Case Study

SE*link*™

Network Lockdown Strategies for Sensors in Critical Environments

Background

Wireless and wired sensors networks are an important aspect of law enforcement and military networks. An array of sensors of many different modalities (including RF, video, acoustics, biological, chemical and thermal) are used in several contexts, to defending sensitive installations such as military bases or strategic infrastructures, detecting and tracking movements of potential threats. Sensors may also be mounted on airborne blimps or surveillance aircraft to collect information while flying over an area under observation. Through distributed coordination, WSN are envisioned to enhance situational awareness and improve the effectiveness of law enforcement and military operations. Nevertheless, these advancements pose challenges in processing extensive data within bandwidth-limited, power-constrained, and dynamically changing environments.

Challenge

In general, sensor networks present significant technical challenges related to data processing, communication, and sensor management. The dynamic and potentially harsh environments, coupled with energy and bandwidth constraints, add further complexity to wireless ad hoc networks, posing challenges in network discovery, control, routing, collaborative information processing, querying, tasking, and security. Deploying sensor nodes in unattended environments exposes networks to various potential attacks, while the inherent power and memory limitations of sensor nodes render conventional security solutions impractical.

Industry

Law Enforcement and Military Sensors' Networks

Challenges

- Security
- Quality of Service
- Scalability
- Energy Efficiency
- Remote maintenance

Goals

- Implementing a cost-effective virtual networking solution for optimised low-speed applications, supporting devices with limited computational and communication resources, while enhancing cyber resilience against security threats.

Solution

SE*link*™ provides a zero trust security model combined with service-level virtual network segmentation, granular privileged access management. Delivering efficiency, security and control to Devices and Networks in a single solution.

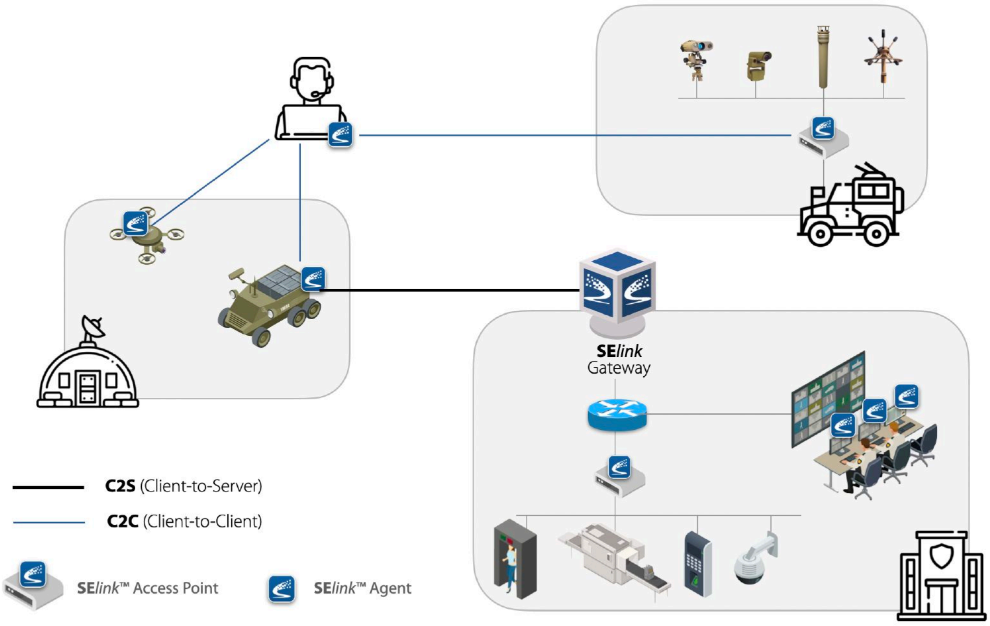
Solution

Building a sensor trust model to solve the problems beyond the capability of cryptographic security of wireless sensor networking applications requiring trust to maintain proper network functionality.

SE*link*™ is a **Zero trust virtual networking** solution for private networks based on the **Assumed Breach model** for the **Resilience** and optimisation of distributed endpoints (devices, users) and sites (Bases, camps, HQ). It is able to replicate heterogenous clients and server behaviours in a seamless way, as in a private LAN; when field sensors communicate with each other or send data to the Command Operation Center (COC) server through SE*link*™, they are all virtually relocated in the same COC server LAN. The **SElink™ Gateway performs Sensors "virtualisation"**, showing to the server the original MAC address and a unique, registered, identifier for each sensor. The advantages are overwhelming. SElink™ protects both the data channel and the access to the communication channel, which can only be used by authorised processes. **Access requests are continuously validated** for finely-tuned access to specific applications and services, compliant to user's needs and privileges. **Zero Trust principles** minimise the need for traditional detection systems. **Network lockdown strategies closing all inbound ports** on each network node by default, make that **all packets** from **unauthorised client applications are dropped**. Devices affected by vulnerabilities, even without vendor knowledge, are at risk of infecting the network provider with major infrastructural risks and significant potential damage. **Native anti-propagation mechanisms** prevent infection spreading. This ensures that the Command Center server is protected even in the event that the sensor is compromised. Sensors would no longer need public static IP addresses to the benefit of a reduction of the attack surface. Lightweight protocols and zero encryption overhead are featured benefits of SE*link*™ as band availability and integration of security is no longer a limit. Easy to be integrated in any environment, over any protocol, portable, multi-device with the benefit of crypto-agility for systems longevity. **Post Quantum Cryptography** ensures the highest level of security in authentication mechanisms.

Benefits for Resilience

1. **Zero Trust Network Access and Assumed Breach model** strategies
2. **Lightweight protocols** for bandwidth sensitive and resource-constrained devices
3. **Zero Encryption Overhead** compared to TLS/SSL
4. **Free from third-party vendor dependancies** for the integration of security into heterogeneous devices
5. **Enhanced system longevity and resilience** to quantum attacks
6. **Seamless encryption updates, redesign-free** through Crypto agility
7. **Rationalisation of operational costs:** NO VPN, NO PKI infrastructures, NO public/static IP addresses
8. **Efficiency and ease of management**


SE*link*
Gateway
C2S (Client-to-Server)
C2C (Client-to-Client)
SE*link*™ Access Point
SE*link*™ Agent