계하였다.

다른 한편 패턴정합체계에서 내부등록기는 data_cal, data_buf, result, irq이다. 여기서 등록기 data_cal의 길이는 16Byte로서 여기에는 패턴정합을 위한 문자렬을 보관한다. 그리고 등록기 data_buf에는 Nios II로부터 새로 입력되는 자료가 기억된다. 또한 등록기 result에는 패턴정합의 결과가, 등록기 irq에는 중단신호가 기억된다.

XOR하쉬함수를 리용할 때 하쉬충돌이 반드시 일어나는데 이것은 패턴정합 IP로 처리한다.

3. 실 험 결 과

체계가 리용한 Snort IDS가 실행되는 콤퓨터의 장치적조건은 Intel(R) Pentium 4 CPU 1.7GHz이고 기억기는 256MB이다.

실험결과는 표와 같다.

표. FPGA와 하쉬방법을 리용한 체계의 대비검사표

방법	장치	주파수/MHz	문자수	론리문수	기억크기/Kbit	론리문수/문자	기억/문자	통과량/Gbps	성능효과무게
XOR Hash	EP2C70F896C6N	130	30 927	3 451	1 075.2	0.111	35.06	1.29	2.674
XOR Hash	EP2C70F896C6N	130	60 927	3 451	1 075.2	0.057	18.07	1.29	5.267
FPGA-based Cuckoo Hashing	XC2VP20 XC2V3 000	272 223	68 266	3 028 3 028	1 116	0.044 0.044	16.74	2.18 1.78	9.966 8.137
V-HashMem	XC2V30	306	33 613	2 084	702	0.060	21.39	2.45	8.635
HashMem	XC2V1 000 XC2VP70	250 338	18 636	2 570 2 570	630	0.140	34.62	2.00 2.70	4.012 5.416
PH-Mem	XC2V1 000	263	20 911	6 272	288	0.300	14.10	2.11	4.721
ROM+Coproc	XC4VLX15	260	32 384	8 480	276	0.260	8.73	2.08	5.896

여러가지 알고리듬에 관한 비교결과는 장치적방법에 의한 처리속도가 쏘프트웨어적인 방법에 비하여 35배 더 빠르다는것을 보여준다.

맺 는 말

FPGA에 기초한 NIDS체계를 제기하고 설계하였다. 설계한 패턴정합체계는 콤퓨터망 보안체계의 요구를 만족시킨다는것을 보여준다.

참 고 문 헌

[1] S. Tomiyama et al.; Field-Programmable Technology, 12, 121, 2007.

[2] Janardhan Singaraju et al.; Microprocessors and Microsystems, 32, 210, 2008.

주체104(2015)년 8월 5일 원고접수

Research of Snort Pattern Matching System based on FPGA

Ho Chol Man, *Pak Song Ho*

This paper presents a pattern matching system based on FPGA. This paper uses Snort rule and XOR hash function to match pattern. Experimental results show that the system can quickly adapt to the demand for hardware reconfiguration and meet the network application requirements.

Key words: pattern matching, intrusion detection, FPGA, Snort, XOR hash