John Hopkins University uses ABot for 5G Network Threat Detection

Rebaca

ENSURING QUALITY ON SCHEDULE

1 Objective

Identify various DDoS attack scenarios on both 5G control plane and data plane and test different remediation techniques.

2 Engagement Details

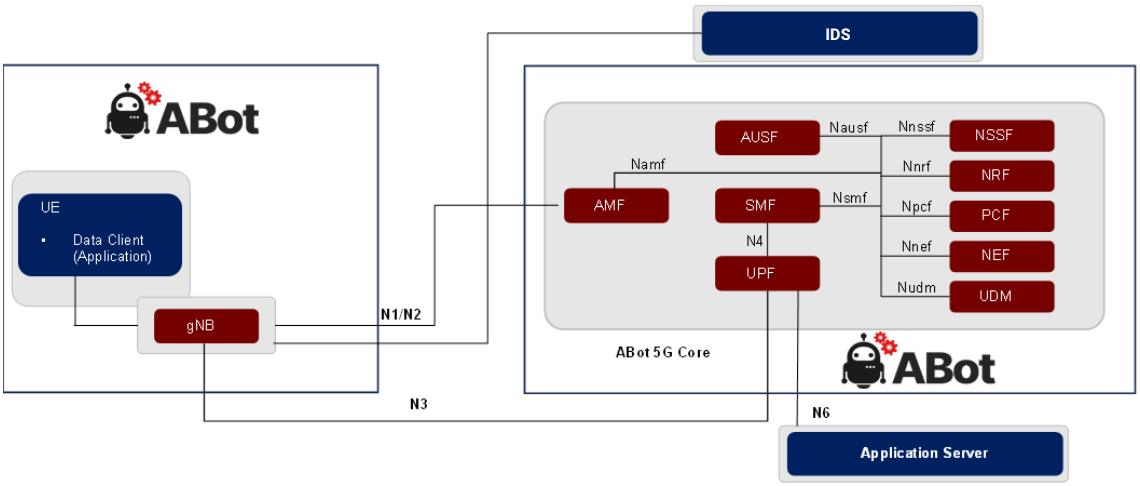
ABot simulated NFs, Use Case scenarios and traffic generators are used to simulate various DDoS attacks on control plane and data plane. Captured PCAPs are fed to an external Intrusion Detection System (IDS) to identify the DoS attack. Different remediation techniques triggered on IDS alerts are then applied by ABot to mitigate the DOS attack. The effectiveness of these techniques is subsequently verified through KPIs captured by ABot Analytics.

2.1 Lab Setup

As a part of Lab setup Rebaca engineering team was involved in the following:

- Proper dimensioning of the VMs based on the scope of the test i.e., total number of UEs, concurrency, throughput, etc.
- Helped in installation and configuration of ABot core and analytics, data server and data client VMs.
- Helped in validation of the test setup by executing Sanity Test suite.

Below diagram shows the topology of JHU test setup in ABot Emulated mode, where ABot 5G Core acts as a SuT.



It the above diagram Data Client is being used for UE emulation and application traffic generation and Data Server (Application server) is being used as Receiver node for UL traffic and Application traffic generator for downlink data. IDS is being used for Sniffing packet from ABot Core VM interfaces and to generate alert in case of DDoS attack.

2.2 Test case execution

ABot has the ability to emulate all NFs in 5GC along with UE and gNodeB. This enabled JHU to simulate a 5G system without any additional cost.

- Rebaca engineers guided the JHU team to execute the test scenarios using the specific features files targeted towards the above-mentioned scenarios.
- Rebaca engineers helped the JHU team to adapt and customize the feature files to create variations of the DDoS attack scenario.

- IDS detects the threat (increased packet rate) and generates alerts.

Rebaca engineers provided customization services to integrate ABot with IDS, to throttle control plane or data plane rate, based on alerts raised by IDS on threshold breach.

Test Case Name: CP_DDoS_Attack_Scenario.feature

Test Scenario: Generate SCTP traffic over N1-N2 interface at a high rate to simulate DDoS attack on control plane

Topology: ABot emulates gNodeB and 5G core.

Test Case Name: DP_DDoS_Attack_Scenario.feature

Test Scenario: Generate TCP traffic over N3 interface at a high rate to simulate DDoS attack on data plane

Topology: ABot emulates gNodeB and 5G core. Also, iPerf client and server are used to send and receive UL/DL TCP traffic

2.3 Test case authoring

Based on use case requirement specified by JHU, Rebaca engineering team developed feature files to simulate DDoS attack scenario, for both control plane and data plane. ABot SmartEditor was used to customize the canned feature files of ABot to meet the requirement. ABot SmartEditor is a 3GPP aware test case authoring tool which requires no background on automation scripting and needs minimal domain knowledge.

2.4 Test Analysis

Rebaca engineers used the Grafana panels to measure the network KPIs to analyze the data throughput pattern, for both SCTP and GTP packets, to confirm that the DDoS scenario simulation and, throttling of the packets after receiving the alert on threshold breach from IDS.

2.5 Control plane DDoS attack scenario simulation

ABot starts the control plane traffic with smaller rate, with significant gaps between individual procedures. ABot then increases the control plane traffic to a consistently high rate.

If the high rate is sustained long enough to breach the threshold defined in IDS, an alert is generated by IDS towards ABot, and ABot will throttle the control plane traffic rate.

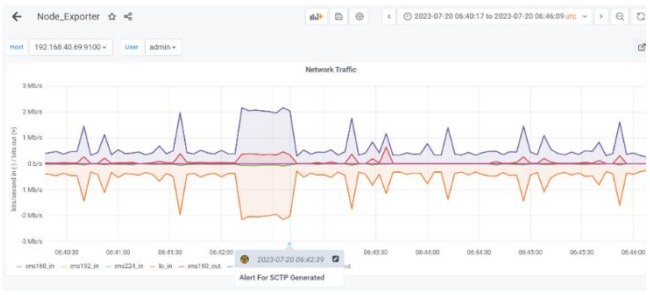


Figure 1: Representation from ABot Grafana

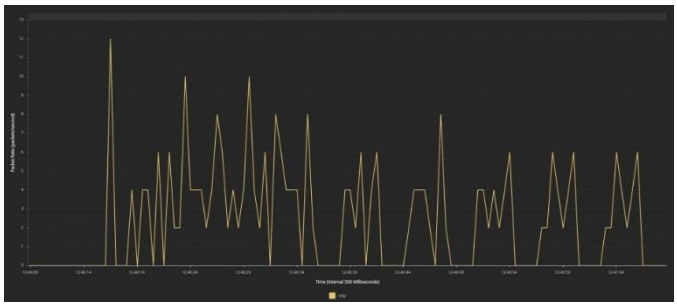


Figure 2: Representation from IDS

2.6 Data plane DDoS attack scenario simulation

ABot starts the Data plane throughput with smaller rate. ABot then increases the throughput to a very high rate. If the rate is high enough to breach the threshold defined in IDS, an alert is generated by IDS towards ABot, and ABot will throttle the throughput rate.

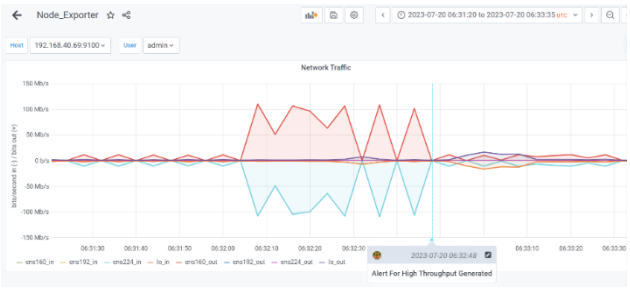


Figure 3: Representation from ABot Grafana

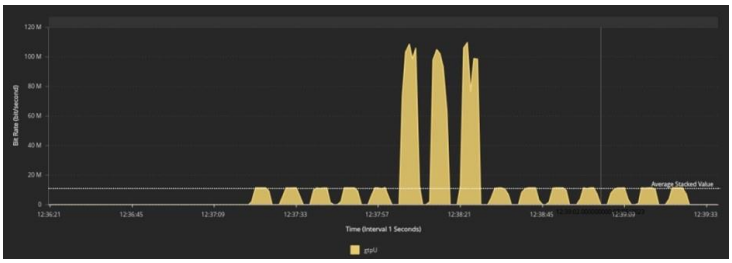


Figure 4: Representation from IDS

3 Analytics

ABot has a powerful analytics capability which helped JHU team to analyze the test execution results using artefacts, such as automation logs, node specific logs, pcaps etc. and identify the root cause of the failed test cases. ABot Analytics also provided insight using various infrastructure and mobility KPIs.

4 Outcome

ABot integrated with IDS, enabling JHU to perform various types of experiments related to DDoS attacks in 5G systems.