Securing Critical Timing Infrastructure

By: Samer Darras

Senior Technical Staff Engineer and Manager in Frequency & Time Systems at Microchip Technology

Member of 1588-2019 Standard Working Group

Table of Contents

1. Status of Precision Time Protocol (PTP) Standards

Precision Timing Protocol (PTP) is a protocol used to synchronize clocks in many critical infrastructure networks such as telecommunication, energy, utilities, transportation and other industries. An important aspect of these crucial networks is that they need to be secure. So the question is, should PTP also be secure – and if so, what are the essentials operators must know to effectively maintain service continuity?

PTP has been used for many years to synchronize clocks based on the assumption that critical infrastructure networks are mostly closed environments, thus less vulnerable to attacks. However, with more focus and awareness today about security across multiple industries, addressing security to protect timing – and more specifically, packet-based timing such as PTP 1588 – has become a much more prominent priority.

In the latest release of the PTP standard IEEE® 1588-2019 (version 2.1), four new security prongs or concepts were introduced to address security and resiliency. These prongs can be used individually or in combination to protect against security attacks.

This paper presents a brief introduction on the four security prongs and addresses the reasons why Prong C and Prong D are key priorities to address PTP security now, while also recognizing the need for authentication or encryption in the longer term.

1.1 Integrated Security Mechanism – Prong A

In Prong A, a new Authentication Type-Length-Value (TLV), a normative TLV, was added at the end of PTP messages to ensure the integrity and authenticity of the messages.

Figure 1-1. PTP Frame with Authentication TLV

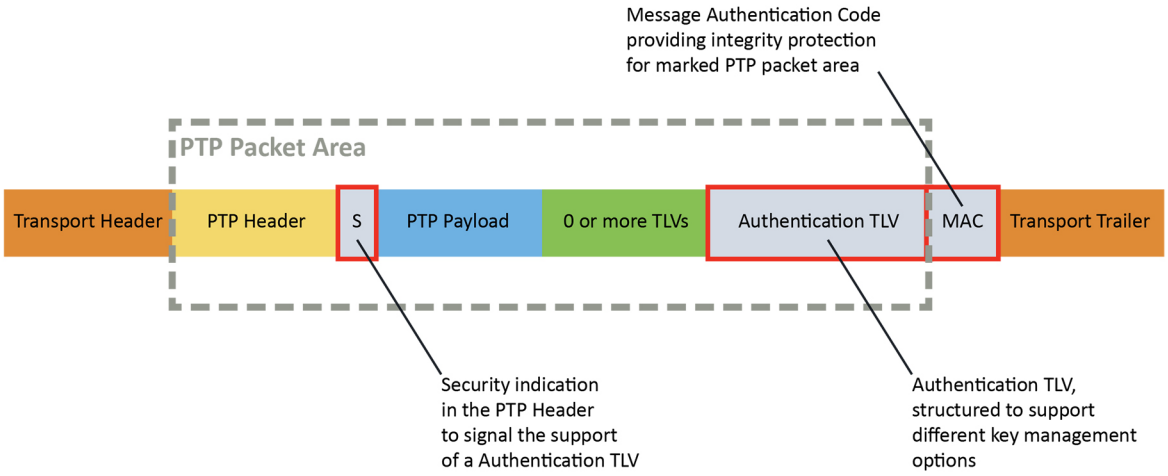


Figure 1-1 shows a 1588 PTP packet with various fields and the specific Authentication TLV appended right ahead of the Message Authentication Code. Right after the PTP header a field (“S”) indicates the Authentication TLV is used in this packet.

Since PTP messages do not carry sensitive information and nothing confidential in timestamps, the integrity and authenticity of the PTP messages are what is important. Integrity ensures the packets were not changed, maliciously or accidentally, along the path. That is why authentication is considered secure without the need for encryption, since PTP information is not confidential.

The security key distribution for the Authentication TLV has not been finalized yet. Currently, proposals are being discussed and reviewed by the Internet Engineering Task Force (IETF) and Institute of Electrical and Electronics Engineers (IEEE).

For this reason, while the authentication of timing packets is a very valuable security enhancement, this capability is probably best implemented once the key distribution is finalized. Therefore, the focus of this paper will not be on this capability, pending further progress in the standards bodies or adoption of authentication keys in PTP clients.

1.2 External Security Mechanisms – Prong B

This prong encompasses using well known transport security mechanisms such as IPsec (IP Security) and MACsec (Media Access Control Security) for securing PTP and basically, using existing security infrastructures that may already have been deployed in a network to secure the transport of PTP messages.

Figure 1-2. PTP Payload Encapsulation in MACsec Frame

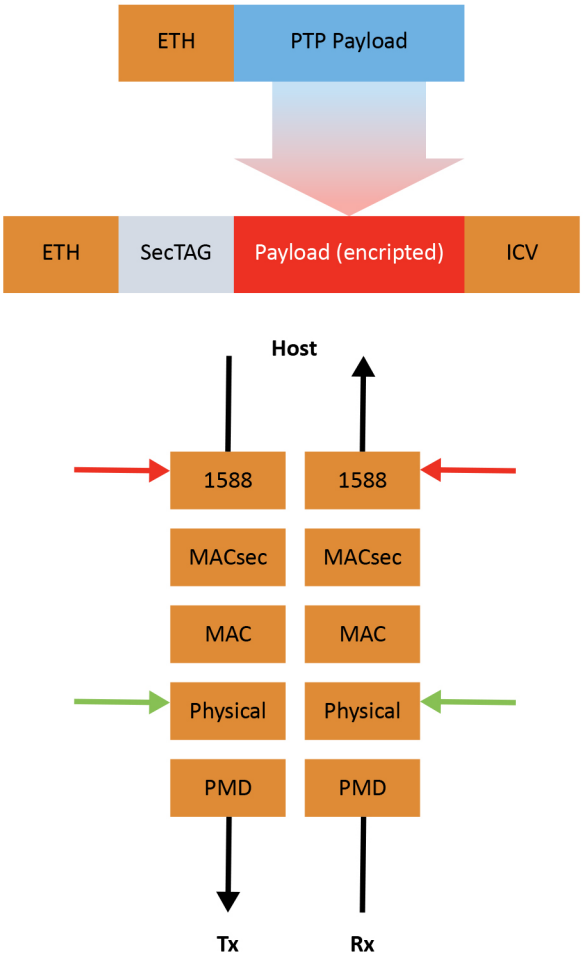


Figure 1-2 shows an encrypted payload preceded by a security TAG field as well as a MACsec layer, both on transmit and receive sides, inserted between the MAC layer and the 1588 layer.

While this approach may sound effective, it is worth noting that because of the added layer of encrypting of PTP packets, the accuracy of the timestamps may degrade, causing it to be outside of the required specifications for some applications. Also, the definition of the timestamp mark is the first byte after the Start of Header (SOH). Prepending data moves, the timestamp is relative to the receiver and requires additional complexity to correct. Application accuracy requirements vary widely and can range from a few nanoseconds in applications such as 5G to milliseconds in a company enterprise network where the primary use case is to synchronize PCs for logging and accounting purposes. These challenges will be discussed later in this paper, along with steps to address them.

The main hurdle to encryption is the requirement to adapt hardware to include a PHY (physical layer of the OSI model) chip that embeds MACsec capabilities. Discussed here also will be the benefits presented by this form of security.

In the short term, however, the assumption will be that operators do not wish to invest in new hardware that supports new PHYs – therefore, the focus here will concentrate on other aspects that can be addressed with today's timing appliances.

IPsec is a secure network protocol suite that authenticates and encrypts packets to provide secure communication between two devices. IPsec is a layer 3 OSI model scheme, it typically processes authentication and encryption of packets in software which adds a lot of variability to the accuracy of timestamps. It somewhat diminishes the value of PTP being so accurate using hardware timestamping.

1.3 Architecture Guidance – Prong C

The architecture that Prong C proposes is a set of methods describing three approaches of securing PTP via resiliency.

1.3.1 Multiple Inputs Using Various Timing Systems

There are other types of timing systems that can be used to complement PTP. Examples include the Global Navigation Satellite System (GNSS), Inter-Range Instrumentation Group (IRIG), and Time-of-Day (ToD), as defined in the ITU G.8271 standard. A timing appliance can test the performance of PTP against other available timing systems to detect timing errors. Having three or more timing systems as potential inputs, the timing appliance can run a majority vote scheme to detect spoofing or delay attacks on the PTP timing system.

A priority scheme can also be used to assign a higher priority value to the more trusted timing systems in the case of a tie when having an even number of timing systems.

Figure 1-3. Timing Appliance with Multiple Timing Systems

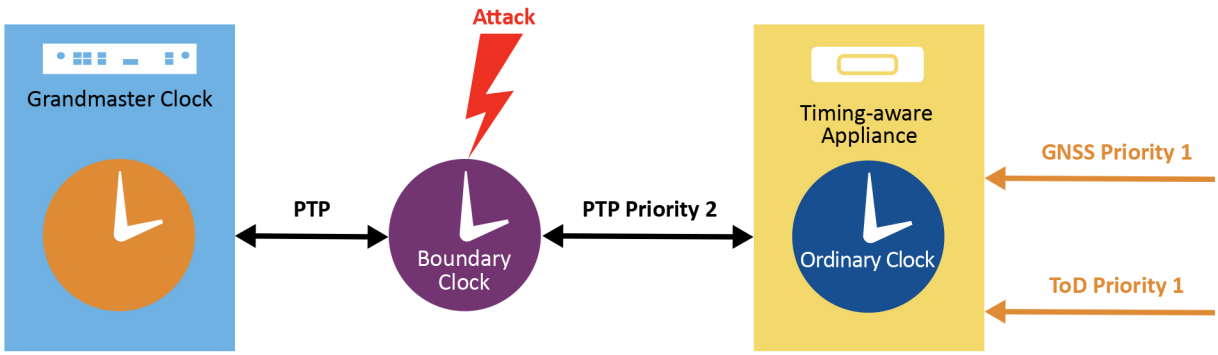


Figure 1-3 shows a timing appliance with multiple timing references, with Priority 1 assigned to GNSS and ToD while Priority 2 is assigned to PTP. If the PTP timing reference path gets compromised, the timing appliance can reject it and use an alternate timing references.

1.3.2 Multiple PTP Grandmasters

Multiple grandmasters can also be used to increase robustness and resiliency against security attacks. In this case, multiple domains and/or multiple profiles can be used to run a majority voting algorithm between multiple PTP instances to detect timing errors.

Figure 1-4. Multiple PTP Grandmaster with Different Domains

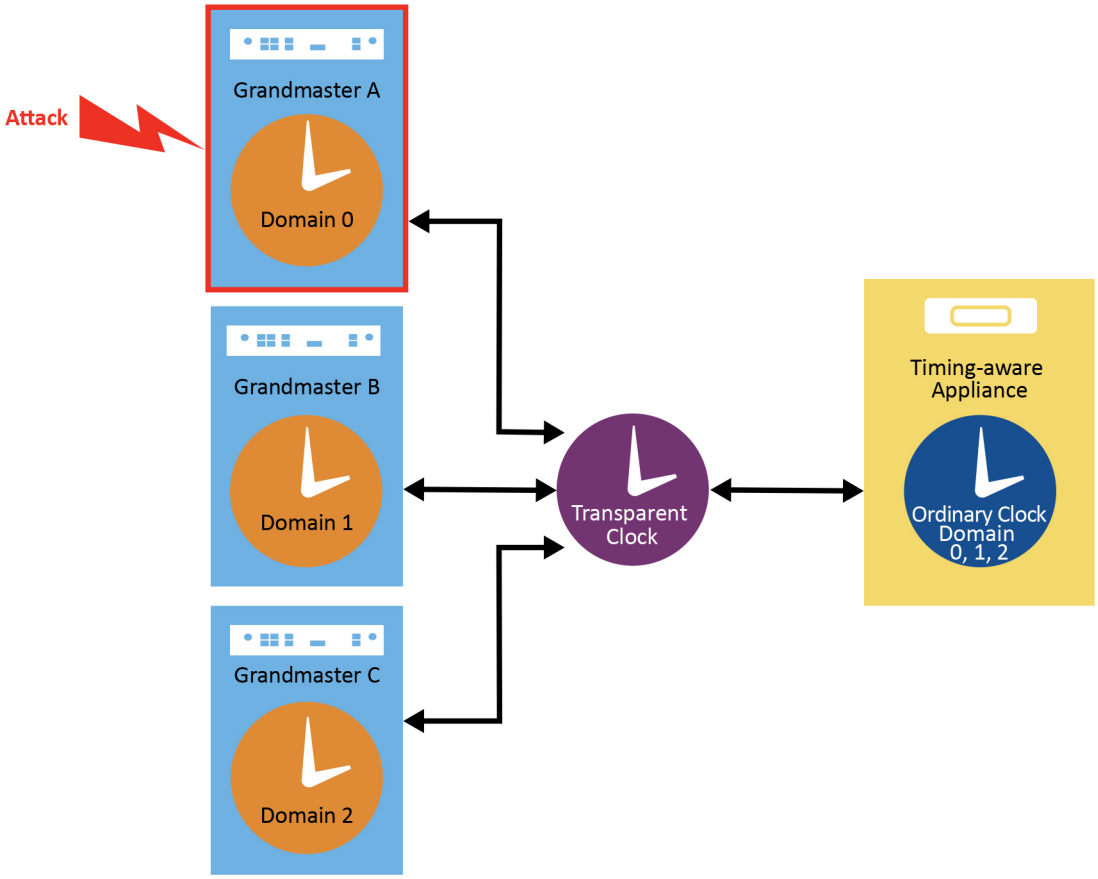


Figure 1-4 shows a timing appliance receiving PTP messages from three separate grandmasters using different PTP domain numbers. If grandmaster A was spoofed, the timing appliance should be able to detect that the timing from grandmaster A does not match the timing coming from grandmasters B and C. In this case, it disqualifies grandmaster A as a timing reference and potentially raises an alarm to the Network Management System (NMS), so a network engineer can investigate and take appropriate action.

1.3.3 Multiple Network Paths

This method describes the use of multiple paths to the timing appliance. A single multi-port grandmaster or multiple grandmasters can be used in this case. If a timing appliance supports multiple physical ports capable of running PTP, then it can compare the timing performance on the paths and run a majority voting algorithm to detect anomalies. The timing appliance can detect large time jumps or unexpected path delay on the path by comparing the timing performance against the other paths.

Figure 1-5. Timing Appliance Using Multiple Paths

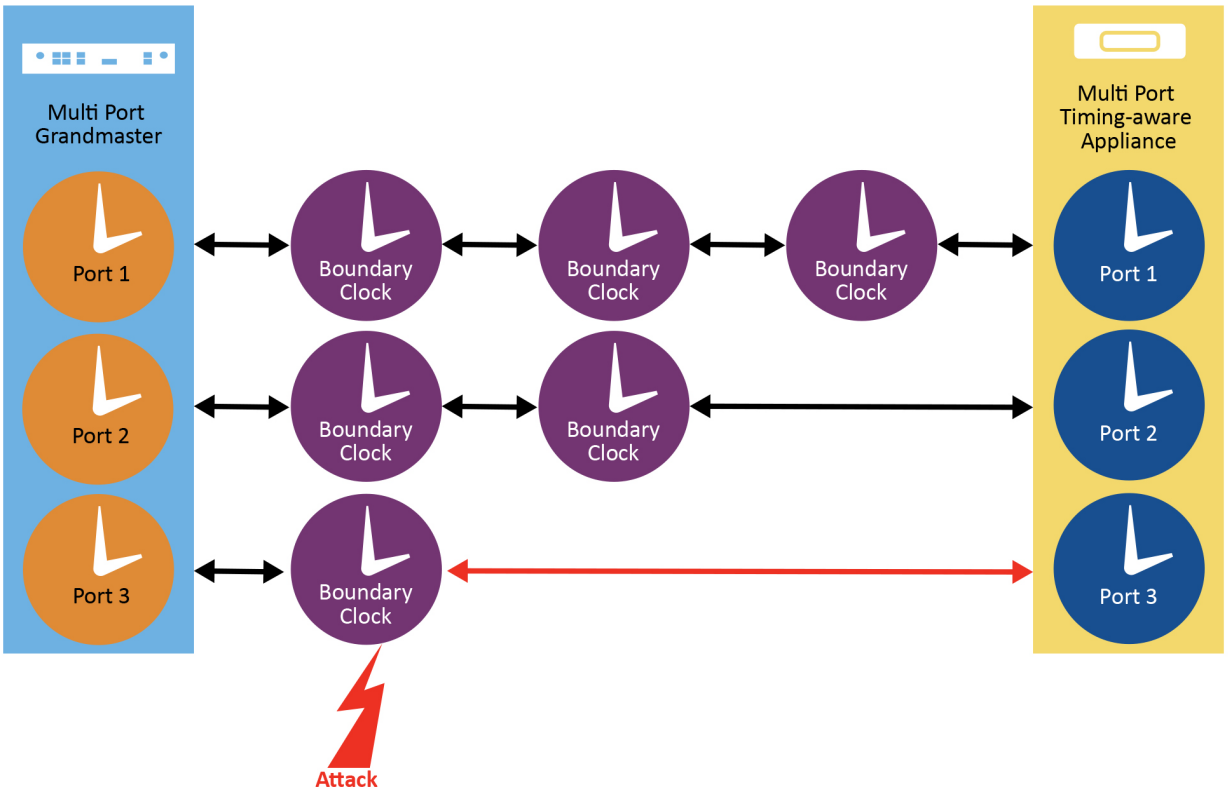


Figure 1-5 describes a multi-port grandmaster connected to a multi-port timing appliance via three different paths, one with three boundary clocks (BCs), one with two boundary clocks and one with a single boundary clock. The standard would select the path with the lower number of BCs. We will show in this document that specific implementation can provide more value than the standard by taking into account other factors than simply the number of BCs on the respective paths.

1.4 Monitoring and Management – Prong D

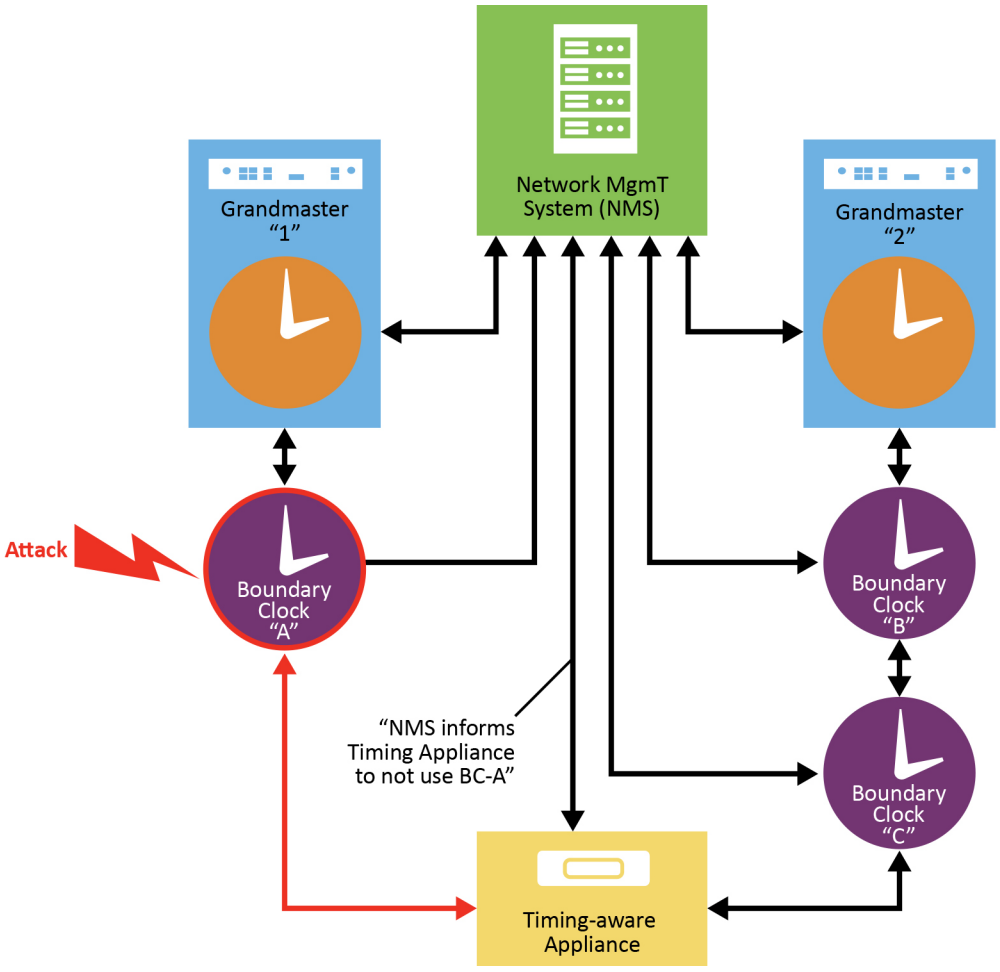
In Prong D, signal monitoring and external management mechanisms can be used to detect time anomalies. Typically, this security approach has more value when it is combined with the architecture security prong, as it feeds very well into the majority voting algorithm to qualify or disqualify a timing system.

Various parameters and aspects could be monitored to enhance security, including factors like link delay, unexpected offset jumps, or large variations in asymmetry between the Sync T1/T2 timestamps and Delay T3/T4 timestamps.

Additional parameters such as counters that can check the PTP message rate or detection of duplicate PTP messages using sequence ID could also provide some indication of possible DoS or replay attacks.

An external Network Management System (NMS) has a higher view of the network topology and can monitor all devices and network changes. Upon detection of an attack on grandmaster or path, it can inform a timing appliance to stop using the grandmaster or path for time synchronization.

Figure 1-6. Monitoring and Management



NMS detects that BC-A was attacked so it informs the Timing Appliance not to synchronize to BC-A, instead use sync from BC-C

2. Recommendations to Secure PTP Today

2.1 Authentication and Encryption

Critical infrastructure networks are closed and protected environments less prone to typical attacks than networks that are more open in nature. Typically, access control mechanisms are very much needed to secure the connectivity to the various timing devices in the network.

Firewalls should be the critical first step. Implementing Authentication, Authorization, Accounting (AAA) mechanisms using servers deployed for the purpose of network security such as TACACS+ or Radius are of great value.

The addition of two-factor authentication (2FA) and security levels to categorize users and respective rights also are recommended steps.

However, authentication of PTP traffic per se (Prong A) is a capability to keep in mind but may not be urgent to deploy now, given the lack of finalization at the standard bodies on the topic of key exchange.

Encryption used to be a hurdle as it relates to PTP, for performance reasons. However, today PHY chips not only embed MACsec encryption but also implement mitigation steps to alleviate the performance drawbacks. Therefore, it is recommended that operators move forward with adoption of encryption of PTP (Prong B) for devices now in the design stage and those in which a future-proof evolution is planned.

2.2 Security and Resiliency

Prong C and Prong D have introduced security approaches that offer security benefits that can be leveraged to ensure the enablement of more resilient networks.

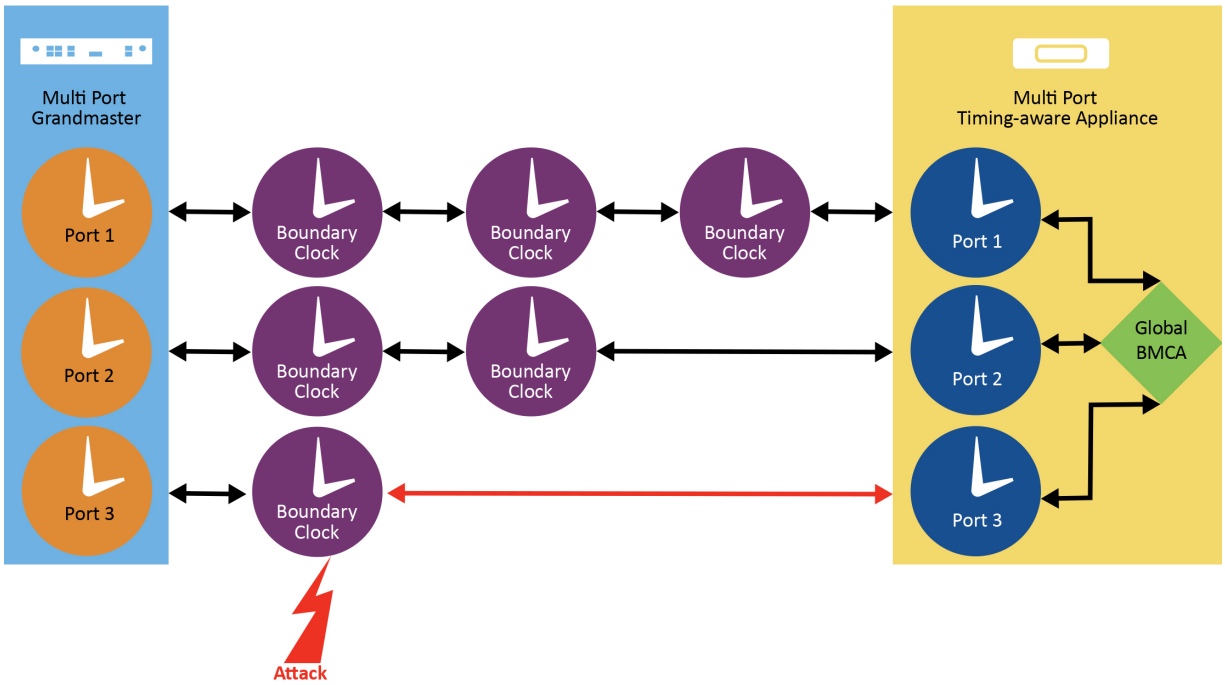
Prong C referred to “majority vote” mechanisms to select the best clock. This majority vote algorithm is defined by the IEEE 1588-2019 standard and involves a Global-Best Master Clock Algorithm (G-BMCA).

2.2.1 Introduction of Global Best Master Clock Algorithm G-BMCA

The Best Master Clock Algorithm (BMCA) is what PTP uses to select the best clock to use as a reference. In the case of a single grandmaster, the BMCA works by selecting the best path from the grandmaster by choosing a path with the least number of boundary clocks, irrespective of the presence of transparent clocks in the path or the path characteristics like jitter, asymmetry and path delay.

G-BMCA was introduced to include path performance and support datasets from multiple PTP instances. The G-BMCA runs as a single instance and uses a Performance Figure of Merit (PFOM) metric calculated in the PTP instance. The PFOM check can be added at any stage in the BMCA datasets comparison tree depending on the confidence level in the metric. Along with datasets from the multiple PTP instances, the G-BMCA decides the best PTP instance that ultimately is used as the reference to the timing appliance.

Figure 2-1. Timing Appliance Using Global BMC Algorithm



It is important to note that Prong C and Prong D were defined for security purposes but can be used to provide more resiliency, by providing a more robust Assisted Partial Timing Support (APTS).

Combined with the ability to support three PTP client inputs and the use of G-BMCA, a grandmaster can leverage three other connected grandmasters in the network and select the best to use for APTS when its GNSS connection is poor, spoofed, jammed or otherwise unavailable.

This enables operators to be confident about the robustness and performance of their critical infrastructure network so GNSS can be backed up by PTP in an intelligent, secure and performant manner.

Using not only the number of BCs in the path as the standard defines but also the characteristics of the links in a broader sense shows the value of embedded algorithms in grandmasters offering capabilities beyond the pure definition of IEEE 1588-2019.

3. Conclusion – Taking the Appropriate Steps to Timing Security

Security has become essential. Securing the timing infrastructure also is a necessity. The four security prongs analyzed in this paper each have strengths and weaknesses. For example, delay attacks cannot be easily detected by the authentication and encryption mechanisms proposed in Prong A and Prong B. Also, some timing appliances lack the complicated hardware of having multiple ports or even the capability of running multiple PTP instances as outlined in the architecture prong.

Microchip Technology continues to invest in supporting the architecture and monitoring, Prong C and Prong D, respectively, as the first phase of addressing PTP security. These architecture and monitoring mechanisms can be easily deployed in existing networks. Similar mechanisms exist today in many telecommunication networks like Virtual Router Redundancy Protocol (VRRP) and can support the adoption of architecture and monitoring of PTP. These capabilities are at the core of Microchip's new 2.3 software version of TimeProvider 4100, which also supports many other security measures highlighted in this paper, beyond those defined by the four prongs of IEEE 1588-2019.

Microchip offers PHY solutions that support MACsec, enabling critical performance which will be considered for new devices.

4. Revision History

Revision	Date	Description
A	11/2021	Initial Revision

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

Trademarks

ISBN: 978-1-5224-9124-8

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820