



Research Article



## **Substantial Overall Performance Pattern-matching Algorithm for Network Stability**

Shoban Babu Sriramoju

**Corresponding Author:**

babuack@yahoo.com

**DOI:**

<http://doi.org/>

10.5281/zenodo.13348198

**Manuscript:**

Received: 15<sup>th</sup> Jan, 2018

Accepted: 7<sup>th</sup> Feb, 2018

Published: 25<sup>th</sup> Mar, 2018

**Publisher:**

Advaita Innovative Research

Association

<http://www.airaacademy.com/>

**ABSTRACT**

The rise in network traffic and speed can create present calculations to eventually turn into performance bottle neck. Because of this, it's quite required to build up speedier and a lot more successful pattern fitting calculations as a way to conquer the difficulties in your operation. The algorithm along with its particular functioning approach are clarified at length. Using a brand new notion of benchmark purpose a two- dimensional selection redesigned predicated on publication established rules from the preprocessing stage, Verify the algorithm a much improved performance and also much more successful.

**Keywords:** Network security, Network intrusion detection.

Project Manager, Ken Excel Software Private Limited, Warangal, India.

**IJRA - Year of 2018 Transactions:**

Month: January - March

Volume – 5, Issue – 17, Page No's:701-704

Subject Stream: Computers

**Paper Communication:** Author Direct

**Paper Reference Id:** IJRA-2018: 5(17)701-704



## Substantial overall performance Pattern-matching algorithm for Network Stability

Shoban Babu Sriramoju

Project Manager, Ken Excel Software Private Limited, Warangal, India.

### ABSTRACT

The rise in network traffic and speed can create present calculations to eventually turn into performance bottle neck. Because of this, it's quite required to build up speedier and a lot more successful pattern fitting calculations as a way to conquer the difficulties in your operation. The algorithm along with its particular functioning approach are clarified at length. Using a brand new notion of benchmark purpose a two- dimensional selection re designed predicated on publication established rules from the preprocessing stage, Verify the algorithm a much improved performance and also much more successful.

**Keywords:** network security, network intrusion detection.

### 1. INTRODUCTION

Network security applications such as firewall, Network Intrusion Detection Systems (NIDS), virus scan software, anti-spam software, are endeavored to detect such attempts by monitoring incoming traffic for suspicious contents. They use a set of signatures (or rules) and report offending packets to the administrators for further actions. Since firewall and quality-of-service (Qos) applications examine multiple fields in the packet header, many firewall rules only have to check roughly 128 bits within the first 40 bytes of a packet header.

On the other hand, signature- based NIDSs, such as Snort [8] and Bro [9], identify threat by testing network packets against rules that specify conditions for both the packet header and content. These applications often rely on pattern matching techniques.

While the pattern matching algorithms are applied to network security, such NIDSs, the speed of pattern matching usually becomes a bottleneck. Previous research results suggest that in the performance of NIDSs, 30% of total processing time is spent

on pattern matching [1], especially in the cases like Web-intensive traffic, this percentage raises up to 80% [2]. The increase in network speed from Mbps to Gbps poses new challenges to technology presses forward, Gigabit and 10 Gigabit Ethernet is becoming a popular network environment. Most of the existing algorithms are not suitable for new generations of network security applications.

In order to protect such environment, one of approach is to improve the performance of signatures detection engine by increasing the efficiency of pattern matching algorithm.

The rest of the paper is organized as follows. Section 2 is contributed to the characterization of the place of pattern matching in network security such as NIDS and discussion relevant prior works in pattern matching algorithm. We discuss our new algorithm in Section 3. Evaluation of the results of our techniques can be found in Section 4. Our contributions are summarized in Section 5.

## 2. NEW PATTERN MATCHING ALGORITHM

A new pattern matching algorithm is presented here. Core part of the algorithm is described briefly as followings.

### *Pattern Matching Algorithm*

Begin

```

1. for (each char1  $\Sigma$ ) do
2.   for(each char2  $\Sigma$ ) do
next[char1,char2]←m+2;
3.   for (each char1  $\Sigma$ ) do
next[char1,pattern[0]]←m+1;
4.   for (i=0 to m-2) do
next[pattern[i],pattern[i+1]]←m-i;
5.   j←0;
6.   while (j≤n) do begin
8.     i←m-1;
9.     while(i>=0 and pattern[i]=text[i+j]) do i←i-1;
10.    if (i<0) then output(match at location j);
11.    if (text[j+m-1,j+m]=pattern[m-2,m-1]) then
j←j+1;
12.  else j←j+next[text[j+m],text[j+m+1]];
13.  end while
14. End

```

## 3. PATTERN RECOGNITION SYSTEM

The anomaly intrusion detection system experiences high false alarm rates while the abuse intrusion detection system needs generalization capacities and can't identify new attack writes. Pattern Recognition strategies have been found to strike a fine adjust in this exchange off. The utilization of pattern recognition and classification has developed in the previous couple of years. The unpredictability of the classification systems and their expanded accessibility has made them more available.

They can channel commotion and concentrate highlights from movement to encourage classification. Pattern classification is a progression of steps, beginning with the information, moving to segmentation, data extraction and translation and at last classification. After the classification, cost components can be added to build the intensity of the decision to act. All together for pattern recognition to be valuable in network security, two huge issues must be tended to; Data extraction and classification. Information from a solitary bundle is lacking for include extraction

Ordering various bundles may give a premise to depicting highlights yet what number of parcels are sufficient and how would we orchestrate the data from numerous parcels to make it helpful for data extraction.

The point of pattern classification is to use the information gained from pattern investigation to train the computer keeping in mind the end goal to achieve the classification. The progression of classification is the piece of the pattern recognition system.

The subsequent stage following Data extraction is classification. It is the way toward utilizing the data set to order the activity as ordinary or ill-conceived movement. The classifications can be isolated into three classifications: typical, Denial of Service and Scan. Numerical qualities were doled out the three classifications in view of their likelihood. Four sorts of classifiers are utilized: Bayesian, Feed Forward with Back propagation, ART2 and Kohonen neural networks.

## 4. CONCLUSIONS

We presented a novel pattern matching algorithm and evaluated its performance by using diverse text strings and various set of pattern strings. The testing results of English text and network traffic show an

improvement of 24% ~31% in average comparing to the case of BM algorithm.

The new algorithm is a variant of BM algorithm and has been greatly improved. A two-dimensional array in the preprocessing phase is redesigned. The concept of reference point, makes the algorithm to have better performance and more efficient. It provides another option for network security applications, not only for Intrusion Detection System, but also for other security applications such as virus scanning, firewalls, and layer seven switches.

## REFERENCES

- 1) Zhou Chunyue, Liu Yun, Zhang Hongke, "A Pattern Matching Based Network Intrusion Detection System", 1-4244-0342-1/06/2006 IEEE.
- 2) Chi-Ho Tsang, Sam Kwong, Hanli Wang, Genetic-fuzzy administer mining approach and evaluation of highlight selection systems for anomaly intrusion detection. The diary of Pattern Recognition 40 (2007).
- 3) Shai Rubin, Somesh Jha, Barton Miller, "Protomatching Network Traffic for High Throughput Network Intrusion Detection", CCS'06, Oct 30-Nov 3, 2006, Alexandria, Virginia, USA.
- 4) Monther Aldwairi, conte, and Paul Franzon, "Configurable String Matching Hardware for Speeding up Intrusion Detection, ACM SIGARCH Computer Architecture News, Vol. 33, No. 1, March 2005.
- 5) Animesh Patcha, Jung-Min Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and most recent Technological Trends", Computer Networks 51 (2007).
- 6) Zachary K. Pastry specialist and Viktor K. Prasanna, High-throughput Linked-Pattern Matching for Intrusion Detection Systems, ANCS'05, Oct 26-28, 2005, Princeton, New Jersey, USA.
- 7) Dit-Yan Yeung, Yuxin Ding, Host-based Intrusion Detection utilizing Dynamic and Static Behavioral Models, The diary of Pattern Recognition 36 (2003).
- 8) Wu Yang, Bin-Xing Fang, Bo Liu, hong-li Zhang, Intrusion Detection System for High-Speed Network, Computer Communications 27 (2004).
- 9) Zachary Baker, V.K. Prasanna, Time and Area Efficient Pattern Matching on FPGAs, FPGA'04, Feb 22-24, 2004, Monterey, California, USA.
- 10) Christopher Kruegel, Giovanni Vigna, William Robertson, A Multi-Model Approach to the Detection of Web-Based Attacks, Computer Networks 48 (2005).
- 11) Shoban Babu Sriramoju, Naveen Kumar Rangaraju, Dr .A. Govardhan, "An improvement to the Role of the Wireless Sensors in Internet of Things" in "International Journal of Pure and Applied Mathematics", Volume 118, No. 24, 2018, ISSN: 1314-3395 (on-line version), url: <http://www.acadpubl.eu/hub/>.
- 12) Shoban Babu Sriramoju, "Analysis and Comparison of Anonymous Techniques for Privacy Preserving in Big Data" in "International Journal of Advanced Research in Computer and Communication Engineering", Vol 6, Issue 12, December 2017, DOI:10.17148/IJARCCCE.2017.6121[ISSN

- (online) : 2278-1021, ISSN(print) : 2319-5940].
- 13) Shoban Babu Sriramoju, " Review on Big Data and Mining Algorithm" in "International Journal for Research in Applied Science and Engineering Technology", Volume-5, Issue-XI, November 2017, 1238-1243 [ ISSN : 2321-9653], www.ijraset.com.
- 14) Shoban Babu Sriramoju, "OPPORTUNITIES AND SECURITY IMPLICATIONS OF BIG DATA MINING" in "International Journal of Research in Science and Engineering", Vol 3, Issue 6, Nov-Dec 2017 [ISSN: 2394-8299].
- 15) Yeshwanth Rao Bhandayker, "Artificial Intelligence and Big Data for Computer Cyber Security Systems" in "Journal of Advances in Science and Technology", Vol. 12, Issue No. 24, November-2016 [ISSN: 2230-9659].
- 16) Sugandhi Maheshwaram, "A Comprehensive Review on the Implementation of Big Data Solutions" in "International Journal of Information Technology and Management", Vol. XI, Issue No. XVII, November-2016 [ISSN: 2249-4510].
- 17) Sugandhi Maheshwaram, "An Overview of Open Research Issues in Big Data Analytics" in "Journal of Advances in Science and Technology", Vol. 14, Issue No. 2, September-2017 [ISSN: 2230-9659].
- 18) Yeshwanth Rao Bhandayker, "Security Mechanisms for Providing Security to the Network" in "International Journal of Information Technology and Management", Vol. 12, Issue No. 1, February-2017, [ISSN: 2249-4510].
- 19) Sriramoju Ajay Babu, Dr. S. Shoban Babu, "Improving Quality of Content Based Image Retrieval with Graph Based Ranking" in "International Journal of Research and Applications", Volume 1, Issue 1, Jan - Mar 2014 [ISSN: 2349-0020].
- 20) Dr. Shoban Babu Sriramoju, Ramesh Gadde, "A Ranking Model Framework for Multiple Vertical Search Domains" in "International Journal of Research and Applications" Vol 1, Issue 1, Jan-Mar 2014 [ISSN: 2349-0020].
- 21) Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, "Risk-Aware Response Answer for Mitigating Painter Routing Attacks" in "International Journal of Information Technology and Management", Volume VI, Issue I, Feb 2014 [ ISSN : 2249-4510 ].