ICAI 2023
12th International Conference on Applied Informatics
Eger, Hungary, 2023

In-network DDoS detection and mitigation using INT data for IoT ecosystem*

Gereltsetseg Altangerel[a], **Máté Tejfel**[b]

[a]Faculty of Informatics, Eötvös Loránd University(ELTE), Budapest, Hungary
gereltsetseg@inf.elte.hu
ORCID: 0000-0002-1594-8158

[b]Faculty of Informatics, Eötvös Loránd University(ELTE), Budapest, Hungary
matej@inf.elte.hu
ORCID: 0000-0001-8982-1398

Abstract

Due to the limited capabilities and diversity of IoT devices, it is challenging to implement robust and unified security standards for these devices. Since the vulnerable IoT devices are outside the control of the network, they can easily become bots or botnets, and attacks from these devices have become very common in recent times [3].

To address this issue, we proposed a real-time IoT anomaly detection and mitigation solution at the programmable data plane in an SDN network environment using INT data. As far as we know, it is the first experiment in which INT data is used to detect IoT attacks in the programmable data plane.

Anomaly detection research in the data plane is currently uncommon compared to SDN control plane-based solutions [6]. The detection can be faster if it is implemented directly in the packet processing path or data plane. Also, most control plane solutions use network traffic datasets(e.g., netflow, wireshark) for IoT anomaly detection [1]. Therefore, the main disadvantage of control plane solutions is that detection cannot be done in real-time. To the best of our knowledge, there is

*The research has been supported by the project "Application Domain Specific Highly Reliable IT Solutions" implemented with the support of the NRDI Fund of Hungary, financed under the Thematic Excellence Programme TKP2020-NKA-06 (National Challenges Sub programme) funding scheme.

only one experimental data plane solution for DDoS detection. It uses the Shannon entropy based on the frequency of source and destination IP addresses [4].

A programmable data plane is the latest concept in computer networking. It allows anyone to quickly design, test, and deploy a variety of applications in the data plane with domain-specific programming languages. One of these applications is In-Band Network Telemetry (INT), a new monitoring system that collects real-time network telemetry information (hop latency, flow latency, queue depth, etc.) from the data plane [5].

We implemented our proposed solution using P4, a domain-specific programming language designed to describe the data plane layer of packet processing algorithms [2]. Before the implementation, we collected INT data (i.e., queue depth of the network device's output interface) from our simulated SDN network under DDoS attack(UDP with ICMP flooding) and non-attack(UDP with ICMP) conditions and performed simple statistical analysis on the collected data. Firstly, we used a t-test statistical analysis to compare these datasets (5000 queue depth records each with and without attack) and smaller datasets consisting of 128 records randomly selected from these datasets. The analysis provided a hypothesis that these datasets were statistically significantly different at 99 percent probability. After that, when we compared these datasets using simple statistical values like mean, median, mode, etc., we found enough differences in these statistics to detect IoT anomalies. Since our anomaly detection solution for IoT ecosystem aims to be simple and fast based on P4-language capabilities, we implemented it based on the mean value of queue depth.

Figure 1 shows our proposed P4 packet processing pipeline for IoT anomaly detection. The pipeline processes the packet according to three states: normal, detection, and mitigation.

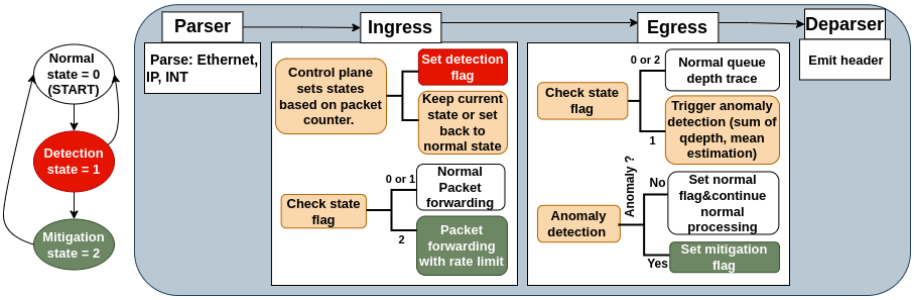

Figure 1. IoT anomaly detection pipeline in P4.

- In the normal state, the packets are processed as shown in the white blocks. To enable anomaly detection or maintain the current state, the value of the packet counter implemented in the ingress is taken into account. The packet counter is only read by the control plane, so the control plane sets one of the above states based on the configured threshold counter value.

- In the detection state, the value of the queue depth on the output interface at the moment of transmission of each 128 packets is added to the stateful register of the egress part (the sum of the 128 queue depth values). The mean of queue depth calculated based on this and the mitigation starts if this mean value is higher than baseline mean of the INT data under normal traffic conditions
- In the mitigation state, attacks are mitigated by limiting the rate of the packet's incoming interface. It goes back to normal state based on the packet counter using the control plane.

The number of queue depth to calculate the mean value is currently set to 128, and a more optimal value can be determined in further experiments, and the smaller the number, the faster the anomaly will be detected. If set to 128, the average anomaly detection time can be found by multiplying the processing time (delay) of one packet by 128. This delay depends on parameters like network protocol, computational power at node, and efficiency of network interface cards.

Based on some basic estimation in our current experiment the detection delay is half as low as the results of previous DDoS [4] research, as well the detection accuracy is similarly high.

References

[1] M. Ahmed, A. Naser Mahmood, J. Hu: *A survey of network anomaly detection techniques*, Journal of Network and Computer Applications 60 (2016), pp. 19–31, issn: 10958592, doi: 10.1016/j.jnca.2015.11.016, url: http://dx.doi.org/10.1016/j.jnca.2015.11.016.

[2] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, D. Walker: *P4: Programming protocol-independent packet processors*, Computer Communication Review 44.3 (2014), pp. 87–95, issn: 19435819, doi: 10.1145/2656877.2656890, arXiv: 1312.1719.

[3] Gartner: *IoT Security Primer : Challenges and Emerging Practices*, February 2018 (2020), pp. 1–21.

[4] A. D. S. Ilha, A. C. Lapolli, J. A. Marques, L. P. Gaspary: *Euclid: A Fully In-Network, P4-Based Approach for Real-Time DDoS Attack Detection and Mitigation*, IEEE Transactions on Network and Service Management 18.3 (2021), pp. 3121–3139, issn: 19324537, doi: 10.1109/TNSM.2020.3048265.

[5] C. Kim, A. Sivaraman, N. Katta, A. Bas, A. Dixit, L. J. Wobker, B. Networks: *In-band Network Telemetry via Programmable Dataplanes*, Sosr Figure 2 (2015), pp. 2–3, url: https://www.cs.princeton.edu/$%5Csim$nkatta/papers/int-demo.pdf.

[6] E. Tsogbaatar, M. H. Bhuyan, Y. Taenaka, D. Fall, K. Gonchigsumlaa, E. Elmroth, Y. Kadobayashi: *DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT*, Internet of Things 14.March (2021), p. 100391, issn: 25426605, doi: 10.1016/j.iot.2021.100391, url: https://doi.org/10.1016/j.iot.2021.100391.