

Contents

1. Introduction.....	1
2. Background.....	3
2.1 A Popular NIDS: Snort.....	3
2.2 Snort component- Detection Engine.....	5
2.3 Snort rule payload keyword.....	7
2.4 SOC (system on chip) platform.....	9
2.5 Multi-pattern matching algorithms.....	10
3. Pre-processor:	12
3.1 Snort content rule.....	12
3.2 Singularity of Snort Rule.....	14
3.3 Modified AC multi-pattern match.....	17
4. Post-processor.....	19
4.1 System Overview.....	19
4.2 Relation between pre/post-processor.....	20
4.3 Post-processor overview.....	20
4.4 Event Group Filter Algorithm.....	22
4.5 Event table.....	24
4.6 Rule table.....	26
4.7 Binary Correlation Match Algorithm.....	31
5. Implementation & Results.....	35
5.1 Pre-processor.....	35
5.2 Post-processor.....	36
5.3 Result.....	41
6. Conclusions.....	47
References.....	50

List of Figures

Figure 2-1. The original architecture of NIDS.....	4
Figure 2-2. The three-dimensional linked list (RTN list).....	6
Figure 2-3. The three-dimensional linked list (RTN & OTN).....	7
Figure 2-4. SoC system design flow.....	10
Figure 2-5. The example of AC tree.....	11
Figure 3-1. The growth of the Snort rule set over the last five years.....	13
Figure 3-2. Original and group-based search domain.....	16
Figure 3-3. Length distribution of the unique strings in Snort 2.3.....	17
Figure 3-4. The architecture of modified AC tree.....	18
Figure 4-1. The proposed novel NIDS architecture.....	19
Figure 4-2. The relationship between pre-processor and post-processor.....	20
Figure 4-3. The architecture of SoC-based post-processor.....	21
Figure 4-4. The flowchart of EGF algorithm.....	23
Figure 4-5. Relationship between input buffer, EGF and micro-processor.....	25
Figure 4-6. Group-based post-processor search domain.....	25
Figure 4-7. The relationship between FEL entry and EventBlock.....	26
Figure 4-8. The decision tree of rule set Table 4-4.....	26
Figure 4-9. The correlation match tree of rule set Table 4-4 (CRM)	28
Figure 4-10. The binary correlation match tree (BCRM).....	29
Figure 4-11. The relationship between CRME and memory device.....	31
Figure 4-12. The flowchart of Binary CRM algorithm.....	32
Figure 4-13. The relationship between each BCRM engine.....	34
Figure 5-1. The diagram of Cyclone (1C20)	36
Figure 5-2. The FSM of hardware-based EFG algorithm.....	38
Figure 5-3. The FSM of CRM algorithm.....	39
Figure 5-4. The logic circuit with CRME, ordering logic and Result Buffer.....	39
Figure 5-5. The SoC-based system critical diagram.....	40
Figure 5-7. The relationship between input buffer and complex rate.....	42
Figure 5-8(a). Case1 latency (ms)	42
Figure 5-8(b). Case1 latency (ms)	43
Figure 5-8(c). Case1 latency (ms)	44
Figure 5-9. Speedup: (SoC-based / Software-based)	44

List of Tables

Table 2-1. Describe all Snort components.....	3
Table 3-1. Appearing count of conditions in several Snort rule sets....	12
Table 3-2. Translate several rule to (condition, relation) form.....	14
Table 3-3. The proportion of multi-event at several Snort rule set.....	14
Table 3-4. All of the rules contain content "YMSG".....	15
Table 3-5. Application types and the corresponding first events.....	15
Table 4-1. The form of FEL entry.....	22
Table 4-2. The input and output form of EGF algorithm.	22
Table 4-3(a). The content of FEL (step 0)	23
Table 4-3(b). The content of FEL (step 1)	24
Table 4-3(c). The content of FEL (step 6)	24
Table 4-4. The example rule set.....	26
Table 4-5. Pop value of each state (CRM)	28
Table 4-6. Pop value of each state (BCRM)	29
Table 4-7. The BCM table from example Table 4-4.....	31
Table 4-8. The content of EventTable.....	32
Table 4-9(a). Binary CRM step-by-step operation.....	33
Table 4-9(b). Binary CRM step-by-step operation.....	34
Table 5-1. Memory size of modified AC.....	35
Table 5-2. Number of matching patterns.....	36
Table 5-3. The specification of development platform.....	36
Table 5-4. The latency of two solutions.....	38
Table 5-5. The resource utility rate.....	40
Table 5-6(a). Case1 latency (ms)	42
Table 5-6(b). Case1 latency (ms)	43
Table 5-6(c). Case1 latency (ms)	43
Table 5-7. Speedup: (SoC-based / SoftWare-based)	44
Table 5-8. SoC-based performance (Mbps)	45