Avnu Alliance® White Paper

Industrial Wireless Time-Sensitive Networking: RFC on the Path Forward

Version 1.0.3 – Friday, January 5, 2018

Authors:

Stephen F Bush (GE Global Research)
Chair: IEEE P1913 - Software-Defined Quantum Communication
Chair: 1906.1-2015 - IEEE Recommended Practice for Nanoscale and Molecular Communication Framework
Guillaume Mantelet (GE Transportation)

Contributors:

Brant Thomsen (Harman International)
Ethan Grossman (Dolby Laboratories)

Executive Summary

This white paper explores thoughts on a roadmap for wireless Time-sensitive Networking (TSN) in an industrial environment. Wired TSN for industrial use is undergoing acceptance and deployment. The next challenge will be developing seamless, wireless TSN capability. This document shows how to leverage the existing industrial wired TSN design for wireless TSN. This document is to be considered a request for comments; constructive corrections, ideas, and comments are very welcome by the author. Please contact wirelesstsn@avnu.org with comments.

About Avnu Alliance

The Avnu Alliance is a community creating an interoperable ecosystem of low-latency, time-synchronized, highly reliable networked devices using open standards. Avnu creates comprehensive certification programs to ensure interoperability of networked devices. The foundational technology enables deterministic synchronized networking based on IEEE Audio Video Bridging (AVB) / Time Sensitive Networking (TSN) base standards. The Alliance, in conjunction with other complimentary standards bodies and alliances, develops complete solutions in professional AV, automotive, industrial control and consumer segments.

Table of Contents

Introduction

Wireless communication in industrial communication systems are beneficial for many obvious reasons including reduced wiring cost and complexity as well as enabling mobility. However, because industrial systems involve life-critical control systems that may be lethal if they become unstable, approaches toward adopting wireless communication tend to be very conservative. It should be clear that reliability is *sine qua non*, regardless of whether communication is wired or wireless.

The term "wireless" in this document is used in the broadest possible sense and includes free-space optical, Li-Fi, Bluetooth, 802.11g/n etc., small (nano, pico) cells: 3G, 4G, LTE, and includes anything else that involves information transfer using the electromagnetic spectrum, including various forms of visible and invisible light, i.e. free-space optical. This document is agnostic as to the wireless technology or technologies used.

Note that Li-Fi stands for Light Fidelity. It is a wireless, bidirectional, optical form of communication that leverages unused visible spectrum reducing load on radio spectrum. Data is transmitted using light whose intensity varies faster than the human eye can detect. Li-Fi uses LED bulbs with a transceiver, and data transmission can be faster than is possible with Wi-Fi.

Industrial systems are comprised of large, complex infrastructure equipment that evolves slowly relative to consumer market devices. Thus, given that wired TSN is undergoing deployment into industrial systems, wired TSN should leverage and integrate seamlessly with wireless TSN. The Theory of Operation for wired TSN should be used to leverage equipment, skill, and development to increase "pull" for wireless into industrial systems.

This document is **not** about developing new technology for wireless TSN, but rather pulling existing wireless technologies under the TSN umbrella and developing a common Theory of Operation. Thus, this white paper is designed to be top-down rather than bottom-up. Finally, this document sketches a roadmap for integrating wireless communication into industrial systems and identifies standards and technology gaps.

Roadmap

The roadmap for integrating wireless TSN into industrial TSN systems takes a conservative, phased approach allowing confidence in reliability of wireless TSN to be gradually increased. The phases are:

(1) Wireless Configuration of Wired TSN

(2) Hybrid Wired-Wireless Time Synchronization

(3) Wireless TSN Scheduling

(4) Wireless Redundancy for Wired TSN

(5) Wireless TSN Switch Deployment.

Each wireless technology would proceed through these phases and NETCONF/YANG management of all phases is mandatory.

Phase 1: Wireless Configuration of Wired TSN

This phase simply implements wireless communication to configure existing wired TSN. This is confined to actions taken by the Centralized Network Configurator (CNC) and the Centralized User Configuration (CUC) processes, including configuration of TSN schedules. These are actions that take place before a system becomes operational and while reliability issues would be an annoyance, they have no life-critical impact because this is configuration, not operation. It is assumed that wireless configuration can communicate with all required hosts in the TSN network.

The use-case for this phase is that a field engineer may utilize a wireless tablet to change the network configuration or retrieve diagnostic information. Augmented reality may be considered at this point as another wireless TSN application. For example, the field engineer may see virtual gauges, status, and other information overlaid on the real equipment as the information becomes relevant to the current task.

This phase is relatively easy and straight-forward; there appears to be no technical or standardization

gap in this phase. Figure 1 shows the wireless communication links for this phase as dashed lines. It should be noted that cybersecurity remains critical in a wireless system, as equipment can be moved and replaced without accessing physical connections.

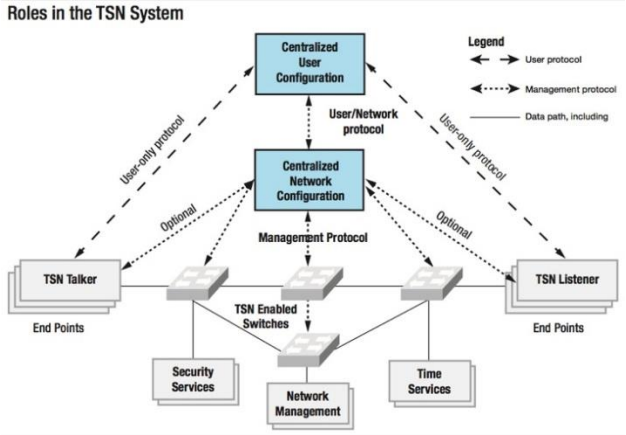

Fig 1 Wireless Communication Links in Phase 1 are Dashed Lines.

Phase 2: Wireless Time Synchronization

The next phase is to integrate wireless gPTP with wired gPTP such that the wireless portion of a hybrid wired-wireless can rely upon reliable wired time synchronization. The concept for this phase of wireless TSN is that all wireless channels have the benefit of reliable time synchronization.

Thus, this phase uses the wired node as an access point with a wired clock and wireless devices may synchronize with it. Wireless devices not on the wired network may use Timing Measurement or Fine Timing Measurement to synchronize; deterministic networking is not considered until Phase 3.

Using Timing Measurement (TM) for wireless synchronization is defined in Clause 12 of the IEEE 802.1AS-2011 specification. Fine Timing Measurement (FTM) is defined in the IEEE 802.11-2016 specification, and synchronization using FTM is described in the IEEE 802.1AS-Rev draft, which is expected to be finalized in 2018.

The gaps in this phase are:

(1) Can the wireless devices use wireless gPTP to synchronize tightly enough with devices that use wired gPTP time synchronization?

(2) Is it feasible to use GNSS only (wired GNSS grandmaster and GNSS for each wireless device) and not require 802.1AS wireless support? (See Appendix A)

Figure 2 illustrates wireless time synchronization. Master clocks must be wired interfaces and wireless interfaces should be slaves in this phase.

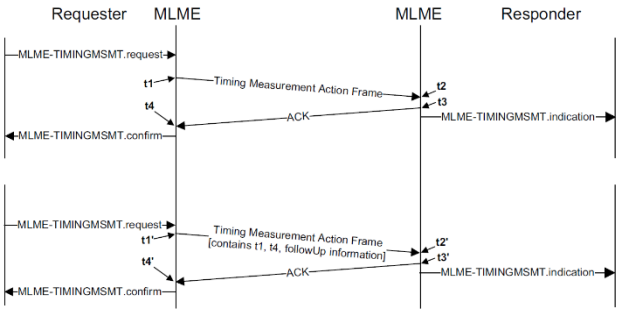

Fig 2 Phase 2 Time Synchronization with wireless TSN.

However, this does not preclude testing with a GNSS receiver enabling a wired or wireless gateway to become a grandmaster as described in 802.1AS Figure 7-1, Figure 7-2, pp. 20 – 21.

Phase 3: Wireless TSN Scheduling

Wireless TSN interfaces must support the semantics of IEEE 802.1Qbv; deterministic traffic is required for industrial systems, so this will be mandatory. Phase 3 simply ensures that 802.1Qbv scheduling is implemented in wireless TSN interfaces as illustrated in Figure 3.

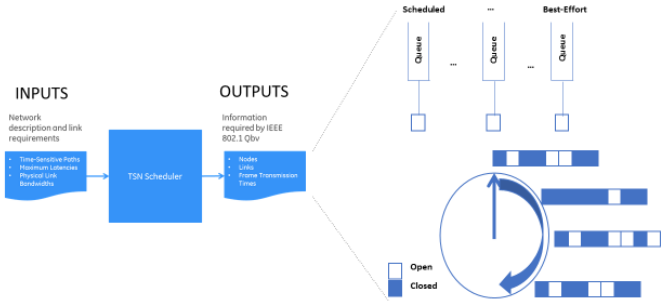

Fig 3 Phase 3 Time Synchronization with Wireless TSN.

This white paper is agnostic as to the specific wireless technologies used. However, the point of TSN is to control message transmission time. Thus, wireless TSN interfaces must be able to implement an 802.1Qbv schedule compliant with the IEEE 802.1Qbv standard, with no other transmission except that specified by the schedule. The CNC will ensure that no collisions take place and the wireless system will benefit greatly from this.

Such a wireless system, having the benefit of wired time synchronization and a deterministic schedule from the CNC, will eliminate data traffic frame collisions on the network. It is recognized that surround networks and the environment can still cause interference, affecting determinism. Note that industrial systems tend to use only scheduled (TT) and best effort (BE) traffic types; rate constrained (RC) traffic offers no apparent benefit for control system communication now. Note that this does not preclude audio/video from being added to a control network if it is certain not to impact reliability.

The fact there are no wireless frame collisions as part of TSN data traffic is significant and helps enable the wireless system to be deterministic. In the presence of competing wireless systems and other sources of electromagnetic interference (EMI), determinism can be defined as a function of bit error rate. In other words, there is some predictability to the environment, and a suitable channel sounding process has been completed.

There are multiple gaps in this phase:

(1) Can the wireless interface implement IEEE 802.1Qbv? There are many wireless scheduling approaches already and some may be extended to implement 802.1Qbv. This document does not intend to specify how at this point.

(2) Can the wireless interface be configured by the CNC just like a wired interface? This requires the use of NETCONF/YANG.

(3) How will synchronization error affect 802.1Qbv performance? Timing Measurement provides accuracy in the low microseconds, so guard bands would need to be larger than for Fine Timing Measurement solutions, where wireless synchronization may be as accurate as current wired synchronization.[1]

Notice in Figure 4 that wireless channel characteristics are hidden behind IEEE 802.1Qbv. For example, retries must occur during the scheduled transmission window and not past the point of usefulness. However, there are no known wireless implementations yet.

[1] For evaluation purposes, and to make the math easy, we will assume Wi-Fi traffic is being sent at 100 Mbps. Network traffic at 100 Mbps takes 80 nanoseconds per byte (1,000,000,000 ns/sec / (100,000,000 bits/sec / 8 bytes/bit)). A maximum 10 microsecond error in synchronization between two wireless devices requires the equivalent of an extra 125 bytes of data between windows where devices don't transmit (10 µs * 1000 ns/µs / 80 ns/byte) to avoid collisions. For windows 100 microseconds long (enough for 1250 bytes of data and headers), there would be up to 10,000 windows per second, or 1,250,000 bytes of wasted airtime per second, which is 10% of the 12,500,000 bytes/second of total bandwidth.
If the window sizes were increased to 1 millisecond (1000 microseconds) each, or Timing Measurement were improved to a 1 microsecond error in synchronization (which is feasible), the wasted airtime would be reduced to 1% of the total bandwidth.
(Note that the amount of bandwidth required to support Timing Measurement or Fine Timing Measurement is considered to be negligible.)

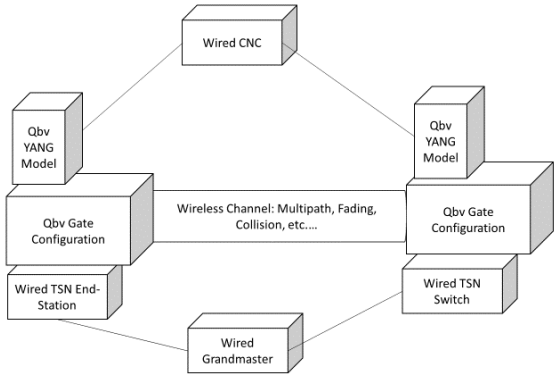

Fig 4 Phase 3 Hide Wireless Channel Behavior Behind IEEE 802.1Qbv.

Phase 4: Wireless Redundancy for Wired TSN

Note that Phases 2 and 3 are validation steps and not yet requiring deployment. In Phase 4, deployment of the wireless system from Phase 3 occurs, but only in the form of increasing reliability via adding redundant communication channels. As a reminder, this is a conservative approach in which wireless TSN is being introduced gradually to industrial systems and earning its trust along the way. In Figure 5, any of the redundant TSN paths may be wireless.

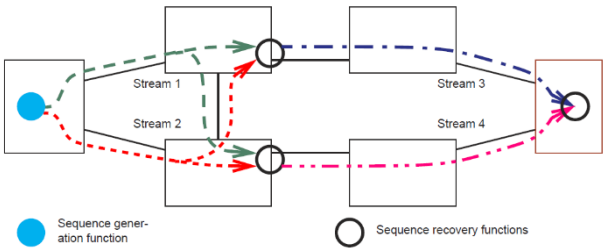

Fig 5 Phase 4 Wireless Redundancy for Wired TSN.

IEEE 802.1CB is the standard for wired TSN reliability. In this phase, some of the redundant channels now include wireless TSN.

The gap in this phase is, of course:

(1) Can wireless TSN interfaces can be seamlessly integrated into IEEE 802.1CB?

Initial indications are that IEEE 802.1CB should work fine with wireless. However, 802.1CB can cause packets to be delivered out of order, so either endpoints need to deal with that or switches need to buffer packets long enough to put them back in order. Given wireless retransmission, the potential need for buffering, determinism, etc. should be carefully analyzed in any design.

Phase 5: Wireless TSN Switch Deployment

In this final phase, wireless TSN is deployed between switches. In other words, wireless communication is now deployed anywhere within a wired TSN network.

The result of the final phase is full integration of wireless TSN that meets wired TSN reliability and performance requirements. A fully wireless TSN system could be deployed using the same CNC and CUC as the wired network.

The IEEE 802.1Qbz and 802.11ak standards allow wireless bridging that is interoperable with wired bridging. Currently, a wireless device is only expected to be connected to one Access Point and any bridging is done in proprietary ways. Those standards would allow for a standardized way to intermingle wired and wireless bridges.

Cybersecurity

Ensuring cybersecurity is a requirement in life-critical control systems for which industrial TSN will provide communication, both wired and wireless. While TSN is more complex than plain Ethernet and thus, presumably more difficult to attack, the argument that this makes TSN inherently secure is false. Each phase of this roadmap must consider cybersecurity tradeoffs with TSN performance including the cybersecurity impact upon latency, jitter, non-determinism, and cost.

Availability and authentication are the most important information assurance aspects for industrial systems. Confidentiality is generally of lower importance.

Cybersecurity within industrial systems, which depends upon authentication and sometimes encryption, is currently insecure. This is because both authentication and encryption depend upon the distribution of a “key” that is required to either

authenticate a user or decrypt a message. Because all cybersecurity mechanisms are based upon the common, shared secret known as a key, key generation, distribution, and lies at the heart of cybersecurity and is the only issue addressed in this roadmap. The specific use of keys, that is, the cybersecurity applications required, may vary widely and are determined by specific wireless applications and threat environments.

Private key exchange is the most secure form of key use; however, it is subject to the problem of securely transmitting keys to message recipients. Public key exchange attempts to solve this by trading-off security. Public key exchange uses two pairs of keys, a public and private key where only the public key needs to be exchanged and a private key is derived from the public key. Unfortunately, the cost of public key exchange is that it is not provably secure and it is possible, given enough computing power, for anyone to derive the private key from the public key. This has forced public key exchange to continuously increase key length to maintain a reasonable sense of security. However, this continual key length increase reduces resources and is not sustainable in the long term. Thus, critical industrial components are insecure in a large part because management and distribution of keys is an insecure process. Once an adversary obtains a key and can decrypt messages, the system is no longer secure. Thus, while it is recognized that keys are only one aspect of cybersecurity, they are the foundation upon which all other cybersecurity mechanisms rest.

Because keys and their secure distribution are fundamental to cybersecurity, this roadmap requires the ability to use symmetric keys and AES ciphers or stronger for all the proposed phases of this roadmap. Use of public key exchange mechanisms may be included if necessary, but is discouraged and expected to be phased out.

Industrial key distribution systems typically include mechanisms such as pre-installed keys, Diffie-Hellman, elliptic-curve, and the emerging quantum key distribution (QKD).

Pre-installed keys may be installed by the vendor during device manufacture. They suffer from an inability to be automatically updated once the device is placed in the field. Diffie-Hellman and elliptic-curve are widely used, but known to be insecure (Adrian, D. et al., 2015) and this roadmap discourages their use. Quantum key distribution is an emerging technology that solves the above problems but is still in its early commercial stages.

Use of the IEEE P1913 keychain YANG model is recommended for TSN because it has precise timestamps for each key and includes features for use with QKD. It enables keys to be managed with key lifetimes that are on the order of Ethernet frame transmission times in gigabit Ethernet networks.

This road map attempts to provide a solid foundation for key distribution as part of its vision, but does not attempt to specify wireless cybersecurity applications. It is recognized that there are several general vulnerabilities in TSN including time synchronization, the CNC and device configuration, and manipulation of IEEE 802.1Qbv schedules.

It is also important to note that there are TSN standards that can be used to enhance cybersecurity over wireless connections. For example, the IEEE 802.1Qci-2017 standard enables a bridge to detect whether or not some systems in a network are conforming to behaviors agreed to by configuration and/or protocol exchanges. These policing and filtering functions can be used to prevent the distribution of network traffic that is disruptive or unexpected, and can improve security by isolating sections of a network in well-defined ways.

Conclusion

There is a myriad of wireless technologies at various stages of maturity including Wi-Fi, 6LoWPAN, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac and above, MIMO technologies, cognitive radio, etc. This white paper is agnostic regarding the specific radio technology or technologies used. It is only required that they meet the progressively challenging requirements for each phase.

As noted, industrial systems are primarily focused upon deterministic communication for control

systems. Therefore, only scheduled (TT) and best effort (BE) traffic are of interest.

It is understood that a wireless TSN system will likely be effectively slower than the equivalent wired TSN system. For example, retransmission to improve reliability may be one reason for longer latency in wireless TSN channels. Careful thought in combining this aspect with IEEE 802.1CB should be considered. However, longer latency of wireless TSN is unlikely to be a problem in many industrial applications. The most critical problem is reliability with determinism; a message must reach its destination within its scheduled period.

This document is to be considered a request for comments; constructive corrections, ideas, and comments are very welcome by the author. Please contact wirelesstsn@avnu.org with comments.

Appendix A – Synchronization

As an alternative to using 802.1AS synchronization, it is possible to use GNSS receivers for wireless synchronization. This makes sense for a widely distributed network, where satellite synchronization is likely to be more accurate than synchronizing time over a network connection. However, there are concerns with using GNSS receivers for a TSN network:

1. How feasible is it that all end-devices will be using GNSS and have clear satellite reception?
2. Is GNSS with 802.1Qbv as likely to be supported as 802.1AS with 802.1Qbv?
3. How do you ensure that switches and Access Points using wired time have the same time base as wireless devices using GNSS (needed for 802.1Qbv support)?

One possibility for using GNSS receivers is that the wired (or wireless) grandmaster would be using GNSS time, which would allow for a mix of both as needed.

An additional timing consideration is that the devices on the network may not all need the correct time, just the same time. For protocols such as 802.1Qbv, the only requirement is that the grandmaster distributes the same time to everyone. If all the devices think the year is 1990, they can still work correctly – if they think it is the same time in the year 1990. More fundamentally, the 802.1Qbv schedules must start from the same epoch and remain synchronized.

Appendix B – IETF Deterministic Networking (DetNet)

This document is intended for use cases where the entire TSN network is under the administrator's control and latency is predicable. In other words, situations where network traffic is centrally managed, not carried over long distances (WANs) or over a third-party network, and IP (layer 3) routing is not required for the TSN traffic.

The IETF currently has a "DetNet" Working Group focused on supporting Deterministic Networking for networks that require IP (layer 3) routing. If you have an interest in DetNet, you are encouraged to learn more at https://datatracker.ietf.org/wg/detnet/about/ .

Unlike TSN networks, DetNet requires that all devices on the network support IPv6 addressing. With DetNet, network routers are configured to allow DetNet traffic to be relayed reliably, securely, and with bounded, end-to-end deterministic latency. Like TSN networks, DetNet is limited to centrally controlled networks, so it will not support "the open Internet."

According to the DetNet Use Cases document, a "DetNet network is intended to integrate between Layer 2 (bridged) network(s) (e.g. AVB/TSN LAN) and Layer 3 (routed) network(s) (e.g. using IP-based protocols)." This would allow a network administrator to use DetNet for "connecting two AVB/TSN LANs ("islands") together through a standard router."

While DetNet includes wireless use-cases, it does not currently include support explicitly for Wi-Fi. Upcoming standards that will make deterministic latency more predictable over Wi-Fi, such as IEEE 802.11ax, could make Wi-Fi more interesting to the DetNet community.

Unlike TSN, DetNet is explicitly agnostic to the timekeeping method used, so IEEE 1588, IEEE 802.1AS, GNSS, and other synchronization protocols are all assumed to be valid if they allow the devices to maintain common time at an acceptable level of accuracy and reliability. Synchronization issues will need to be addressed before using DetNet for Industrial networks.

References

Avnu Alliance Best Practices – Theory of Operation for TSN-enabled Industrial Systems: http://avnu.org/knowledgebase/theory-of-operation/

Global Positioning System Standard Positioning Service Performance Standard: https://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf

IEEE 1913 – Software-Defined Quantum Communication Draft *(Under Development)*: https://standards.ieee.org/develop/project/1913.html (YANG module: sqdc-qkd@2017-07-20)

IEEE 802.1AS-2011: https://standards.ieee.org/findstds/standard/802.1AS-2011.html

IEEE 802.1AS-Rev *(Under Development)*: http://www.ieee802.org/1/pages/802.1AS-rev.html

IEEE 802.1CB-2017: https://standards.ieee.org/findstds/standard/802.1CB-2017.html

IEEE 802.1Qbv-2015: https://standards.ieee.org/findstds/standard/802.1Qbv-2015.html

IEEE 802.1Qbz-2016: https://standards.ieee.org/findstds/standard/802.1Qbz-2016.html

IEEE 802.1Qci-2017: http://standards.ieee.org/findstds/standard/802.1Qci-2017.html

IEEE 802.11-2016 (includes Timing Measurement and Fine Timing Measurement): https://standards.ieee.org/findstds/standard/802.11-2016.html

IEEE 802.11ak *(Under Development)*: http://www.ieee802.org/11/Reports/802.11_Timelines.htm#tgak http://standards.ieee.org/develop/project/802.11ak.html

IEEE 802.11ax *(Under Development)*: http://www.ieee802.org/11/Reports/802.11_Timelines.htm#tgax http://standards.ieee.org/develop/project/802.11ax.html

IEEE 802.15.7-2011 – IEEE Standard for Local and Metropolitan Area Networks--Part 15.7: Short-Range Wireless Optical Communication Using Visible Light: https://standards.ieee.org/findstds/standard/802.15.7-2011.html

IETF DetNet *(Under Development)*: https://datatracker.ietf.org/wg/detnet/about/ https://www.ietf.org/mailman/listinfo/detnet

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., … Paul, S. Z. (2015). Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. Ccs, 5–17.: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf