# ISG ZSM PoC Proposal:

# Zero-touch closed-control security management of attacks detection and mitigation

## 1 PoC Project Details

### 1.1 PoC Project

| | |
|---|---|
| PoC Number: | #7 |
| PoC Project Name: | Zero-touch closed-control security management of attacks detection and mitigation |
| PoC Project Host: | CTTC |
| Short Description: | PoC will demonstrate 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 MTC devices on 5G CN components, focusing on Distributed Denial of Service (DDoS) attacks. |

### 1.2 PoC Team Members

| | 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 environment for PoC<br>(2) Contribute to MonB5G MS component development |
| 2 | EURECOM | no | adlen.ksentini@eurecom.fr | | research center | (1) AE and DE component development<br>(2) Algorithm research on improving DDoS detection capabilities |
| 3 | NEC | yes | zhao.xu@neclab.eu | | supplier | Development of overall MonB5G components |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | (MS, AE and DE) |
| 4 | OTE | no | vvlahodimi@cosmote.gr | | network/service provider | Provide network equipment and domain controllers for PoC |

(*) Identify the PoC Point of Contact with an X.

(**) The Role will be network/service provider, supplier, or other (universities, research centers, test labs, Open Source projects, integrators, etc…).

All the PoC Team members listed above declare that the information in this proposal is conformant to their plans at this date and commit to inform ETSI timely in case of changes in the PoC Team, scope or timeline.

## 1.3 PoC Project Scope

### 1.3.1 PoC Topics

PoC Topics identified in this clause need to be taken for the PoC Topic List identified by ISG ZSM and publicly available in the ZSM WIKI. PoC Teams addressing these topics commit to submit the expected contributions in a timely manner.

| PoC Topic Code | PoC Topic Description | Related WI | Expected Contribution | Target Date |
|---|---|---|---|---|
| Topic 3 (Intent-driven Closed-loop automation) | Demonstration of closed loop automation for mitigating against DDoS attacks from MTC (Machine Type Communication) devices on 5G Core Network (CN) components,<br><br>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:<br><br>- 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 | ZSM009-1 | Demo | February 2023 |

| | | | | |
|---|---|---|---|---|
| | 7.2.1-1 is mapped with MS in MonB5G architecture.<br><br>- 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.<br><br>- 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.<br><br>- 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.<br><br>- 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.<br><br>- 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.<br><br>- 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)<br><br>- 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

List here any additional topic for which the PoC plans to provide input/feedback to the ISG ZSM.

| PoC Topic Code | PoC Topic Description | Related WG/WI | Expected Contribution | Target Date |
|---|---|---|---|---|
| A | | | | |
| B | | | | |

## 1.4 PoC Project Milestones

| PoC Milestone | Milestone description | Target Date | Additional Info |
|---|---|---|---|
| P.S | PoC Project Start | September 2022 | |
| P.C1 | PoC Expected Contribution 1 | November 2022 | Design of zero touch 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:<br>- MS interacting with a 5G CN to collect data on the UE attach request received by the AMF and their timestamp.<br>- AE running the ML algorithm to detect attack issued by MTC devices inside a mMTC slice<br>- DE interacting with the AMF and UDM to de-register involved UEs in an attack and add them to the list of banned devices. |
| P.C2 | PoC Expected Contribution 2 | January 2023 | Full PoC integrated with OAI AMF/UDM and fully operating. |
| P.D | PoC Demo | February 2023 | Venue candidates are: IoT solutions World congress end of January 2023 or MWC end of 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 |

| | | | |
|---|---|---|---|
| | | | |
| P.E | PoC Project End | February 2023 | |

NOTE: Milestones need to be entered in chronological order.

## 1.5 Additional Details

More details about the PoC content can be found in MonB5G project's dissemination and communication activities: https://www.monb5g.eu/dissemination-n-communication/ .

# 2 PoC Technical Details

## 2.1 PoC Overview

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 signaling 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 will use OpenAirInteface (OAI)[1] 5G Core Network and rely 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 PoC Architecture

[1] https://openairinterface.org/

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

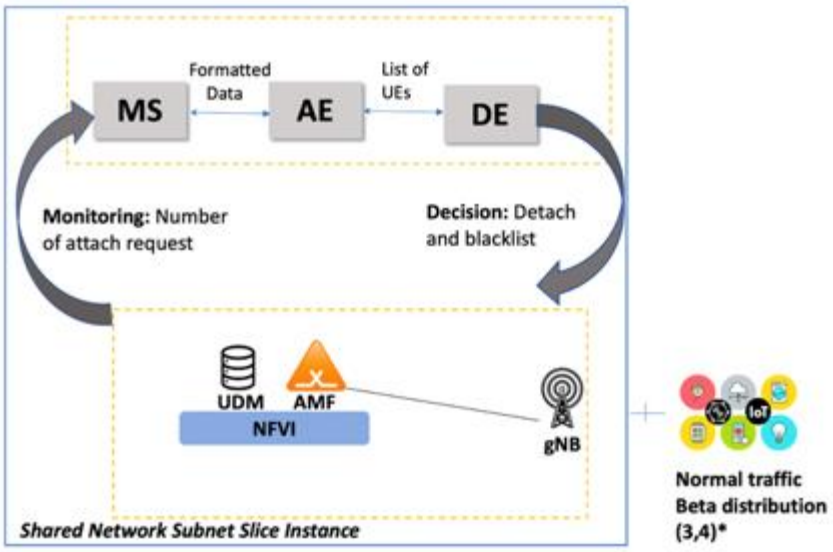


**Figure 1:High level view of the PoC architecture**

Figure 1 illustrates the high-level view of the PoC and its components. 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 gNBs) 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 gNB 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 correspond 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 a attach request to AMF.

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

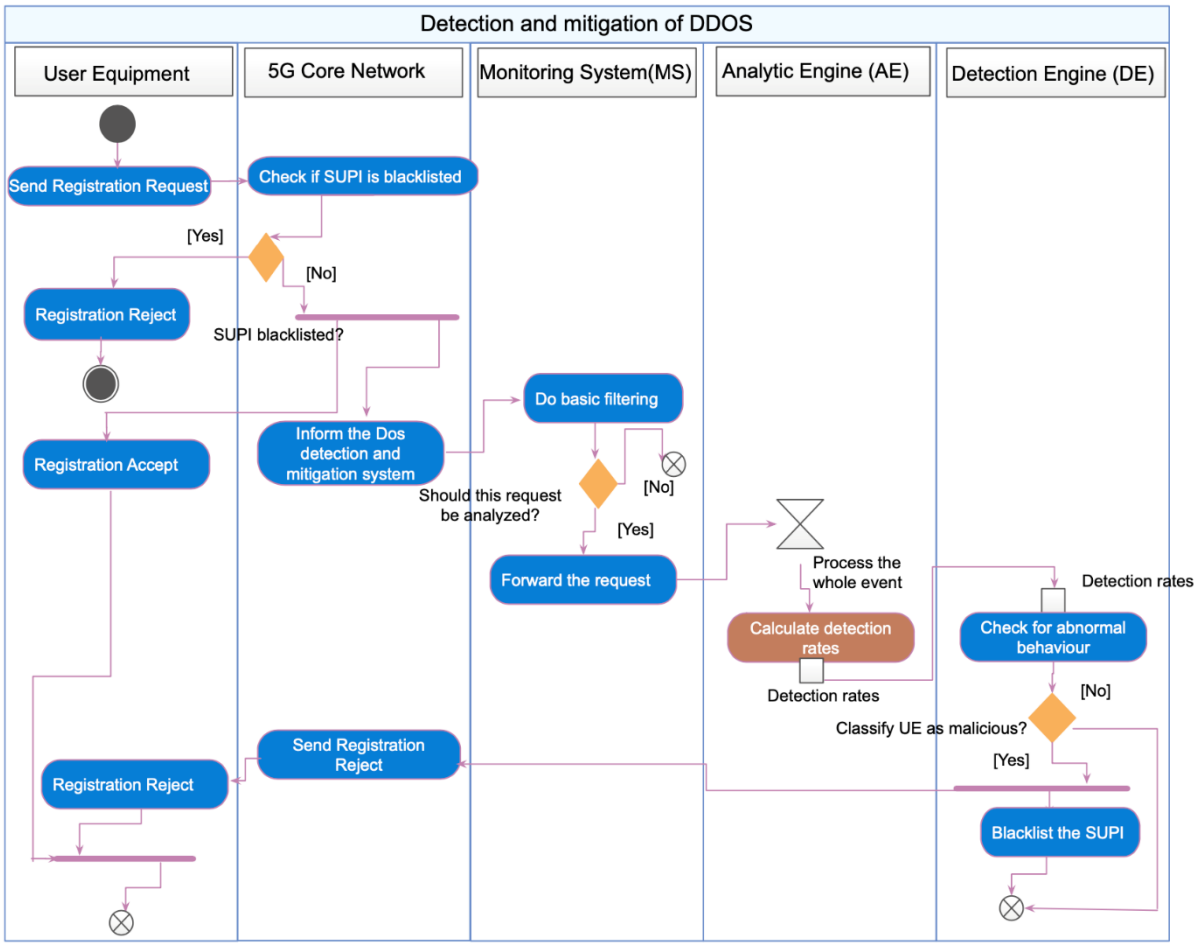


**Figure 2: Interaction of the mMTC network slice and the closed-control loop to detect and mitigate attacks**

Figure 2 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.

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.