ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

DNA Sequencing and Implementation of Network Intrusion Detection System

Kamesh M[1], Sandhya U [2], Sarathy D [3], Gowthami C P [4], Augustine C [5]

Assistant Professor, Department of ECE., GRT Institute of Engineering and Technology, Tiruttani, Tamilnadu, India[1,2,3,4,5]

ABSTRACT:Deoxyribonucleic acid (DNA) is a molecule that carries the genetic information of human beings. it is responsible for the growth and proper functioning of the species. By analyzing this DNA we can able to identify the diseases and genetic ailments. DNA sequencing is used to compare two given DNA strands in a much faster and effective manner. The same concept can be used to detect any security breach in a network by comparing the data with that of the trojan.

KEYWORDS:DNA, DNA Sequencing, Network intrusion detection system, Security

I. INTRODUCTION

The proliferation of Internet and networking applications, coupled with the wide-spread availability of system hacks and viruses have increased the need for network security. Firewalls have been used extensively to prevent access to systems from all but a few, well defined access points (ports), but they cannot eliminate all security threats, nor can they detect attacks when they happen. Stateful inspection firewalls are able to understand details of the protocol that are inspecting by tracking the state of a connection.

Current network security needs, require a much more efficient analysis and understanding of the application data. Content-based security threats and problems occur more frequently, in an everyday basis. Virus and worm inflections, SPAMs (unsolicited e-mails), email spoofing, and dangerous or undesirable data, get more and more annoying and cause innumerable problems. Therefore, next generation firewalls should provide deep packet Inspection capabilities, in order to provide protection from these attacks. The algorithm check the packet header and rely on pattern matching techniques and make selections based on the packet contentsand the payload. Network Intrusion Detection Systems (NIDS) implement deep packet scrutiny and scan packet's payload regarding for patterns that would indicate security threats. Matching every incoming byte, though, alongside thousands of pattern characters at wide rates is a complicated task.

The same pattern matching can be used to compare the given DNA sequences and find out the resemblances between them. These resemblances can be used to identify any sickness in person or if he is disease prone in future. Also it can be used for security purposes.

II. RELATED WORK

Protein comparison is gaining importance year after year since it has been demonstrated that biologists can find correlation between different species, or genetic mutations that can lead to cancer and genetic diseases. Protein sequence alignment is the most computational intensive task when performing protein comparison. It is possible to apply a technique called pipeline interleaving to increase the throughput of loop-based SAs. Pipeline interleaving has been explored especially in the case of digital filters; here, we introduce this method for SAs, which has never been proposed before. This requires an analysis and redesigns procedure of each PE, but also a careful retiming of inputs to guarantee synchronization between the neighboring PEs. The SA that implements a protein alignment algorithm, presented in is used as case study to show benefits in terms of increased frequency and dynamic power saved.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

Network Intrusion Detection Systems (NIDS) attempt to detect attacks by monitoring incoming traffic for suspicious contents. They collect data from network, monitor activity across network, analyze packets, and report any intrusive behavior in an automated fashion. Intrusion detection systems use advanced pattern matching techniqueson network packets to identify known attacks. They use simple rules (or search patterns) to identify possible security threats, much like virus detection software, and report offending packets to the administrators for further actions. NIDSs should be updated frequently, since new signatures may be added or others may change on a weekly basis.

NIDS rules usually refer to the header as well as to the payload of a packet. Header rules check for equality (or range) in numerical fields and are straightforward to implement. More computationally-intensive is the text search of the packet payload against hundreds of patterns that must be performed at wire-speed.

III. PROPOSED WORK

Software-based Intrusion Detection Systems can only support modest throughput. On the other hand, hardware can easily adapt in NIDS application needs, achieving better performance with reasonable cost. Here, we investigate various hardware-based solutions for string matching. Several companies such as Cisco, Net Screen and PMC-Sierra produce firewalls, or else called ASIC security programmable co-processors. Additionally, much work has been done in FPGA-based string matching for NIDS, since FPGAs give the advantage of reconfiguration. All these ASIC and FPGA-based approaches offer much better performance as compared to software solutions.

Other than Pattern matching “algorithm” decision, there are a lot of other issues that also needs to consider before choosing any one of them. Fast matching is the normal need for the decision but there are some other issues to be kept in mind like combating false positives example in some cases it is possible that payload contains a pattern for buffer overflow attack via telnet application protocol but what if there was no active telnet session between two hosts. Some of issues with respect to choice of algorithm and limitations of signature matching have been stated below.

- Memory vs. Speed
- Signature format
- Session-Based and Application Level Signature Matching

Two are the main concepts that characterize SAs: local transmission of data (i.e., there are not global signals except from the clock) and parallel computation (i.e., all PEs work in the same way on different data). SAs can have different shapes: for example, PEs can be arranged in a bi dimensional matrix-like shape, as is shown in Fig. 1(a), they can be linear, as in Fig.1(b), or even have strange shapes as hexagonal, or as in Fig. 1, with signals flowing in three different directions. In general, an array processor is designed, as explained in [7], starting from the algorithm description of the problem and executing three steps: 1) dependence graph (DG) design, which consists in obtaining a graphical representation of an algorithm, where nodes represent computations and edges represent data dependencies; 2) signal flow graph (SFG) derivation, which consists in shrinking the DG along one axis.

Subsequently, an SFG has a dimensionless than the correspondent DG; this is because in a DG each node represents one simple computation, while in the SFG a node is a processing unit, that should be reused in successive time steps, and for this reason nodes of a line in a DG can be mapped to a single node in the SFG; and 3) array processor design, that consists in designing the internal structure of each PE.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

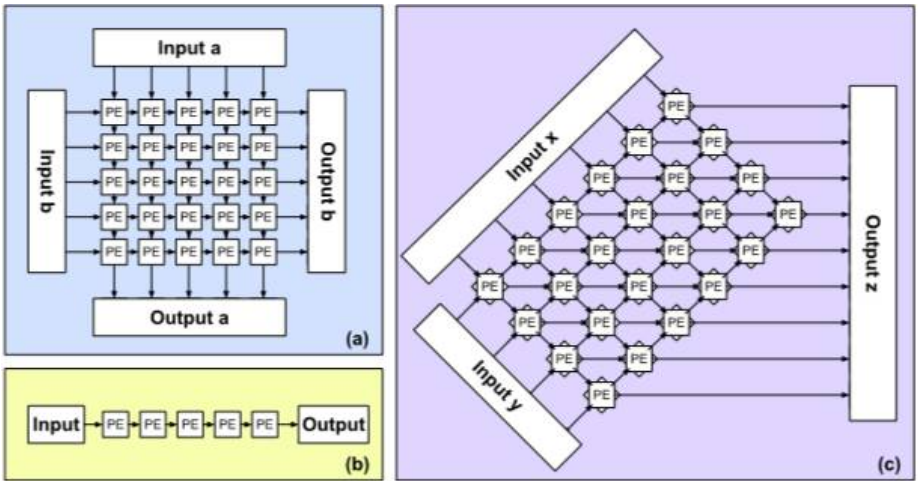

Fig.1. Systolic Array

In this paper we introduce concept of interleaving to SAs that has been never proposed. To do so, we first introduce a taxonomy of SAs and we explain how interleaving is provided at PE-level and how the concept can be extended to the whole SA. SAs can be divided into two main classes: those cells that have an WIL, and those Without internal loop; the former can be further split in SAs that store results in the cells and SAs where the partial result is passed through the cells to obtain the final value (WIL-PT). The DGS S-W SA belongs to this last class.

Given the processing bandwidth limits of General purpose processors (GPP), which can assist only a few hundred Mbps throughput, H/W-based NIDS (ASIC or FPGA) is an smart alternative solution. Many ASIC intrusion detection systems usually store their rules via large memory blocks, and examine incoming packets in integrated processing engines. Generally, ASICs programmable security co-processors are expensive, complicated, and although they can support higher throughput compared to GPP, they do not achieve impressive performance. The memory blocks that store the NIDS rules are re-loaded, whenever an updated rule-set is available. The most common technique for pattern matching in ASIC intrusion detection systems is the use of regular expressions. Updating the rule-set is not a trivial procedure, since the system must be able to support a variation of rules, with sometimes complex syntax, and special features. On the other hand, FPGAs are more suitable, because they are reconfigurable they provide H/W speed and exploit parallelism.

IV. EXPERIMENTAL RESULTS

The simulation studies involve the overall working which has been given in fig.2. The Sequencing method compares the first set of coordinates with the library file. If the first set of coordinates matches then only it moves on to next set of coordinates for comparison, else the DNA sequence does not match and the process stops. The same technique is used for detection of trojan virus. The modelSim Simulation report is given in fig 3. The area utilization report and power dissipation report is given in figure 4 and figure 5 respectively. The number of logic elements taken to implement the given concept can be reduced in a significant manner. The power dissipation is also less compared to the existing methods.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

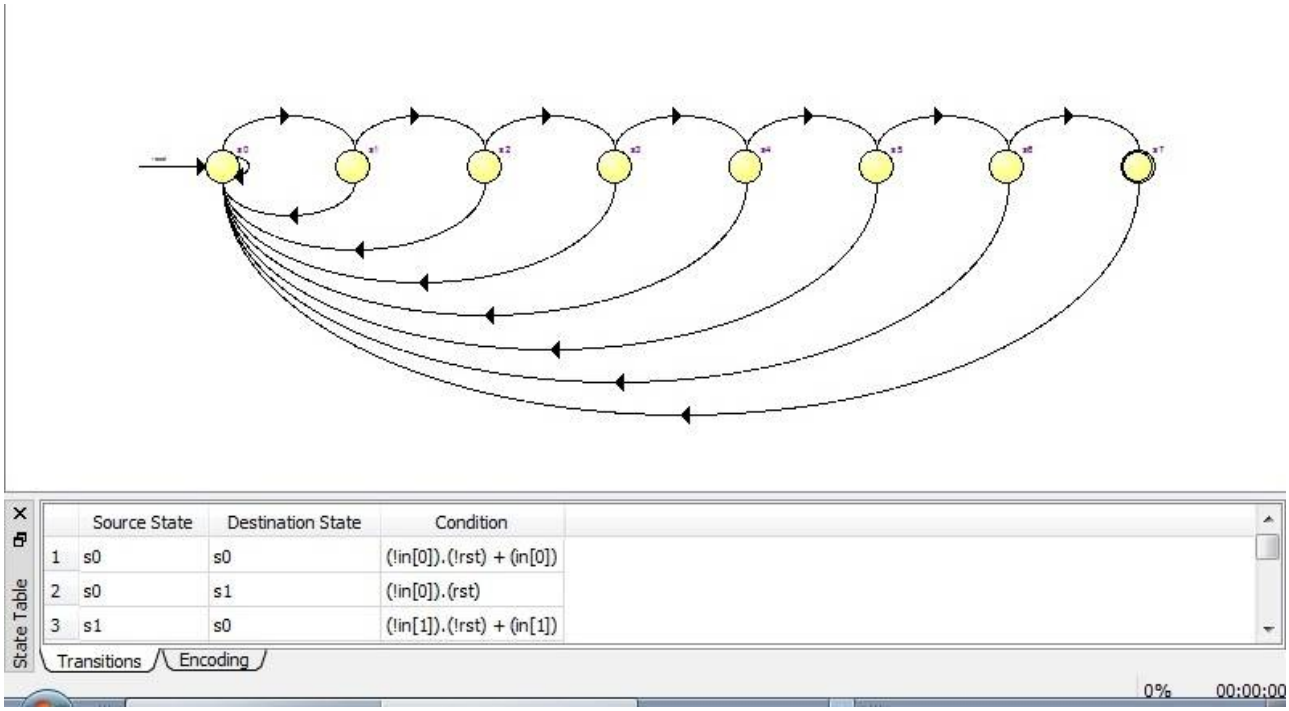

Fig.2 State Machine Report

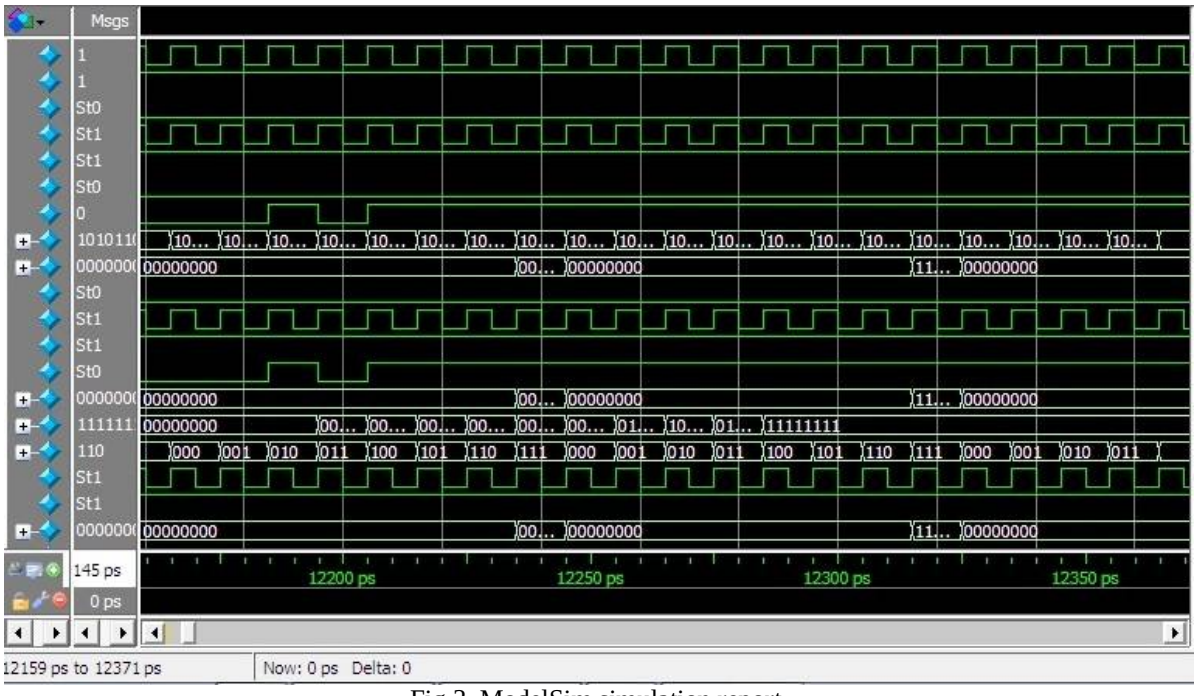

Fig.3. ModelSim simulation report

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

Flow Summary	
Flow Status	Successful - Thu Apr 12 00:02:57 2012
Quartus II Version	11.0 Build 208 07/03/2011 SP 1 SJ Web Edition
Revision Name	shorttop
Top-level Entity Name	longtop
Family	Cyclone III
Total logic elements	90 / 5,136 (2 %)
Total combinational functions	83 / 5,136 (2 %)
Dedicated logic registers	75 / 5,136 (1 %)
Total registers	75
Total pins	3 / 183 (2 %)
Total virtual pins	0
Total memory bits	0 / 423,936 (0 %)
Embedded Multiplier 9-bit elements	0 / 46 (0 %)
Total PLLs	0 / 2 (0 %)
Device	EP3C5F256C6
Timing Models	Final

Fig.4. Area Utilization Report

PowerPlay Power Analyzer Summary	
PowerPlay Power Analyzer Status	Successful - Thu Apr 12 00:03:59 2012
Quartus II Version	11.0 Build 208 07/03/2011 SP 1 SJ Web Edition
Revision Name	shorttop
Top-level Entity Name	longtop
Family	Cyclone III
Device	EP3C5F256C6
Power Models	Final
Total Thermal Power Dissipation	55.27 mW
Core Dynamic Thermal Power Dissipation	0.00 mW
Core Static Thermal Power Dissipation	46.12 mW
I/O Thermal Power Dissipation	9.16 mW
Power Estimation Confidence	Low: user provided insufficient toggle rate data

Fig. 5. Power Dissipation Report

V. CONCLUSION

The proposed DFA parallel string matching scheme minimizes total memory requirements. The problem of various pattern lengths can be solved by dividing long target patterns into sub-patterns with a fixed length. The memory-efficient bit-split FSM architectures can lessen the total memory requirements. Thus NIDS uses reduced memory requirements for the real rule sets, and it is concluded that the proposed string matching scheme is useful for reducing total memory requirements of parallel string matching engines.

REFERENCES

[1] P.-C. Lin, Y.-D. Lin, T.-H. Lee, and Y.-C. Lai, "Using String Matching for Deep Packet Inspection," IEEE Computer, vol. 41, no. 4, pp. 23-28, Apr. 2008.
[2] C.-H. Lin, Y.-T. Tai, and S.-C. Chang, "Optimization of Pattern Matching Algorithm for Memory Based Architecture," Proc. Third ACM/IEEE Symp. Architecture for Networking and Comm. Systems, pp. 11-16, 2007.
[3] Virtex-4 FPGA User Guide, http://www.xilinx.com/support/ documentation/user_guides/ug070.pdf., 2011.
[4] F. Yu, Z. Chen, Y. Diao, T.V. Lakshman, and R.H. Katz, "Fast and Memory-Efficient Regular Expression Matching for Deep Packet Inspection," Proc. Second ACM/IEEE Symp. Architecture for Networking and Comm. Systems, pp. 93-102, 2006.
[5] A.V. Aho and M.J. Corasick, "Efficient String Matching: An Aid to Bibliographic Search," Comm. ACM, vol. 18, no 6, pp. 333-340, 1975.
[6] H. Kim, H. Hong, H.-S. Kim, and S. Kang, "A Memory-Efficient Parallel String Matching for Intrusion Detection Systems," IEEE Comm. Letters, vol. 13, no. 12, pp. 1004-1006, Dec. 2009.
[7] L. Tan and T. Sherwood, "A High Throughput String Matching Architecture for Intrusion Detection and Prevention," Proc. 32nd IEEE/ACM Int'l Symp. Computer Architecture, pp. 112-122, 2005.
[8] L. Tan, B. Brotherton, and T. Sherwood, "Bit-Split String-Matching Engines for Intrusion Detection and Prevention," ACM Trans. Architecture and Code Optimization, vol. 3, no. 1, pp. 3-34, Mar. 2006.
[9] J. Bispo et al., "Regular Expression Matching for ReconfigurablePacket Inspection," Proc. IEEE Int'l Conf. Field-Programmable Technology (FPT 06), IEEE Press, 2006, pp.119-126.
[10] R. Sommer and V. Paxson, "Enhancing Byte-Level NetworkIntrusion Detection Signatures with Context," Proc. ACMComputer and Comm. Security (CCS 03), ACM Press, 2003,pp. 262-271.
[11] V. Paxson et al., "Rethinking Hardware Support for NetworkAnalysis and Intrusion Prevention," Proc. Usenix WorkshopHot Topics in Security, Usenix, 2006, pp. 63-68; http://imawhiner.com/csl/usenix/06hotsec/tech/paxson.html.
[12] R. Sommer and V. Paxson, "Enhancing Byte-Level NetworkIntrusion Detection Signatures with Context," Proc. ACMComputer and Comm. Security (CCS 03), ACM Press, 2003,pp. 262-271.

BIOGRAPHY

Kamesh M has received his B.E., degree in Electronics and Communication from VelTech Engineering College, Anna University, India and received his Master of Engineering in communication Systems from SSN College of Engineering , Anna University, India, in 2013. Presently he is working as an Assistant professor in GRT Institute of engineering and technology India. His research area includes wireless communication, Networking and Mobile Communications.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 6, June 2018

Sandhya U has received her B.E., degree in Electronics and Communication from Maamallan institute of technology, Anna University, India and received her Master of Engineering in communication Systems from Rajalakshmi Engineering college , Anna University, India, in 2014. Presently she is working as an Assistant professor in GRT Institute of engineering and technology India. Her research area includes wireless communication, Networking and Mobile Communications.

Sarathy D has received his B.E., degree in Electronics and Communication from VelTechhightechdr.rangarajandr.sakunthala Engineering College, Anna University, India, in 2009 and received his Master of Engineering in embedded System and technology from PSN College of Engineering and technology, Anna University, India, in 2011. Presently he is working as an Assistant professor in GRT Institute of engineering and technology India. His research area includes communication system and Mobile Communications.

Gowthami C P has received her B.E. degree in Electronics and communication from Jaya Engineering College, Anna University, India and received her Master of Engineering in Applied Electronics from Sriram Engineering College, Anna University, India, in 2013. Presently she is working as an Assistant Professor in GRT Institute of engineering and Technology India. Her area research includes wireless communication, Networking and Mobile Communications.

Augustine C has received his B.E., degree in Electronics and Communication from GTECH Engineering College, Anna University, India and received his Master of Engineering in communication engineering from VIT University, India. in 2010. Presently he is working as an Assistant professor in GRT Institute of engineering and technology India. His research interest includes wireless communication, noise reduction in mobile communications.