304. A MEMORY-EFFICIENT HARDWARE IMPLEMENTATION OF PARALLEL STRING MATCHING FOR INTRUSION DETECTION SYSTEMS

Ms. Flemin Nicklet [1], Dr. S. Prakash[2], ECE Dept, Jerusalem College of Engineering
nickijess12@gmail.com [1]

High speed and always-on network access is becoming common place around the world, creating a demand for increased network security. Network Intrusion Detection Systems (NIDS) attempt to detect and prevent attacks from the network using pattern-matching rules in a way similar to anti-virus software. For the low-cost hardware-based intrusion detection systems, this project work proposed a memory-efficient parallel string matching scheme. In order to reduce the number of state transitions, the finite state machine tiles in a string matcher adopt bit-level input symbols. 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 mitigated, so that memory usage in homogeneous string matchers can be efficient. In order to identify each original long pattern being divided, a two-stage sequential matching scheme is proposed for the successive matches with sub-patterns.

Index Terms- Network Intrusion Detection System (NIDS), Deterministic Finite Automata (DFA), Pattern matching, Pattern division.

ISBN 978-81-904760-6-5