Latency Shift Keying for IoT Connectivity

ID: 2024-033

Executive Statement:

A groundbreaking method to secure communications between untrusted IoT devices and trusted networks using network latency.

Description:

Wireless Latency Shift Keying (LSK) is an innovative communication technique that modulates data through network latency, allowing secure data transmission between untrusted wireless devices and a trusted network without full network access. By manipulating packet latency, LSK encodes and transmits data without conventional network rights, leveraging existing WiFi hardware and software implementations. The technology is exemplified through Wicket, an application that dynamically manages network spaces for IoT devices, enhancing security without hardware modifications.

Key Advantages:

- Enhances security for IoT devices within home networks.
- Operates with existing WiFi hardware, requiring no physical modifications.
- Facilitates secure communication without granting full network access.
- Dynamic management of network connections through Wicket application.
- Maintains low bit error rates across varying network conditions.

Problems Solved:

- Security risks associated with integrating untrusted IoT devices into home networks.
- Vulnerability of IoT devices being exploited for cyberattacks or as botnet components.
- Conventional WiFi security models' limitations in offering either complete trust or lack thereof.
- Provides an option to connect sensors to wireless networks without an initial setup.

Market Applications:

- Secure network communication for smart home devices.
- Enhanced security protocols for IoT devices in sensitive environments.
- Network security solutions for consumer and enterprise IoT applications.
- Communication technologies for untrusted devices within trusted networks.