Case Study

Improving Access control and Quality-Of-Service over bandwidth-limited Satellite Communication Networks

Background

Satellite communication is a growing market worth USD 131.68 billion, globally, expected to experience an annual growth of 9.10% by 2028* due to its prevalent applications across various industries. The increasing maturation of this industry's technology has attracted government interest and company investments in services ranging from national defence to media broadcasting. Furthermore, satellite operations has been proven essential in the function of critical infrastructures, particularly when responding to emergency situations. Considering the increasing demand in data transfer and communications, satellite networks will likely integrate with IoT devices to create the new generation of mobile satellite networks, built to provide anytime-anywhere communication services. This integration will inevitably expose satellite systems to the cyber security risks that come with extensive connectivity and expansive attack surfaces.

Challenge

There are many challenges to resolve in the security of the satellite network industry. The operational system has many open design problems that negatively impact the Quality-of-Service (QoS) and user experience. Currently, the primary focus of vendors is to provide services with high data rates and low latency. Adding security protocols is treated as an undesirable overhead that increases power consumption and memory usage. The absence of cyber security systems, particularly during the manufacturing process, remains an overlooked weakness generating insecure protocols and weak authentication mechanisms.

Industry

Satellite Communication Networks

Challenge

- The increasingly complex integration of satellite networks, coupled with poor encryption protocols, makes it harder to protect traffic data from threat actors

Goals

- Reduce the surface of attack across space, ground, user and link
- Improve QoS and bandwidth consumption
- Seamless security integration into multivendor devices
- Strengthen access control mechanisms for isolation and protection against supply chain attacks
- Implement network virtualisation for smoother integration of sat components into 5G systems

Solution

SE*link*™ provides a zero trust security model combined with software-defined network segmentation and whitelisting practices. Delivering Data, Device, Network Security and Control in one single solution

Solution

Security is a mandatory requirement for satellite networks. Satellite technology provides low and limited network bandwidth resulting in network congestion, reduced Quality-of-Service (QoS) of applications and late packet delivery issues. This may cause the loss of synchronisation, therefore a careful evaluation of encryption systems is required to prevent Quality of Service degradation and unnecessary bandwidth consumption due to security processing.

SE*link*™ is a service-oriented, secure, virtual networking solution to protect end-point and network alike. Able to replicate heterogenous clients and server behaviours in a seamless way, as in a private LAN; when a satellite device is connected to the Terrestrial Network Operation Center (NOC) server through SE*link*™, it is virtually relocated in the same NOC server LAN.

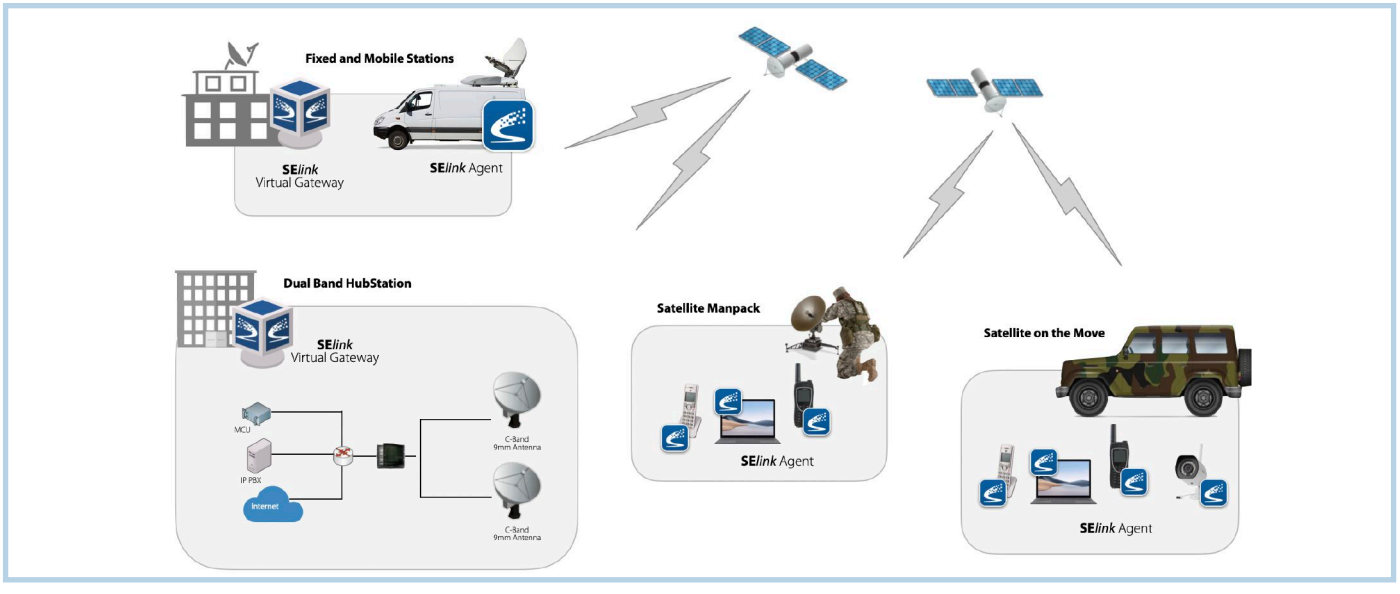
The SElink™ Gateway performs satellite terminals "virtualisation", showing to the server the original MAC address and a unique, registered, identifier for each Satellite device in the network.

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 controlled by Zero Trust Access mechanisms confining malware to its origin. This ensures that the Ground Station server is protected even in the event that the satellite device is compromised, for example in the event of a supply chain attack. Satellite devices no longer need public static IP addresses to the benefit of a reduction of the attack surface as well as operational costs. Lightweight protocols and zero encryption overhead make the integration of security into bandwidth sensitive devices no longer an issue, making resource utilisation efficient, allow the optimal response and guarantee target performance to the most TCP/IP services. Smart mechanisms such as automatic session recovery, packets aggregation over the same packet header and TCP header overhead reduction prevent packet filtering from providers and improve service availability. Easy to integrate in any environment, over any protocol, portable, multi-device with the benefit of crypto-agility, SE*link*™ security techniques, are resilient and resistant to quantum computing attacks.

Benefits

1. **Zero Trust Network Access and Assumed Breach model** strategies
2. **Lightweight protocols** for bandwidth sensitive and resource-constrained devices
3. **Low-bandwidth strategies coupled with smart mechanisms** to improve QoS and availability of service
4. **Zero Encryption Overhead** compared to TLS/SSL/IPSec
5. **Free from third-party vendor dependancies** for the integration of security into heterogeneous devices
6. **Seamless encryption updates, redesign-free** through crypto agility
7. **Rationalisation of operational costs:** NO VPN, NO static IP addresses, required
8. **Efficiency and ease of management**

** Source: Verified Market Research "Satellite Communication (SATCOM) Market Size And Forecast"*



Blu5 Group
info@blu5group.com
www.blu5group.com