Case Study

Optimising connectivity and security to rural areas over TV White Space networks

Background

Universal Internet access is part of the UN's sustainable development goals, and despite a strong global growth in the use of the Internet has been recorded (from 4.1 billion in 2019 to 4.9 billion in 2021), ITU confirms that among the 4.9 billion Internet users, many hundreds of millions lack broadband access, sensibly limiting the usability of their connection. This is often due to a lack of infrastructure, large distances and dispersed populations. Providing connectivity and Internet access to a number of rural businesses and communities, in challenging terrain, remain a priority for the global development. Wireless technologies like the TV White Spaces (unused broadcasting radio frequencies) promise to overcome the shortcomings of existing short multi-hop wireless architectures and protocols by offering more availability, wider bandwidth and longer-range communications.

Challenge

TV White spaces are the enabling technology for sensing, monitoring, IoT, wireless broadband access, real-time and smart utility applications. Despite all the benefits of TV white space networking, several key challenges associated with wide availability, diverse bandwidth and longer communication range need to be addressed properly: interference mitigation, handoff and spectrum mobility, QoS throughout heterogenous networks, proper security to ensure safety in TV white spaces networking protocols. TV White space protocols currently being developed lack proper security measures.

Industry

TV White Space Wireless Communications

Challenge

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

Goals

- Manage and optimise the performance of wireless networks through network virtualisation
- Guarantee optimal quality of service
- Reduce the surface of attack across networks, users and links
- Seamless security integration into heterogeneous networks
- Strengthen access control mechanisms for isolation and protection against supply chain attacks

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

TV white spaces' characteristics make them suitable for long range, low-power, and large area applications such as sensing and monitoring applications, agricultural IoT applications, wireless broadband access, real-time applications, smart and connected communities. Applicability of TV white spaces to long range communications however require high bandwidth, less interference, energy efficiency and inexpensive communication protocols to develop highly scalable wireless communication networks.

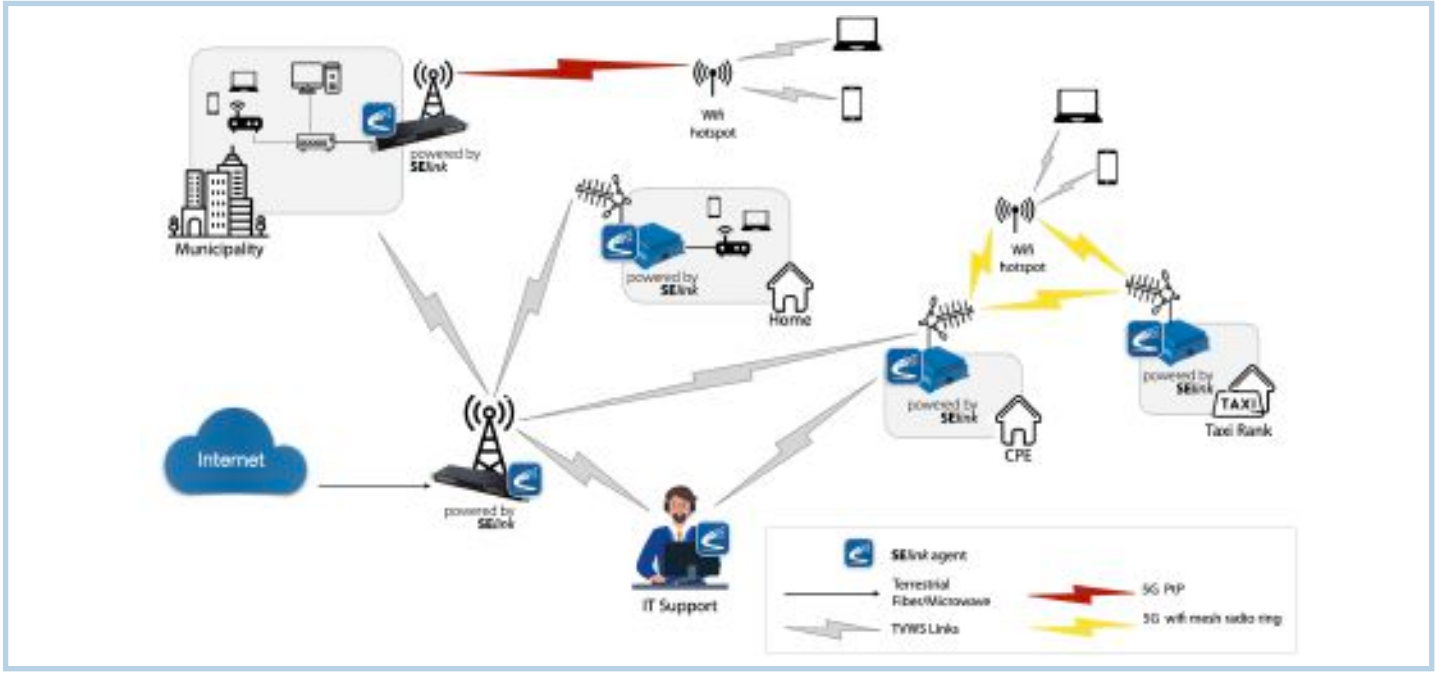
SE*link*™ is a service-oriented, secure, virtual networking solution to protect end-point and network alike. Able to replicate heterogenous clients and server behaviours in a seamless way, as in a private LAN; when a device is connected to the TVWS Access point through SE*link*™, it is virtually relocated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

The SElink™ Gateway performs network "virtualisation", showing to the TVWS Access point the original MAC address and a unique, registered, identifier for each device in the network.

The advantages are overwhelming. SElink™ protects 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 TVWS Access Point is protected even in the event that the field device is compromised, for example in the event of a supply chain attack. Network 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 networks
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. **Network agnostic** for easy integration into heterogeneous networks
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**



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