PoC Report

1 PoC Project Details

1.1 PoC Project Review

PoC Number:	7
PoC Project Name:	Zero-touch closed-control security management of attacks detection and mitigation
PoC Project Host:	CTTC
Short Description:	This PoC demonstrates H2020 MonB5G (Distributed management of Network Slices in beyond 5G) projects' zero-touch security management solution that uses a closed-control loop featuring Machine Learning (ML) to detect and mitigate in-slice attacks issued from Machine Type Communication (MTC) devices on 5G Core Network (CN) components, focusing on Distributed Denial of Service (DDoS) attacks.
PoC Project Status : *(Ongoing/Completed)*	Completed

1.2 PoC Team Members Review

	Organisation name	ISG ZSM participant (yes/no)	Contact (Email)	PoC Point of Contact (*)	Role (**)	PoC Components
1	CTTC	yes	engin.zeydan@cttc.cat	X	research center	(1) Providing cloud native MS for PoC (2) Contribute to MonB5G MS component development
2	EURECOM	no	adlen.ksentini@eurecom.fr		research center	(1) AE and DE component development (2) Algorithm research on improving DDoS detection capabilities (3) Providing cloud native environment for PoC
3	NEC	yes	zhao.xu@neclab.eu		supplier	(1) Providing cloud native AE and DE for PoC (2) Development of overall MonB5G components (MS, AE and DE) in containerized cloud native environment
4	OTE	no	vvlahodimi@cosmote.gr		network/service provider	(1) Provide configuration information and feedback for 5G core network equipment during PoC (2) Building generic KPIs to be monitored during PoC

(*) Identify the PoC Point of Contact with an X.
(**) The Role will be network operator/service provider, infrastructure provider, application provider or other.

All the PoC Team members listed above declare that the information in this report is conformant to their activities during the PoC Project.

1.3 PoC Project Scope Review

1.3.1 PoC Topics

Report the status of all the PoC Topics and Expected Contributions anticipated in the PoC Proposal

PoC Topic Code	PoC Topic Description	Related WI	Submitted Contribution link	Date	Status (*)
Topic 3 (Intent-	Demonstration of closed loop	ZSM009	Demo	February 2023	Completed

driven Closed-loop automation)	automation for mitigating against DDoS attacks from MTC (Machine Type Communication) devices on 5G Core Network (CN) components,				
(*) Planned, On-going, Completed, delayed (new target date), Abandoned					

The proposed framework is aligned with the "Figure 7.2.1-1: Functional view of a Closed Loop and its stages within the ZSM framework" in ZSM009-1. The mapping of the in-scope management components of MonB5G with ZSM services and capabilities defined in Section 7.2 Functional view is as follows:

- The monitoring stage is realized, fully or in part, by the (domain or E2E) data collection management services (clauses 6.5.2 and 6.6.2 of ETSI GS ZSM 002). The "Monitoring" stage of Figure 7.2.1-1 is mapped with MS in MonB5G architecture.
- The analysis stage is realized, fully or in part, by the (domain or E2E) analytics management services (clauses 6.5.3 and 6.6.3 of ETSI GS ZSM 002). The "Analysis" stage of Figure 7.2.1-1 is mapped with AE.
- The decision stage is realized, fully or in part, by the (domain or E2E) intelligence management services (clauses 6.5.4 and 6.6.4 of ETSI GS ZSM 002). The "Decision" stage of Figure 7.2.1-1 is mapped with DE.
- The execution stage is realized, fully or in part, by the domain orchestration and control management services (clauses 6.5.5 and 6.5.6 of ETSI GS ZSM 002), when the CL is deployed within a management domain. The "Execution" stage is mapped with Actuators.
- Knowledge is realized, fully or in part, by the (domain or cross-domain) data services (clause 6.4 of ETSI GS ZSM 002) The "Knowledge" of Figure 7.2.1-1 is mapped to store historical data for training ML algorithms in MonB5G architecture.
- The communication and interoperation between the CL stages may be realized, fully or in part, by the (domain or cross-domain) integration fabric management services. These stages in Figure 7.2.1-1 is mapped with the message bus in MonB5G.
- The primary flow of data and control messages are expressed by arrows M2A (is between MS and AE), A2D (is between AE and DE), D2E (is between DE and Actuator) and E2M (is between Actuator and MS)
- The double-headed arrows K1 (Store historical information), K2 (Store historical analytics insights), K3 (Store historical workflows) and K4 (Store historical actions)

1.3.2 Other topics in scope

Report the status of all the additional PoC Topics and Contributions anticipated in the PoC Proposal.

PoC Topic Code	PoC Topic Description	Related WI	Submitted Contribution link	Date	Status (*)
(*) Planned, On-going, Completed, delayed (new target date), Abandoned					

1.4 PoC Project Milestones Review

PoC Milestone	Milestone description	Target Date	Additional Info	Completion Date
P.S	PoC Project Start	September 2022		1 September 2022
P.C1	PoC Expected Contribution 1	November 2022	Design of ZSM system featuring a closed-control loop using MonB5G devised elements: Monitoring System (MS), Analytical Engine (AE), and Decision Engin (DE). At this step, components that will be ready: - MS interacting with a 5G CN to collect data on the UE attach request received by the AMF and their timestamp. - AE running the ML algorithm to detect attack issued by MTC devices inside a mMTC slice DE interacting with the AMF and UDM to de-register involved UEs in an attack and add them to the list of banned devices.	30 November 2022
P.C2	PoC Expected Contribution 2	January 2023	Full PoC integrated with OAI AMF/UDM and fully operating.	15 January 2023
P.D	PoC Demo	February 2023	IoT Solutions World Congress 2023, Barcelona	31 January- 2 February 2023
P.R	PoC Report	February 2023	mMTC attack scenario: Security inside the closed-loop domain of the mMTC slice, employing the three key components of the MonB5G architecture: MS, AE, and DE	28 February 2023
P.E	PoC Project End	February 2023		28 February 2023

1.5 Confirmation of PoC Event Occurrence

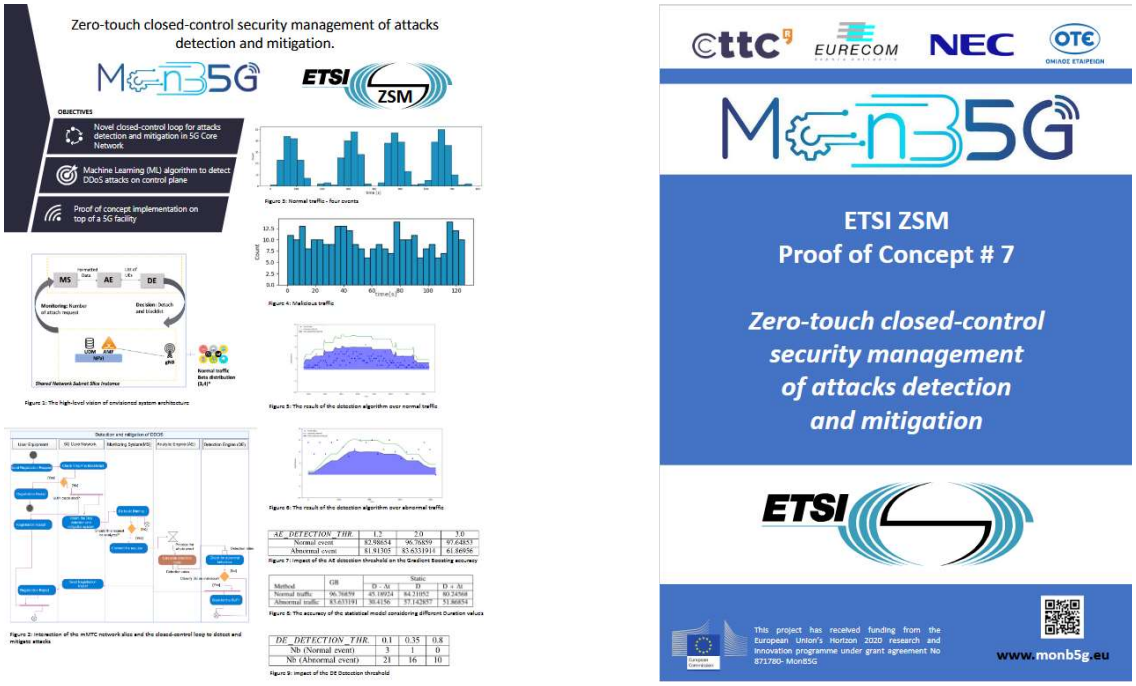
The PoC was presented in a F2F event, whose details are captured below:

- **Event Name**: IoT Solutions World Congress (IOTSWC) (https://www.iotsworldcongress.com/).
- **Event Occurrence**: Barcelona, Spain, 31 January-2 February 2023.
- **Event description**: IOTSWC is the leading event on trends in digital transformation, based on disruptive technologies.
- **Event statistics**: IOTSWC 23 edition had 15.500 attendees.

For the PoC showcasing, the PoC team presented in the MonB5G project booth:

- **One poster** (see Figure 1). It was available for public consultation at the project booths during the full event.
- **Two roll-ups** (see Figure 1 and Figure 2).
- **Displayed a pre-recorded video of the demo** (see Figure 2). The video was continuously reproduced at project booths during the full event.

- **Displayed MonB5G generic video** (see Figure 3). The video was continuously reproduced at project booths during the full event.



(a) **(b)**

Figure 1: (a) Poster promoting ETSI ZSM PoC#7, (b) ETSI ZSM PoC#7 Roll-up.

Figure 2 shows the PoC team members who physically attended, at the MonB5G project booth (including both screens).

Figure 2: PoC team members and MonB5G booth

A video presenting PoC#7 has been published in MonB5G YouTube channel:
https://www.youtube.com/watch?v=Vclyp-N03mI

2 ZSM PoC Technical Report

2.1 Setting the scene

This section details the rationale and motivation behind PoC#7.

2.1.1 Problem statement

5G was designed with built-in security controls to address many of the threats found in 4G/3G/2G networks, such as enforcing mutual authentication to prevent fake base-station attacks, encrypting subscriber identities, and enforcing more secure cipher suites. However, more functionality always comes with new risks and attack vectors when opening the network to IoT devices, particularly. Some of these risks can affect the performances of 5G network functions (mainly the service availability). By embracing network slicing, 5G networks can mitigate inter-slice attacks as isolation is one of the key features.

Indeed, the isolation guaranteed by network slicing offers performance guarantees to the applications and ensures isolation, such that attacks (e.g., leakage, breach, Distributed DDoS - DDoS) remain contained and do not propagate to the network. However, an in-slice attack may correspond to a subset of the UEs attached to a specific network slice issuing malicious traffic towards the infrastructure services. A typical example is compromised MTC devices (i.e., IoT devices) generating a massive number of network attachment requests. These attacks need to be quickly identified and mitigated to avoid system failure. It is worth noting that 3GPP clearly stated in [1] that 5G networks should be protected from DDoS attacks, where mechanisms detecting and mitigating this type of attacks are needed.

2.1.2 Use case description

The proposed use case relies on ML to detect abnormal traffic of MTC devices that could cause DDoS on the control plane of the 5G core network (by flooding the AMF with signalling messages). Hence, it will be possible to mitigate the attack by making efficient decisions to prevent flooding of the AMF with traffic and causing DDoS or deteriorating performance for legitimate users. This type of attack can be more effective on mMTC than other 5G services, assuming the very high number of MTC devices supposed to support.

In this work, we assume that a mMTC slice is composed of: (1) a shared sub-slice with other existing network slices, which runs the 5G CN (including the AMF) and gNodeB; (2) a specific subslice to run the application that collects data from the MTC devices. It is well accepted that MTC devices generate two main types of traffic [2]. The first one is “Periodic”, where the devices emit data periodically, which may correspond to the case of meteorological data. The second type is “Event-Driven”. In this case, the devices emit data when a specific event occurs; for example, smoke (the signal of a possible fire) is detected.

Detecting anomalous traffic in the first type is simple, as most of the anomaly detection algorithms can directly be applied to the problem. However, predicting when an event will consistently occur for the second type of traffic is very challenging. While there exist models for the traffic during activity periods, it is difficult to solve the problem of finding anomalies just by trying to learn the function the data distribution follows, if we consider time-series data.

To detect malicious traffic of MTC devices, we will consider the traffic model proposed by 3GPP, which suggests that traffic of MTC devices' connection after detecting an event follows the β(3, 4) probability distribution [3]. Accordingly, we assume that (1) normal traffic follows the β(3, 4) probability distribution; (2) the detection events do not overlap (i.e., each event is independent of the other). We argue the latter by the fact that most of the devices run only one type of application, which monitors a single event.

2.2 PoC description

2.2.1 PoC objectives

The objective of the PoC is to demonstrate MonB5G approach featuring zero-touch security management of in-slice attack detection and mitigation considering mMTC slices in 5G. The MonB5G ZSM approach relies on a closed-control loop that uses machine learning to detect abnormal traffic of MTC devices that could cause DDoS on the control plane of the 5G core network (by flooding the AMF with signalling messages) and extract the list of possible UE involved in the attack.
The mitigation step consists in de-registering and placing the concerned in UE in a banned list. Hence these decisions prevent flooding of the AMF with traffic and causing DDoS or deteriorating performance for legitimate users. This type of attack can be more effective on mMTC than other 5G services, assuming the very high number of MTC devices supposed to support.
The PoC uses OpenAirInteface (OAI)[1] 5G Core Network and relies on My5GRANtester[2] to generate MTC traffic emulating an attack. All the MonB5G components MS, AE and DE will run as containers in a cloud-native environment.

2.2.2 PoC architecture

Figure 3 illustrates the high-level view of the PoC and its components.

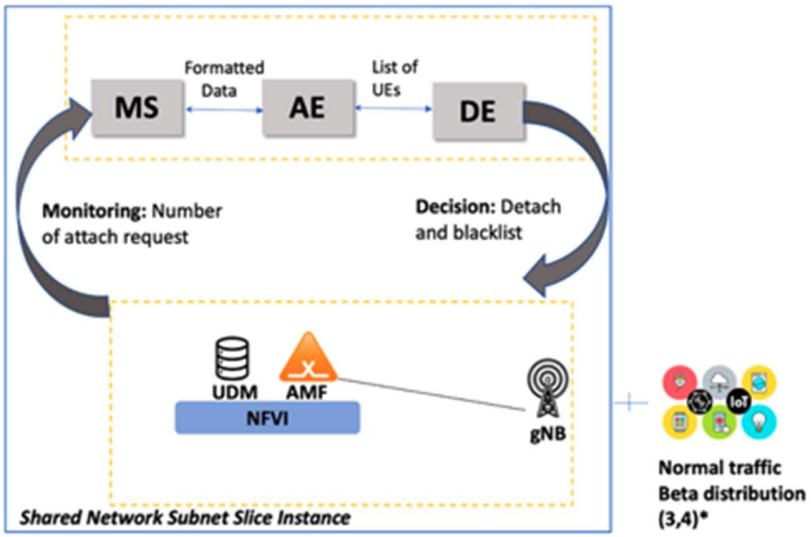


Figure 3: High level view of the PoC architecture

The envisioned system is composed of the closed-control components (MS, AE, and DE) that interact and protect the shared sub-slice components (5G CN and gNodeBs) against DDoS attacks. Here, we focus on protecting the

[1] https://openairinterface.org/
[2] https://github.com/my5G/my5G-RANTester

AMF as it is the entry point of the 5G CN and treats all the Attach requests coming from the different gNodeB under its control. The closed-control loop is composed of three entities: MS, which collects information from the AMF, AE, which uses ML to predict attacks, and Decision Engine (DE), which reacts to the alert sent by the AE by acting on the AMF (block and blacklist UE). The control-loop runs as software and can be co-located with the orchestrator managing the life cycle of the shared sub-slice. It should be noted that the AMF, via an Element Manager (EM), exposes API for an orchestrator to extract and monitor information on the AMF's functioning or to change the configuration of the latter. In the proposed framework, the MS monitors the Attach Request received by the AMF, and the DE requests to send Registration Reject to suspected devices.

It should be noted that we followed 3GPP recommendation on the normal traffic generated by MTC devices when detecting an event that corresponds to Beta (3,4) [3]. It should be noted that AMF's EM is an agent that exposes REST API that allows the configuration and monitoring of AMF. Among the possible remote configuration are: send messages to UE such as send registration reject to UE, update the slice id supported by AMF, etc. Regarding monitoring, EM exposes API to monitor the number of attach request, for instance, during a period or register to event notification. In the latter, EM sends a notification each time a UE has sent an attach request to AMF.

2.2.3 PoC user story

Figure 4 highlights the interaction among the different actors involved in detecting and mitigating DDoS attacks: the mMTC network slice components (UEs and 5GCN) and the closed-control loop elements (MS, AE, and DE). It is worth noting that the closed-control loop run in parallel to the mMTC network slice elements and uses only the monitored attach requests to detect and mitigate attacks.

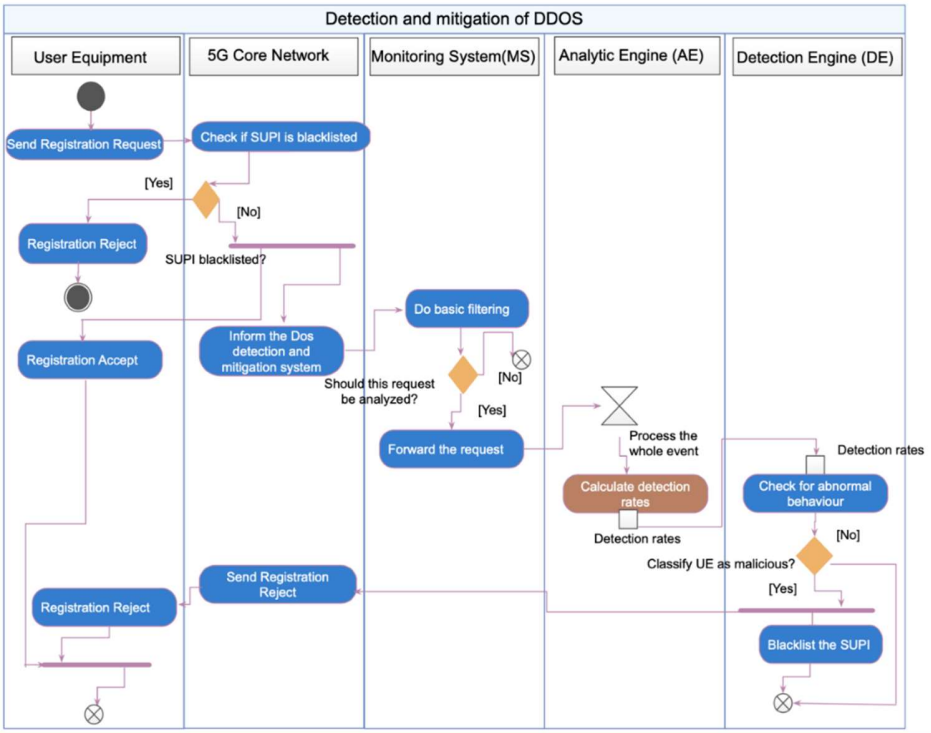


Figure 4: Interaction of the mMTC network slice and the closed-control loop to detect and mitigate attacks

In the considered scenario, the MTC devices (or UEs), when detecting an event or participating in an attack, first send an Attach request to AMF. The latter must first authenticate the device and then give it access to the network resources (register the device), mainly to the data plane, to send its data. During the authentication process, the

AMF checks with the Unified Data Management (UDM) if the device is blacklisted or not. To recall, the UDM is the 5G Core network function, which stores subscribers' information (Subscriber Permanent Identifier -SUPI - Quality of Service -QoS- Policy, the key k, Operator key, etc.). The device can be blacklisted if it has participated in an attack.

2.2.4 PoC setup

To validate the proposed zero-touch security management system, we have used a 5G testbed deployed at EURECOM. We have implemented the closed-control loop components (i.e., MS, AE, and DE) and an Element Manager (EM) on top of the AMF. The latter exposes API to (1) MS to monitor the Attach Request message; (2) DE to detach and blacklist UEs involved in an attack.

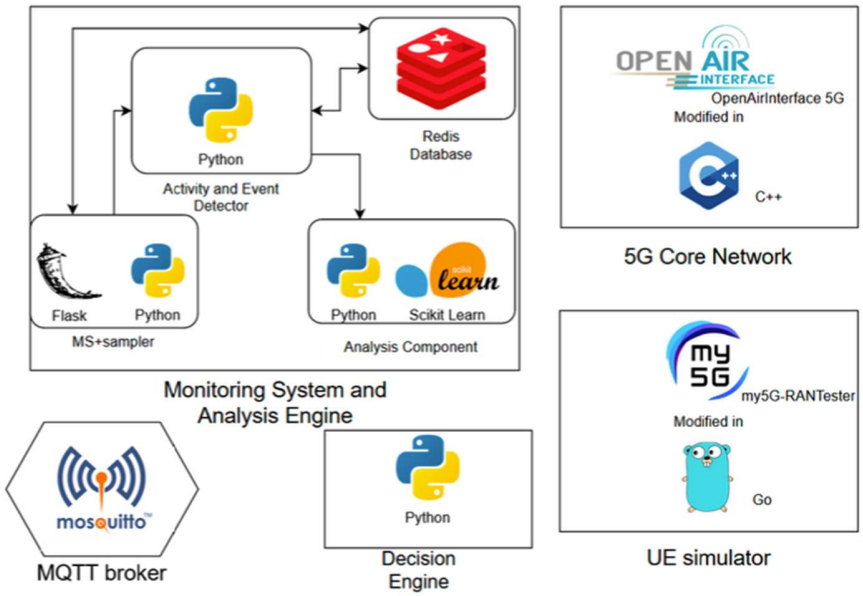


Figure 5: Test platform and technological components.

Figure 5 illustrates the different technologies used to implement the above-mentioned components. As a quick reminder, the roles of the different components are:

- **MS and sampler**: MS is the first component to receive traffic from the 5G CN. It performs basic filtering on it. While the sampler does sampling of the input data, it receives information on Attach Requests as they are received (with no guaranteed periodicity) and emits periodic data, with the number of Attach Requests received in time intervals of a given length.
- **Activity and Event Detectors**: These components receive the sampled data and should detect an event. For each event, these components only emit data at its end, with the number of requests on each time-slice and all the UEs that emitted traffic during the event.
- **Analysis Component:** This component runs the ML algorithm on the given data, calculating a detection rate for each time-slice (for all devices in the time-slice).
- **DE:** This component receives data from the Analysis Component and decides which devices should be disconnected from the network and then blacklisted.

- **MQTT Broker:** is used to implementing the communication bus between the different components of the closed-loop control system, and between the closed-loop control system and the AMF.

Regarding the UE, we used and updated a 5G UE emulator, my5G-RANTester to be able to send a high number of UE Attach Request messages in parallel to simulate an attack or normal traffic. Indeed, my5G-RANTester is a tool for emulating control and data planes of the UEs and gNodeB. my5G-RANTester follows the 3GPP Release 15 standard for RAN. By using my5G-RANTester, it is possible to generate different workloads and test several functionalities of a 5G CN, including its compliance with the 3GPP standards. Scalability is also a relevant feature of the my5GRANTester, which can mimic the behaviour of a large number of UEs and gNodeBs simultaneously accessing a 5G CN. Currently, the wireless channel is not implemented in the tool. The AMF and 5G CN components are based on OAI.

2.3 PoC showcasing

This section provides a description of workflow execution for this PoC in attack detection with abnormal and normal traffic.

2.3.1 PoC execution: workflow sequence

2.3.1.1 Scenario 1: Attack Detection with abnormal traffic

Goal	The objective of this scenario is to demonstrate the robustness of MonB5G for identifying, detecting and then mitigating the in-slice attacks. Malicious events (mMTC attacks) would be detected thanks to various MonB5G's components including Monitoring System (MS), Analytics Engine (AE), and Decision Engine (DE).
Pre-conditions	• High number of attach requests.
Post-conditions	• Malicious devices are blacklisted and disconnected from the network.
Sequence flow	The proposed closed-control loop is composed of 3 components (MS, AE, and DE) that interact and protect the shared sub-slice components (5G CN and gNodeBs) against DDoS attacks. Here, we focus on protecting the AMF as it is the entry point of the 5G CN and treats all the Attach Requests coming from the different gNodeB under its control. The closed-control loop is composed of three entities: 1. MS: collects information from the AMF, MS monitors the Attach Request received by the AMF. 2. AE: uses Gradient Boosting algorithm to predict attacks, and 3. DE: reacts to the alert sent by AE by acting on AMF (block and blacklist UE), it requests AMF to send Registration Reject to suspected devices. 4. AMF sends a registration request to UE backlisted. 5. Malicious devices are disconnected.

2.3.1.2 Scenario 2: Attack Detection with normal traffic

Goal	The objective of this scenario is to demonstrate the robustness of MonB5G for identifying, detecting and then mitigating the in-slice attacks. Normal events are identified as normal thanks to various MonB5G's components including Monitoring System (MS), Analytics Engine (AE), and Decision Engine (DE).
Pre-conditions	• High number of attach requests.

Post-conditions	• Normal devices continue to be connected to the network.
Sequence flow	The proposed closed-control loop is composed of 3 components (MS, AE, and DE) that interact and protect the shared sub-slice components (5G CN and gNodeBs) against DDoS attacks. Here, we focus on protecting the AMF as it is the entry point of the 5G CN and treats all the Attach Requests coming from the different gNodeB under its control. The closed-control loop is composed of three entities: 6. MS: collects information from the AMF, MS monitors the Attach Request received by the AMF. 7. AE: uses Gradient Boosting algorithm to predict attacks, and no alert is sent to DE 8. DE: receives no alert and takes no action. Actions are blacklisting or blocking UEs. 9. Normal devices continue keeping connected.

2.4 PoC Suggested Action Items

PoC #7 exemplifies an evolutionary path solution for secure zero touch network service and management based on the utilization of triplet (MS + AE +DE) proposed in MonB5G. The PoC has shown that detecting and mitigating in-slice attacks on 5G Core Network components using ML techniques and ZSM concept (i.e., closed control loop) can protect 5G from Distributed Denial of Service (DDoS) attacks.

The PoC#7 sets the ground for future experimentation in the future, with:

- Other advanced attack scenarios like model poisoning attacks, vulnerabilities and misconfiguration in 5G core network, UE identification due to malicious MS, AE, DE components.
- Focus on more operational and KPI enriching aspects for above listed set of attacks and provide assurance to monitoring, analysis and decision-making process.

References

[1] Architecture enhancements for 5G System (5GS) to support network data analytics services, 3GPP TS 23.288 version 16.4.0 Release 16, July, 2020.

[2] Florian Metzger and Tobias Hoßfeld and André Bauer et al, Modeling of Aggregated IoT Traffic and its Application to an IoT Cloud, Proceedings of the IEEE, 1558-2256, doi = 10.1109/JPROC.2019.2901578, mar, 2019.

[3] Markus Laner and Philipp Svoboda and Navid Nikaein et al, Traffic Models for Machine Type Communications, ISWCS 2013; The Tenth International Symposium on Wireless Communication Systems, August 2013.