ARTES 4000138681/22/UK/ND
A programme of and funded by the European Space Agency

jeans

JAMMING DETECTION AND MITIGATION FOR SATELLITE NETWORKS

The JEANS project aims to develop advanced techniques for detecting and mitigating jamming attacks in satellite IoT systems. Given the increasing vulnerability of satellite communications due to massive IoT device deployment, the project focuses on evaluating different IoT protocols and anti-jamming strategies.

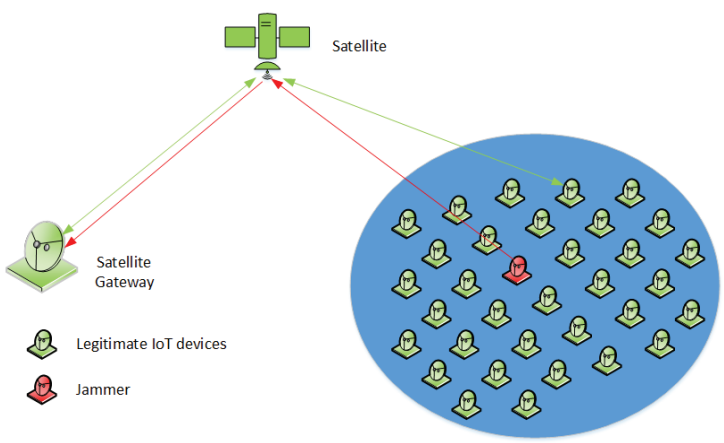
Key Tasks

- **Jamming Detection:** The project identified jamming attempts by analyzing system metrics such as throughput and receiver characteristics linked to the communication protocol. Detection algorithms were optimized to quickly identify jamming attempts with minimal complexity.
- **Anti-Jamming Techniques**: The performance of various anti-jamming strategies was evaluated to reduce the impact of these attacks, ensuring that communication and system performance remained intact.
- **Software Testbed Development**: A large-scale simulation environment was built to test the effectiveness of jamming detection and mitigation methods, enabling comprehensive performance evaluations under real-world conditions.

Performance evaluations

Two protocols, E-SSA and NB-IoT, were analysed for their resilience to common jamming attacks, such as preamble flooding and playback attacks.

Performance evaluations indicated that E-SSA outperforms NB-IoT in terms of jamming detection and mitigation. As a result, E-SSA was selected as the preferred protocol.



mbi
Politecnico di Torino
WISER

Main assumptions

The receiver is unaware of the intensity of the jamming signal. The jammer is partially aware of the IoT communication protocol, and can only target the uplink communication. The jammer's EIRP (Equivalent Isotropic Radiated Power) cannot exceed the legitimate terminal's maximum transmit power by more than 2 dB. Jammers can introduce malicious data flows unexpectedly and can carry out only one type of attack at a time. While the jammer can capture and decode broadcast signals, it cannot access encrypted communication from legitimate terminals.

Design and implementation

The design and implementation of IoT protocols E-SSA and NB-IoT focus on jamming detection and mitigation strategies. For NB-IoT, four types of NPRACH preamble flooding jammers are considered: single-tone (standard and non-standard) and multi-tone (standard and non-standard). Jamming detection uses average received power and a Neyman-Pearson test, while mitigation increases available subcarriers.

For S-MIM air-interface attacks, random preamble flooding and playback attacks are addressed.

Detection uses demodulation metrics and burst duplication checks. Mitigation involves a rolling preamble mechanism for flooding attacks and deleting duplicated bursts for playback attacks.

Achievements and lessons learned

Simulation results reveal **NB-IoT** vulnerabilities on the NPRACH, leading to potential Denial of Service (DoS) attacks. Pairing RA requests with information packets on the NPUSCH in energy-saving scenarios causes underperformance due to the NPRACH contention method. Modifying the RA format by sending information bits in the preamble is proposed to improve energy efficiency and resilience against jamming, while ensuring compatibility with other 3GPP standards.

For **E-SSA**, the following key outcomes have been achieved through simulations and validation on the verification platform:

- Effective detection of Random Preamble Flooding Attacks without overloading the receiver.
- The Rolling Preambles mitigation technique prevents overload and maintains performance if jamming is minimal.
- Random Playback Attack detection and mitigation successfully discard duplicates without overwhelming system resources.