**Denial-of-Sleep Attacks against IoT Networks**

**ABSTRACT**

Numerous medium access control (MAC) have been proposed for Low-power Lossy Networks (LLNs) over the recent years. They aim at ensuring both energy efficiency and robustness of the communication transmissions. Nowadays, we observe deployments of LLNs for potentially critical application scenarios (e.g., plant monitoring, building automation), which require both determinism and security guarantees. They involve battery-powered devices which communicate over lossy wireless links. Radio interfaces are turned off by a node as soon as no traffic is to be sent or relayed. Denial-of-sleep attacks consist in exhausting the devices by forcing them to keep their radio on. We here focus on jamming attacks whose impact can be mitigated by approaches such as time-division and channel hopping techniques. We use the IEEE 802.15.4e standard to show that such approaches manage to be resistant to basic jamming but yet remain vulnerable to selective jamming. We discuss the potential impacts of such onslaughts, depending on the knowledge gained by the attacker, and to what extent envisioned protections may allow jamming attacks to be handled at upper layers.

**EXISTING SYSTEM**

Slow channel hopping has recently gained much attention as it has been proved to combat efficiently narrow band noise [3], thus becoming highly common in industrial networks. As they allow to manage critical facilities (e.g., power grid, water treatment plant), these so-called Industrial Internet of Things (IIoT) networks require security at every layer of the communication stack, while inheriting vulnerabilities of classical IoT networks. Denial of service attacks are some of the security problems that must be tackled once deploying such IoT networks. Thus, energy awareness and security have become two interrelated challenges to be addressed.

**Disadvantages of Existing System:**

1. Denial of service attacks.
2. Security problems

**PROPOSED SYSTEM**

In this paper, we focus on the vulnerabilities of MAC solutions and the mechanisms they can embed to provide security by nature. We especially investigate physical jamming scenarios where attackers prevent communications from taking place, thus leading to further retransmissions and additional duty of the target devices. We detail some existing attacks before focusing on communication technologies which are being investigated by some of the main standardization bodies. We consider time-synchronized and channel hopping (TSCH) networks that are being designed for industrial wireless devices. Those solutions minimize the risks of collisions and reduce idle listening, while providing some cryptographic suites to ensure authentication and encryption if needed. We describe how some Denial-of-Sleep attacks could yet be successful over such networks. We anticipate their potential impact, depending on the knowledge an attacker would be able to gain. Some preliminary simulation results show how various scenarios of selective jamming can perform against TSCH networks.

**Advantages of Proposed System:**

1. Proposed system can provide security by nature.
2. Minimize the risks of collisions.
3. Reduce idle listening

**SYSTEM IMPLEMENTATION**

**SYSTEM REQUIREMENTS**

# Hardware Requirements:

# Processor - Pentium –IV

* Speed - 1.1 GHz
* Ram - 256 MB
* Hard Disk - 20 GB
* Key Board - Standard Windows Keyboard
* Mouse - Two or Three Button Mouse
* Monitor - SVGA

**Software Requirements:**

* Operating System - Windows XP
* Coding Language - Java