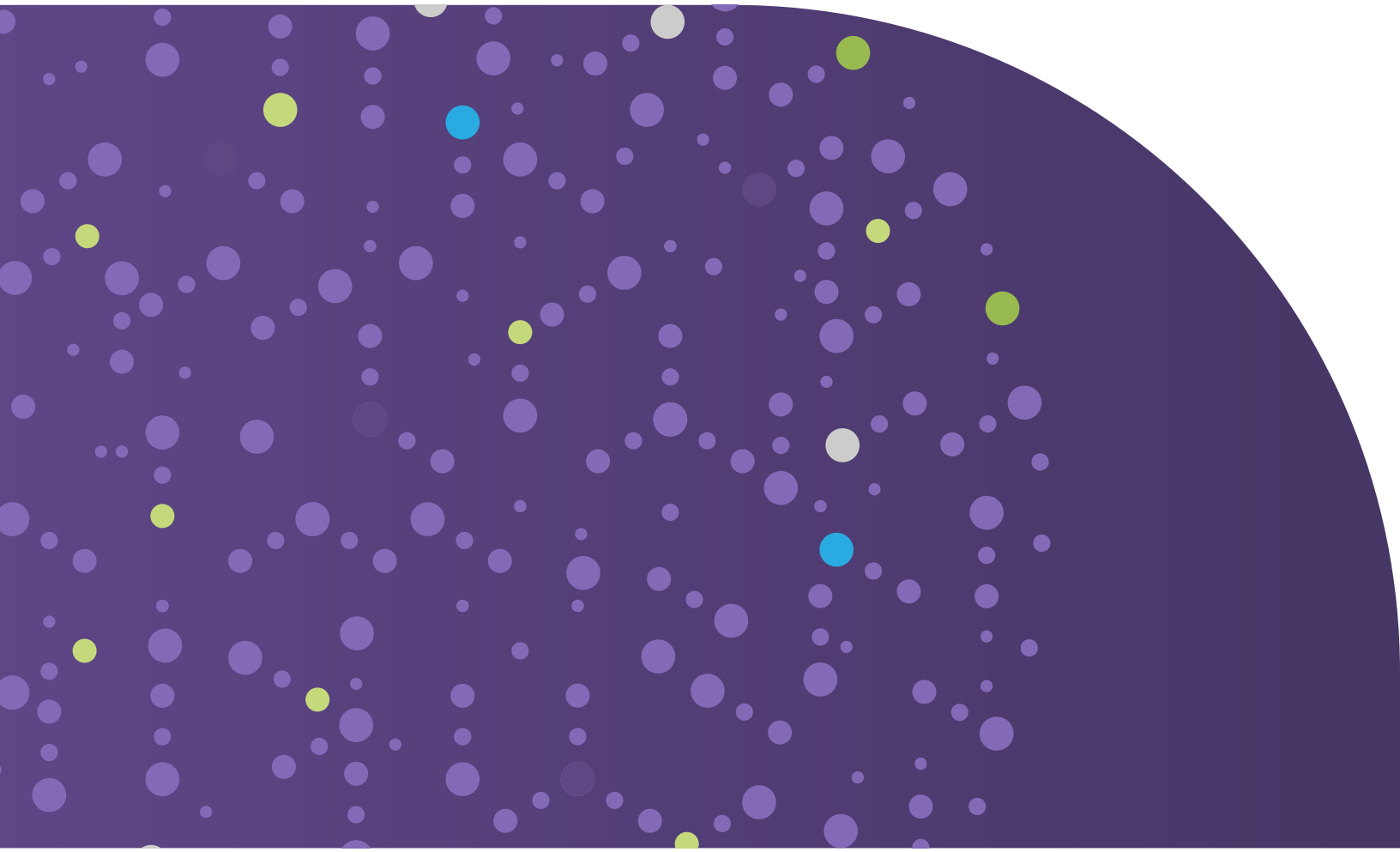
REMOTE MANAGEMENT & CONTROL FOR SMART AMPLIFIERS

Comparing the options for MSOs



AOI QUANTUM BANDWIDTH®

eBook

INTRODUCTION

The Benefits and Risks of Smart Amplifiers

The introduction of Smart Amplifiers brings forth many efficiencies and operational savings from amplifier setup and diagnostic information. With these benefits come challenges that need to be managed well. Smart amplifiers require processing and firmware that has never been seen in amplifiers, which allows for the ease of automated setup and balancing but also adds a new set of failure points. Imagine deploying cable modems without being able to do remote and mass firmware upgrades -- this would not happen. A similar risk applies when deploying smart amplifiers without including remote management, which has the ability to do remote firmware upgrades. The cable industry is realizing that any firmware issue without remote control and management would cost hundreds of millions and will severely impact customer satisfaction. Therefore, operators and vendors are working together to create a standard for transponders and controllers that allow remote management, control, and upgrades of smart amplifiers.

Recognizing the critical role of remote management capabilities in deploying smart amplifiers, it is important to understand and compare the underlying technologies that facilitate it. The technologies at the forefront are LoRaWAN and HMS (Hybrid Management Sub-Layer), each presenting distinct approaches and advantages. Understanding the technologies is vital for cable operators as they navigate through the options and make informed decisions that align with their network's operational needs and strategic goals. Particularly, how LoRaWAN can be an effective remote management technology due to its robust features and implementation benefits.

UNDERSTANDING LoRaWAN

LoRaWAN is an innovation designed for low-power, cost-effective implementations where interoperability is required, and it has been deployed in millions of telecommunication endpoints. It excels in scenarios requiring virtualized control with deep penetration and broad coverage of endpoints, like elements of a cable network, due to its ability to maintain strong signal integrity over long distances and through physical barriers -- qualities essential for expansive and complex network environments. The technology leverages robust modulation schemes, such as FSK, making it ideal for HFC networks where noise ingress from multiple sources is a constant threat.

Open Source

LoRaWAN's status as an open-source technology significantly enhances its appeal to cable providers. This open-source nature fosters a dynamic, collaborative environment that fuels innovation and adaptability. For cable operators, it means access to a platform that's continuously refined by a global community, ensuring a versatile and future-proof solution. Furthermore, LoRaWAN's widespread adoption across various sectors underscores its reliability, with a substantial user base and extensive real-world applications providing concrete evidence of its effectiveness and robustness in diverse operational scenarios.

In practical applications, LoRaWAN provides a reliable and secure connection to multiple endpoints. Its strengths are manifested in remote monitoring and management tasks within HFC networks. It's particularly adept at remote firmware pushes, fault detection, efficient operational management, and predictive maintenance, underlining its utility in enhancing network performance and reliability.

UNDERSTANDING LORAWAN

Advantages of LoRaWAN

LoRaWAN's primary advantages are its open-source design, with global collaborators constantly refining functionality, and its inherent security, which has been deployed across millions of endpoints worldwide. Its open protocol nature ensures seamless interoperability across various devices and networks. Additionally, its ability to manage thousands of end nodes over vast areas with secure, bi-directional communication makes it a robust choice for expansive network operations.

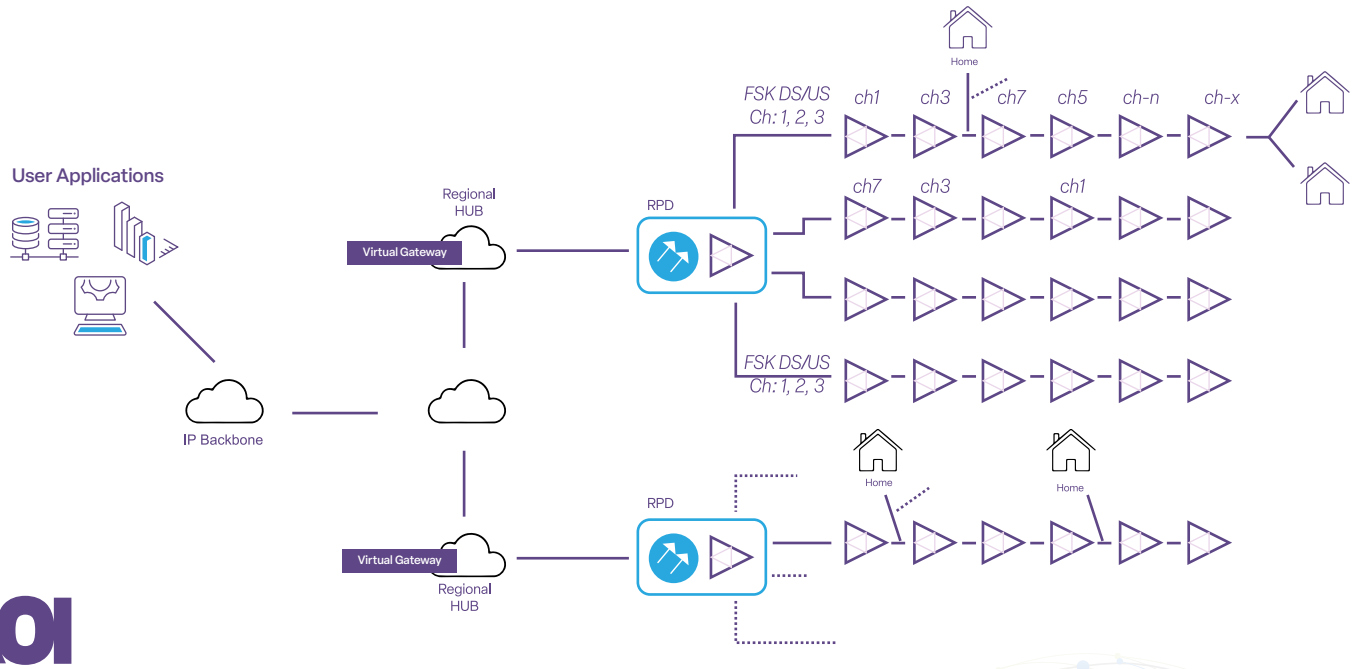
Limitations and Considerations

LoRaWAN is only limited by design restrictions. For use in HFC networks, it must be clear whether end users want to use SCTE 25-1[1] transmission, NDR/NDF[2] transmission, or both. These decisions will determine the optimum transponder design and data transmission rate capabilities.

[1] SCTE 25-1 is a physical layer specification that uses FSK as the modulation scheme. This uses UART style protocol to transfer 38.4 kbps of LoRaWAN data between the transponder and the controller.

[2] NDR/NDF is Narrowband Digital Return and Narrowband Digital Forward technology. This digitizes an analog portion of the US and DS spectrum that can be processed at the headend. NDR/NDF can be used to carry multiple FSK modulated signals, allowing one to support multiple 40kbps LoRaWAN data channels between the transponder and the controller.

LoRaWAN Network Architecture in HFC



UNDERSTANDING HMS

Introduction to HMS

The HMS subcommittee under the SCTE developed a suite of specifications to monitor the HFC network outside plant elements. It details the physical and data link layer protocols, the core message set, and the transponder electromechanical interface can be based on the SCTE 25-3. Although this spec specifically defines electromechanical interface requirements between a power supply to transponder interface bus.

HMS Features and Strengths

HMS is a standards-based protocol that leverages UART-based transport. HMS is a bespoke set of specifications for use in cable operations and has proven to be a cost-effective means of monitoring products for CATV networks. HMS also supports diagnostic capabilities that enable monitoring and troubleshooting of network issues. This includes the ability to perform status checks and diagnostics on network equipment.

Challenges in HMS Implementation

The significant challenges in implementing HMS center around its proprietary, single-source nature and lack of security. Only one HFC vendor is working on a modified version of HMS which is currently missing a defined security protocol.

COMPARING LORAWAN & HMS

Scalability and Network Coverage

LoRaWAN and HMS provide virtualized control that integrates into cable operators' northbound EMS and network management systems. They both leverage a modulation scheme for transponders that optimizes performance in noisy cable networks while maintaining data transmission integrity.

Security and Data Integrity

LoRaWAN ensures secure data transmission with robust security measures built into the system. The fundamental properties of LoRaWAN security include mutual authentication, integrity protection, and confidentiality. Application payloads are encrypted end-to-end using a 128-bit AES key, which offers users a high level of security by protecting data from unauthorized access and ensuring that the data remains intact and confidential throughout its journey from sender to receiver.

HMS does not offer integrated security encryption in its current instance. As of the publishing of this paper, there are ongoing discussions between an HMS provider and cable operators to define the best security option moving forward.

Power Consumption and Efficiency

Both LoRaWAN and HMS will use FSK modulation in their transponders, which results in very low power consumption (<1W) while still providing efficient and reliable data transmission.

Technology Comparisons

At a high level, the implementation of LoRaWAN is quite similar to HMS. However, the major difference lies in the embedded security and technology advancements from multiple global participants in LoRaWAN Open Source, compared to HMS, which has only a single contributor. As a result, interoperability can be a challenge with HMS.

Looking into the specifics reveals that LoRaWAN has the advantage of being continuously improved over the last decade. On the other hand, HMS was initially conceived in 1996, when there were not many FSK chipsets available. Some of the advantages of using FSK modulation with reliable packet structure at a cost-effective price have not been realized. Although SNMP is still widely used in the industry, modern data collection techniques are moving away from SNMP and are adopting more advanced data collection techniques such as streaming telemetry.

FEATURE	LORAWAN	HMS
STANDARDS BASED	Yes	Yes for MAC and PHY. No for application elements
COST	Low	Low
POWER CONSUMPTION	Low	Low
PROVISIONING AND ACTIVATION	Yes (Open-Source SW Available)	Not Specified
APPLICATION	Used in agriculture, smart cities, remote monitoring	For Cable Headend Plant Based Devices
SECURITY	Yes	No
OPEN SOURCE SW ELEMENTS	Yes	No
OVERALL COMPLEXITY	Low	High

The Advantages of LoRaWAN

Embedded Security and Open-Source Differentiation

LoRaWAN distinguishes itself with its robust embedded security and constant innovation resulting from global contributions to its open protocol code base. LoRaWAN is an open-source telecommunications standard, not an adapted cable standard, with limited contributions by a single vendor. LoRaWAN's security architecture is robust, employing end-to-end encryption to ensure data integrity and prevent unauthorized network access. This is crucial for maintaining the confidentiality and security of network management data. Using unique network keys for each device further reinforces this security, making LoRaWAN a reliable choice for critical infrastructure.

Cable Operator Risk & Insurance Policy

From a financial standpoint, LoRaWAN presents multiple use cases that will provide operational savings to MSOs. From remotely pinpointing ingress and mitigation or predictive AI applications allowing preventative maintenance before outages exist to virtual and real-time design maps with geo-locations, there are endless use cases. However, beyond these benefits, LoRaWAN also acts as an operational safeguard. Should a firmware issue arise, it can be addressed immediately and cost-effectively through remote updates. Without this capability, operators would incur significant costs and operational disruptions, as physical site visits for firmware installations across numerous amplifiers would be required. Operators deploying smart amplifiers without this insurance policy may reap the benefits of this new technology; however, they also take on massive risks.

Conclusion

In this review of the remote management & control of HFC amplifiers, we've outlined two viable solutions with their unique advantages. LoRaWAN, with its vast contributors and strong security, emerges as a particularly compelling option for operators seeking efficiency and reliability.

Let AOI guide you through this pivotal journey into the future of remote management. For more information on AOI's LoRaWAN-based QuantumLink, VISIT HERE.