Asian Journal of Multidisciplinary Research (AJMR) 2017

E-ISSN: 2395-1710 P-ISSN: 2395-1729
Volume 03- Issue02 -, pp-01-03

Research Paper Open Access

AN INTRUSION DETECTION SYSTEM USING INTERNET OF VEHICLE

Preethi.D[1], Poonkuzhali.P[2], Jayashree.M[3,] Vijayakumar.V[4], Dr. N. Danapaquiame[5]
[1, 2,3B]. Tech Student, Asst. Professor[4], Associate Professor[5]
Department of Computer Science and Engineering,
Sri Manakula Vinayagar Engineering College,
1preethidilipkumar2511@gmail.com, 2Kuzhali1995@gmail.com,
3jayashree27raman@gmail.com
4vijayakumarv@smvec.ac.in, n.danapaquiame@gmail.com

Abstract

Internet of Vehicles (henceforth called IoV) is a public network system andhigh-value target for intrusions that may cause efficiency issues, privacy leakages or even physical damage. Conventional intrusion detection methods are normally designed for the Internet infrastructures which cannot directly apply in the context of IoV. This work proposes an FPGA based intrusion detection method that can not only achieve real-time scanning performance but also be applied in vehicular environment. We evaluate our scheme on a how that the proposed system can achieve a throughput of more than 39 Gbps on existing FPGA platform which is about 15% higher than state-of-the-art techniques and the total power consumption for the prototype is about 7.5 w. Moreover, the processing latency of the prototype is about 4 us and is about one sixtieth part of the popular software IDS systems.

Introduction

IoV is an open and integrated network system that connects human intelligence, vehicles, things, environments and the public Internet . Although many researches that support IoV have been proposed , academic attentions paid on intrusion detection are limited. In IoV premises, each entity can communicate with others directly and share information and intelligence. Unlike the Internet, no central security devices are deployed between two communication peers, thereby each entity of IoV should be responsible for its own security. Moreover, IoV is a high-value target for intruders to exploit for the massive private and driving-aid information exchanged in it. To develop intrusion detection system for IoV, there are several facts should be considered. First, each entity in IoV should have an intrusion detection system (IDS) to protect itself. The physical size and power supply of the IDS are limited. Traditional Intrusion Detection System (IDS) do not consider those factors. Second, IoV is an intelligence-aid and real-time system. The deployment of IDS in each entity should not alleviate the real-time performance of IoV. In other word, the scanning performance and system latency of IDS for IoV should be competent enough for being deployed in real-time environment. The processing capacity of FPGA based RegEx matching system is co-determined by two factors: operating frequency and the number of bytes the system can process

every clock period. Norio Yamagaki, etc. propose a multi-stride conversion algorithm which can generate multi-stride NFAs of 2k bytes Multi-stride NFA is a variation of NFA, and it can process multiple bytes each time. The conversion of NFA into multi-stride NFA is simply done by parsing and combining transitions of NFA. Essentially, multi-stride conversion on NFA is an effective approach to promote performance and reduce latency. But the scheme suffers from the problems.

Related works

[1] Wenliang Fu," **A Practiclal Intrusion Detection System For Internet of Vehicles**", Department of Computer Science and Technology, Beijing Institute of Technology, Beijing, has proposed IoV which can achieve high performance, low latency and acceptable energy consumption. Specifically, which focus on FPGA platform, and propose a novel data model based on current multi-stride NFA.[2] YANG Fangchun,"**A Overview of Internet of Vehicles**", Department of Networking and Switching Technology, has proposed that the rapid development of Internet and communication technologies, vehicles that often quickly move in cities or suburbs have strong computation and communication abilities. IoV is emerging as an important part of the smart or intelligent cities being proposed and developed around the world. IoV is a complex integrated network system that interconnects people within and around vehicles, intelligent systems on board vehicles, and various cyber-physical systems in urban environments. IoV goes beyond telematics, vehicle ad hoc networks, and intelligent transportation by integrating vehicles, sensors, and mobile devices into a global network to enable various services to be delivered to vehicular and transportation systems and to people on board and around vehicles.[3] Randy Smith, " **XFA: Faster Signature MatchingWith Extended Automata**", Department of Electronic Engineering from University of Wisconsin–Madison has proposed augment traditional finite state automata with a scratch memory that is manipulated by instructions attached to edges and states. It provide a formal definition for XFAs and present a technique for constructing them from regular expressions. It performed a feasibility study using a set of HTTP signatures from Snort and observed that XFAs have matching speeds approaching DFAs yet memory requirements similar to NFAs. Compared to multiple DFA-based techniques, our tests used 10× less memory *and* were 20× faster.[4] Masanori Bando," **Scalable Lookahead Regular Expression Detection System for Deep Packet Inspections**", Department of Information Engineering from Tohoku University, has proposed LaFA, an on-chip RegEx detection system that is highly scalable. The scalability of existing schemes is generally limited by the traditional per-character state processing and state transition detection paradigm. The main focus of existing schemes is on optimizing the number of states and the required transitions, but not on the suboptimal character-based detection method. Furthermore, the potential benefits of allowing out-of-sequence detection instead of detecting components of a RegEx in the order of appearance have not been explored. We propose to clearly separate detection operations from state transitions, opening up opportunities to further optimize traditional FAs. LaFA employs a novel lookahead technique to reorder the sequence of pattern detections.

Research directions

Research on RegEx matching has been proposed that they can be put into two categories: memory based and non-memory based. The former type relies on memories

to implement NFA or DFA; the latter type use FPGA logic research such as LUTs and flap-flops to carry out automata. Memory based methods carry out matching logic by running a lookup engine according to input characters and transition tables. Matching results can be obtained by looking up a result table using current active states. To improve the inspecting performance and rule-supporting capacity, researches have been proposed on increasing the memory access and usage from the prospective of transition precition.

Discussion

RegEx is a sequence of character that is capable of describing a certain string pattern.Each character in a regular expression is either understood to be a regular character with its literal meaning or a meta-character with its special meaning. From the perspective of functions, there are mainly two kinds of meta-characters: one is for representing a set of regular characters and the other is for describing repeat patterns of the preceding elements . To carry out the logic of repeat meta-character, repeat transition, which points to its starting state, has been introduced such as those in dotted lines. Because multi-stride conversion algorithm combines multiple 1-byte transitions for each multi-byte transition, repeat transition can lead to automata explosion.

Conclusion

we propose an intrusion detection system for IoV which can achieve high performance, low latency and acceptable energy consumption. Specifically, we focus on FPGA platform, and propose a novel data model based on current multi-stride NFA. Experiments show that the proposed system can achieve a throughput of more than 39 Gbps on existing FPGA platform and the total power consumption for the FPGA is about 7.5 w. Moreover, the processing latency of the prototype is about 4 us, and is about one sixtieth part of the latency of the popular software IDS. Our proposal could meet current need of IoV for IDS techniques. But the proposed method has following drawbacks. First, Link-NFA is specified for FPGA, it is unlikely to be implemented in other hardware platform such as those based on GPU and CPU. Second, the number of NFAs it may grow rapidly in some extreme cases. Third, as is discussed in 5.1, Link-NFA utilizes FIFOs to temporarily store intermediate results. Overrun may occur if too many intermediate results are reported by Sub-NFAs.

References

[1] “yang f,wang s,li j,lui z and sun q,”An overview of Internet of Vehicles”, China Communications, 11(10): 1-15, 2014.

[2] r. smith, c. estan, and s. jha, “XFA: Faster signature matching with extended automata[C]”, Proceedings of IEEE Symposium on Security and Privacy, pp.187–201, IEEE, 2008

[3] wang x,xu y,jiang j,ormond o,liu b,” StriFA: Stried iFnite Automata for high speed regular expression matching in network intrusion detection system[J]”, Systems Journal, IEEE, vol.7, no.3, pp.374–384, 2013.

[4] yamagaki n, sidhu r, and kamiya s, “Highspeed regular expression matching engine using multi-character NFA[C]”, Proceedings of Field Programmable Logic and Applications, pp.131–136, IEEE, 2008.