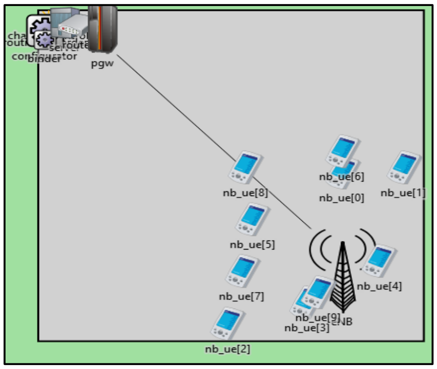
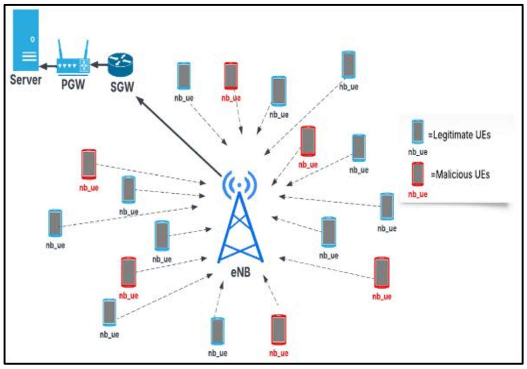
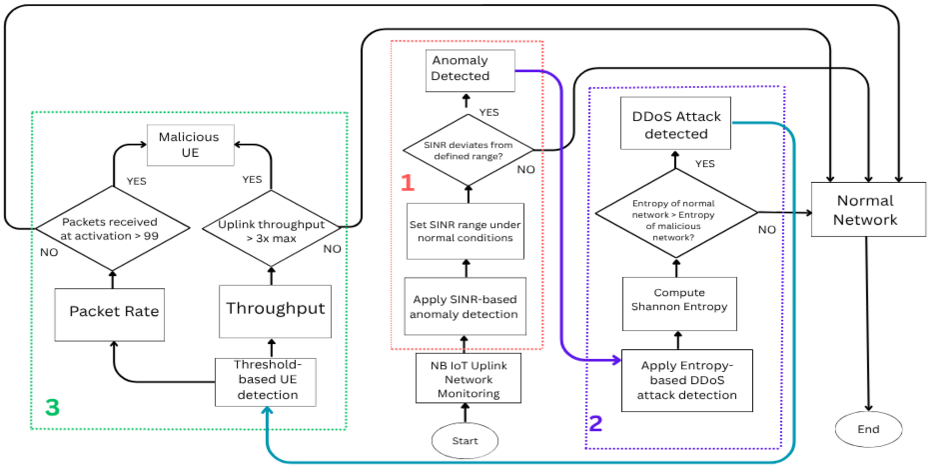
NED University of Engineering and Technology

Final Year Project Showcase Batch-2021
for the Year 2025

Department of Telecommunications Engineering
Name of Programme: Telecommunications Engineering

1	**Project Idea**	**Enhancing NB-IoT Network Security through Proactive Threat Detection** This project proposes a security framework for Narrowband Internet of Things (NB-IoT) networks that proactively detects cyber threats. Given the increasing use of NB-IoT in critical infrastructure such as smart cities, healthcare, and industrial systems, the vulnerability of these networks to Distributed Denial of Service (DDoS) attacks and other malicious intrusions is a growing concern. The project implements lightweight detection algorithms tailored for NB-IoT's constrained environments, offering an early warning system based on anomalous behavior in communication traffic.
2	**Process**	An uplink NB-IoT communication system was modeled in OMNeT++, using the INET and SimuLTE frameworks. The system was tested under three adversarial threat cases to evaluate its resilience against varying levels of network compromise: • Case I (33% Malicious Nodes): A low-intensity attack scenario with one-third of UEs behaving maliciously. • Case II (50% Malicious Nodes): A moderate compromise where half of the network was affected. • Case III (>50% Malicious Nodes): A high-intensity attack scenario with a majority of UEs acting maliciously. During each scenario, the simulation environment was used to monitor Key Network Performance Indicators (KPIs) such as SINR, throughput, and burst packet transmissions.Traffic data from the simulations was exported as CSV files and analyzed offline using Python. The detection techniques applied included Entropy-based anomaly detection, SINR deviation monitoring and Threshold-based evaluation as shown in Figure 1.
3	**Outcome**	The detection system successfully identified malicious behavior in all three threat scenarios with high accuracy and minimal false positives. It maintained network throughput and minimized performance loss, even when over 50% of nodes were compromised. A key innovation was the use of a hybrid model combining signal quality analysis and traffic entropy, enhancing detection precision. The system proved scalable, adaptable to different attack intensities, making it practical for real-world NB-IoT deployments.
4	**Evidence (Theoretical Basis)**	The project is grounded in a comprehensive literature review on DDoS attack trends and anomaly detection methods in LPWANs, particularly NB-IoT. The system was tested through simulations of urban macro-cell scenarios, replicating realistic network conditions. Detection algorithms were benchmarked across three threat levels (33%, 50%, >50% malicious nodes) to evaluate their performance. Results were also compared against a baseline setup to measure the extent of network degradation and the framework's ability to support recovery under attack.
5	**Competitive Advantage or Unique Selling Proposition** This project presents a practical, innovative, and scalable security solution tailored for NB-IoT networks. Its strength lies in a proactive threat detection model that not only addresses current security limitations but also aligns with global sustainability goals and industrial needs. The solution is cost-effective, compatible with existing infrastructure, and suited to a wide range of critical applications from smart healthcare to industrial automation making it highly attractive for industry adoption. Below are the selected aspects highlighting its competitive edge:	

a	**Cost reduction of existing Product**	- The use of simulated evaluation environments eliminates the need for expensive physical prototypes during development and testing. - The detection framework is fully compatible with existing NB-IoT infrastructure, avoiding any need for costly hardware upgrades or replacements.
b	**Process Improvement which leads to superior product or cost reduction, efficiency improvement of the whole process** (e.g. What is the issue is current process and what improvement you suggests)	- Current IoT security systems are largely reactive, leading to delayed threat responses and extended downtimes. - This project introduces a proactive detection approach, using lightweight algorithms that identify anomalies early reducing service disruptions and improving network resilience.
c	**Attainment of any SDG** (e.g. How it is achieved and why it is necessary for the region)	**SDG 8:** Decent Work and Economic Growth: Secure and reliable IoT networks contribute to safer industrial environments, enabling automation and digital growth across sectors. **SDG 9:** Industry, Innovation, and Infrastructure: The project enhances digital infrastructure by embedding security into NB-IoT systems that support smart industries.
d	**Expanding of Market share** (e.g. how it expand and what is the problem with the current market	By securing core functions of NB-IoT networks, the project supports market expansion into sensitive domains such as smart utilities, urban infrastructure monitoring, and digital healthcare, where security is a primary barrier.
e	**Capture new market (**e.g. Niche market or unaddressed segment**)**	Opens new potential in critical communication sectors such as emergency response systems, remote diagnostics, and industrial IoT, where built-in resilience and security are mandatory.
f	**Any Environmental Aspect** (e.g. carbon reduction, energy-efficient, etc.)	The detection algorithms are energy-efficient, aligning with NB-IoT's low-power operation model. This makes them ideal for battery-powered, long-lifecycle IoT devices, contributing to reduced energy consumption and sustainable tech deployment.
g	**Any Other Aspect**	No
6	**Target Market** (Industries, Groups, Individuals, Families, Students, etc) Please provide some detail about the end-user of the product, process, or service	The proposed solution caters to a diverse set of stakeholders across industries and sectors where secure and reliable NB-IoT communication is critical. The primary target markets include: - Telecommunications providers, IoT infrastructure developers, and cybersecurity firms seeking to enhance the resilience of NB-IoT networks. - Public sector organizations involved in the deployment of smart city initiatives, environmental monitoring, and utility management systems that rely on NB-IoT. - Academic institutions and research laboratories working on NB-IoT security, network optimization, and threat detection models for constrained environments.

7	**Team Members (Names & Roll No.)**	Syeda Mahum Arif (TC-21041): arif4430393@cloud.neduet.edu.pk Noor us Sabah (TC-21042): sabah4403287@cloud.neduet.edu.pk Adnia Nosheen (TC-21054): nosheen4430282@cloud.neduet.edu.pk Zainab Ishtiaq (TC-21055): ishtiaq4404164@cloud.neduet.edu.pk
8	**Supervisor Name**	Dr.M.Imran Aslam
9	**Supervisor Email Address**	iaslam@cloud.neduet.edu.pk
10	**Pictures (If any)**	 binder configurator pgw nb_ue[8] nb_ue[6] nb_ue[0] nb_ue[1] nb_ue[5] nb_ue[4] nb_ue[7] nb_ue[9] nb_ue[3] eNB nb_ue[2]  Server PGW SGW eNB nb_ue =Legitimate UEs =Malicious UEs Figure 1: Simulation Setup of NB-IoT Network using OMNeT++ Figure 3: NB-IoT Network Model under DDoS attack  Start NB IoT Uplink Network Monitoring Apply SINR-based anomaly detection Set SINR range under normal conditions SINR deviates from defined range? YES NO Anomaly Detected 1 Apply Entropy-based DDoS attack detection Compute Shannon Entropy Entropy of normal network > Entropy of malicious network? YES NO DDoS Attack detected 2 Normal Network End Threshold-based UE detection Packet Rate Throughput Packets received at activation > 99 Uplink throughput > 3x max YES NO Malicious UE 3 Figure 2: Multi-stepped Threat detection Methodology for NB-IoT Uplink Network
11	**Video (If any)**	N/A