STRING MATCHING APPLICATION FOR NETWORK SECURITY

Jamuna Bhandari
jamuna.bhandari@muj.manipal.edu

Anil Kumar
anil.kumar@jaipur.manipal.edu
Department of computer science and Engineering
Manipal University Jaipur

Abstract - String matching is one of the key of network security, biological applications and many areas are benefited from a faster string matching algorithm. The effectiveness and efficiency of string matching algorithms is important for applications like as network intrusion detection systems, virus detection, medical science and web content filters system. This paper reviews what works has been done in the field of security on the bases of string matching and their performance under various situations. Also discusses the characteristics of string matching algorithms, highlights their application on network content security and research areas on string matching.

Keywords*:* String matching, Network security, patterns, text, DFA(Deterministic Finite Automata), Deep Packet Inspection, signature.

I. INTRODUCTION

Online applications are increasing very rapidly; the network security arises as big issue to be discussed. String matching is a key concept for computer applications. Whenever we talk about the detection of intrusion, suspected information or some keywords passing over network we need to match them or search them for many security purpose. This task is done by string matching algorithms and this algorithm should be fast and effective, so that any kind of attack can be prevented or detected before reach to receiving end its destination.

String searching algorithms called string matching algorithms that try to find a place where one or several strings (also called patterns) are found within a larger string (Text) or information passing over network in terms of text, keywords, signatures etc. widely deployed network intrusion detection and prevention systems often use signature-based method to detect possible malicious attacks, so string matching algorithm is their basic operation. String matching has recently proven useful for deep packet inspection to detect intrusions in networks, scan for virus's protection, and refine internet content. Many works has been done in both algorithm design and hardware implementation to speed up the inspection, minimize pattern storage space, and handle regular expressions efficiently. Along with the rapid development of network technology, demands for anti attack and security protection are now facing a drastic increase in almost all network applications and systems.

II. WORK DONE IN NETWORK SECURITY

This section discuss about the work done in the field of network security. To check network security, many algorithms has been proposed, some of them are discussed in this section.

For the low-cost hardware-based intrusion detection systems, [1] proposes a memory-efficient parallel string matching scheme. The finite state machine tiles in a string matcher adopt bit-level input symbols to reduce the number of state transitions. Long target patterns are divided into sub patterns with a fixed length; deterministic finite automata are built with the sub patterns. Using the pattern dividing, the variety of target pattern lengths can be extenuated, so that memory usage in string matchers can be efficient. Two-stage sequential matching scheme is proposed for the successive matches with sub patterns in order to identify each original long pattern being divided. Experimental results show that total memory requirements decrease on average by 47.8 percent and 62.8 percent discussed [1].

Traffic volumes of Internet are growing constantly; string matching using the Deterministic Finite Automaton will be the performance bottleneck of Deep Packet Inspection[2]. The recently proposed bit-split string matching algorithm suffers from the unnecessary state transitions problem, limiting the efficiency of deep packet inspection of network security. The root cause behind the fact that each tiny DFA of the bit-split algorithm only processes a k-bit substring of individual character input, but cannot verify whether the entire character belongs to the set of original alphabet of signature rules[3] proposes a byte-filtered string matching algorithm, where bloom filters are used to pre process each byte of every incoming packet payload to check whether the input byte belongs to the original set of alphabet or not, before process bit-split string matching. The

experimental results show that compared to the bit-split algorithm, [4]byte-filtered algorithm enormously decreases the time of string matching as well as the number of state transitions of tiny DFAs on both synthetic and real signature rule sets.

III. RESEARCH AREA

This section discusses some of research areas which are need to be enhancing periodically for better results.

The application of string matching is widely useful in many areas, based on this there are so many scopes for research in terrorist attack through cyber, medical science is also using the concept of matching for many biological analyses, huge area of online and offline library sciences already progressing in many directions, different types of anti-viruses are mostly releases on market based on their effective and faster detection nature they will prefer more by users. So many more areas can be covered by research on such matching concepts. There are large amount of variety and interesting research are still need to be adopt by researcher to extend the applications on string matching. Most important factor of string matching is its application is not limited, its requirements and improvements should be done frequently.

REFERENCES

[1] HyunJin Kim 'A Memory-Efficient Bit-Split Parallel String Matching Using Pattern Dividing for Intrusion Detection Systems' IEEE COMMUNICATIONS LETTERS, VOL. 13, NO. 12, DECEMBER 2009

[2] Prasad. R, Agarwal. S, 'A new parameterized string matching algorithm by combining bit-parallelism and suffix automata' IEEE International Conference on Computer and Information Technology, 2008.

[3] Kun Huang, Dafang Zhang 'A Byte-Filtered String Matching Algorithm for Fast Deep Packet Inspection' IEEE 9TH Young Computer Scientists, 2008. ICYCS 2008.

[4] R. Smith, S.Jha 'XFA: Faster Signature Matching with Extended Automata' IEEE Symposium on Security and Privacy (Oakland), May 2008.