Threat Sensitive Networking

On the Security of IEEE 802.1CB and (un)Effectiveness of Existing Security Solutions

de Vos, Adriaan; Brighente, Alessandro; Conti, Mauro

DOI
10.1007/978-3-031-25460-4_4

Publication date
2023

Document Version
Final published version

Published in
Computer Security. ESORICS 2022 International Workshops - CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT and SECOMANE 2022, EIS 2022, and SecAssure 2022, Revised Selected Papers

Citation (APA)
de Vos, A., Brighente, A., & Conti, M. (2023). Threat Sensitive Networking: On the Security of IEEE 802.1CB and (un)Effectiveness of Existing Security Solutions. In S. Katsikas, F. Cuppens, C. Kalloniatis, J. Mylopoulos, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, M. A. Sotelo Monge, M. Albanese, B. Katt, S. Pirbhulal, & A. Shukla (Eds.), *Computer Security. ESORICS 2022 International Workshops - CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT and SECOMANE 2022, EIS 2022, and SecAssure 2022, Revised Selected Papers* (pp. 67-80). (Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Vol. 13785). Springer. https://doi.org/10.1007/978-3-031-25460-4_4

Threat Sensitive Networking: On the Security of IEEE 802.1CB and (un)Effectiveness of Existing Security Solutions

Adriaan de Vos[1(✉)], Alessandro Brighente[2], and Mauro Conti[1,2]

[1] Delft University of Technology, Delft, The Netherlands
info@adriaandevos.nl, m.conti@tudelft.nl
[2] University of Padua, Padua, Italy
{alessandro.brighente,mauro.conti}@unipd.it

Abstract. IEEE 802.1CB provides a standard for reliable packet delivery within Time-Sensitive Networking (TSN). As this standard is envisioned to be used in mission-critical networks in the near future, it has to be protected against security threats. The integrity of the network communication should be the biggest focus as guaranteed delivery is essential. However, IEEE 802.1CB does not come with security guarantees. Indeed, as we show in this paper, an attacker may be able to exploit different threat vectors to impair the correctness of communication, impacting on the safety of users. Due to TSN strict delay and reliability requirements, classical security solutions can not be easily applied without significant efforts. Therefore, researchers proposed multiple solutions to guarantee secure communication. However, the current state-of-the-art is not able to guarantee both security and timing guarantees.

In this paper, we provide a detailed analysis of the security of IEEE 802.1CB exploiting the STRIDE methodology. Compared to the existing state-of-the art on the subject, we provide a deeper analysis of the possible threats and their effect. We then analyze available solutions for security in IEEE 802.1CB, and compare their performance in terms of time, reliability, and security guarantees. Based on our analysis, we show that, although there exist promising solutions trying to provide security to 802.1CB, there is still a gap to be filled both in terms of security and latency guarantees.

Keywords: IEEE 802.1CB · Time-Sensitive Networking (TSN) · Replication and Elimination for Reliability (FRER) · Ethernet · Security

1 Introduction

Traditional networking solutions can not be used for mission-critical applications such as automotive, avionics, and industrial networks. Indeed, traditional

S. Katsikas et al. (Eds.): ESORICS 2022 Workshops, LNCS 13785, pp. 67–80, 2023.
https://doi.org/10.1007/978-3-031-25460-4_4

networks were not designed to deliver real-time and ultra-reliable communication. In addition, many existing network solutions are incompatible with each other, a factor that complicates the development and deployment of real-time networks. As a response to these problems, the IEEE has published the specification of a new networking standard called Time-Sensitive Networking (TSN) [1]. This standard extends the Ethernet data link layer to ensure that time- and safety-critical traffic achieves an extremely low packet loss rate and a finite, low, and stable end-to-end latency. Due to this, TSN is the prominent standard to be implemented in modern Cyber-Physical Systems (CPS). These systems cover the edge between the digital and the real world and include industrial applications such as flood defence, smart grids, transportation networks, automotive vehicles, etc. With these systems, insufficient security could cause serious adverse effects as people trust their lives to the correct working of these systems. In recent years CPS are becoming more connected to the internet [2] and are increasingly often the target of malicious actors [3–6], so they need to be secured.

One specific standard within TSN is IEEE 802.1CB [7]. This standard focuses on providing increased redundancy to network communications. This standard is also called Frame Replication and Elimination for Reliability (FRER), and it is often combined with IEEE 802.1Qca to configure multiple disjoint paths within a network. This technique increases frame delivery reliability by using sequence numbering and sending duplicate frames over disjoint paths within IEEE 802.1CB compatible switches and endpoints. These replicated frames protect against hard and soft errors of the underlying links and nodes. Finally, these duplicate frames need to be detected and eliminated at their destination as the standard defines that only the first arrived frame should propagate further. This functionality, however, introduces a security issue which we explore further throughout the paper, as an attacker could modify or delay frames to spoof the sequence numbers, tamper with the payload, or execute Denial of Service (DoS) attacks. These attacks impact the integrity and availability of the network communications and could therefore result in acting upon incorrect data, or involve serious consequences to the performance of critical infrastructure.

In this paper, we first provide an in-depth analysis of the security of IEEE 802.1CB. Although other researchers analyzed TSN security at a high level, there are no contributions providing a detailed analysis of the security of IEEE 802.1CB. To this aim, we exploit the widely accepted STRIDE methodology [15] to identify all the possible threats and their effect on IEEE 802.1CB. We then analyze and compare existing state-of-the-art security solutions for IEEE 802.1CB. We compare these solutions in terms of their capability in mitigating the attacks identified via our analysis and in terms of their time requirements and delay guarantees. Via our analysis, we show that, although some solutions propose promising approaches, there is no available solution able to guarantee full security to IEEE 802.1CB, nor is there a solution able to provide jitter guarantees (which is among the requirements of IEEE 802.1CB).

The rest of the paper is organized as follows. Section 2 provides a summary of the Time-Sensitive Networking standard and short descriptions of the available features, Sect. 3 dives into the specifics of IEEE 802.1CB, Sect. 4 describes the

possible security risks and their effects, Sect. 5 summarizes existing solutions that try solving these security risks, Sect. 6 gives an overview of these solutions, and Sect. 7 discusses the related work. Finally, the conclusions are presented in Sect. 8.

2 Time-Sensitive Networking

The IEEE 802.1 Time-Sensitive Networking (TSN) standard extends the IEEE 802.1 Audio Video Bridging (AVB) standards released in 2011. These AVB standards provide some extended features for IEEE 802.1 networks in regards to low-latency traffic flows, bandwidth reservation, and synchronization [8]. While these features improved the feasibility of using it for mission-critical applications, it was not extensive enough to support a wide variety of applications as it only focused on audio and video streams. While modern automotive, avionics, and industrial networks might transfer these kinds of streams, they also require other types of streams. Moreover, these applications require a wide variety of sensors and actuators that need reliable real-time communication to ensure good operation. For this, there has been quite some development in the last decade by different companies to create their proprietary network solutions [9]. However, these solutions are not compatible with each other. Therefore, IEEE released the TSN standard to ensure that all components of different networks can efficiently work together while achieving the requirements for such mission-critical applications.

For this section, we take IEEE 802.1Q-2018 [10] as the central reference implementation and describe the TSN related features released within. This central reference document bundles the latest features and updates once every 3 to 6 years. The standard focuses on providing a deterministic service with the following Key Performance Indicators (KPI) [11], namely guaranteed delivery with bounded latency, low delay variation (jitter), and low packet loss.

For guaranteed delivery with bounded latency, the protocol makes sure that some capacity is reserved for specific data streams to prevent congestion throughout the network. The bounded latency provides a guarantee about the worst-case delay for packet delivery. The low delay variation reduces the likelihood that delivered packets arrive in an incorrect order. Furthermore, the low packet loss reduces the likelihood that no message is received at all. Combining these KPIs provides a very reliable and deterministic network that would fit well for mission-critical systems.

The IEEE 802.1Q-2018 standard focuses on delivering wired network communication in a network of switches/bridges and some end devices that are each connected to this network through separate cables. These end devices could be workstations, sensors, actuators, or other devices requiring network communication. The basic functionality of this standard is to provide Quality of Service (QoS) and virtual Local Area Networks (LANs) to an Ethernet network. In addition, this standard contains many optional features, of which only a subset has to be implemented based on the application's requirements for network communication. As each feature focuses on a different improvement, we can divide them into the following categories according to [11].

Timing and Synchronization ensures that all components within the network (both the bridge and end-devices) have synchronized clocks. This synchronization is necessary for mission-critical systems such as fully automatic driving as they require a common notion of time for sensor fusion.

Bounded Low latency ensures configuration within the network to reserve capacity for certain types of messages or allow time-critical messages to interrupt non-time-critical messages. This traffic shaping ensures minimal delay for critical messages within the network, which is needed for mission-critical systems to quickly act upon their received sensors.

Resource Management provides algorithms and configuration options to divide the available network bandwidth into reserved streams by establishing and enforcing bandwidth contracts between network components. These reservations ensure a deterministic network where no packet loss due to congestion occurs as each application has a maximum throughput they need to adhere to.

High-Reliability provides methods to improve the reliability of packet delivery within the network by using Quality Of Service (QoS), non-shortest network paths, or redundant packet transmission. As mission-critical systems often have real-time applications, they cannot tolerate delays due to re-transmissions of lost frames.

3 IEEE 802.1CB

In this section, we delve deeper into the High-Reliability category of the TSN standards and specifically into 802.1CB-2017 Frame Replication and Elimination for Reliability (FRER). This standard specifies procedures and protocols for network components that provide identification and replication of packets for redundant transmission and identification/elimination of duplicate packets. However, it does not describe how these disjoint paths should be created and configured. This feature provides an increased probability that a given packet will be delivered. However, it is highly suggested to use it in cooperation with other means to increase the probability of correct delivery further. Research has shown that while this standard does a great job in improving the reliability, there are still some difficult challenges that have to be resolved to increase the reliability of this feature even further [7,12]. We give a short description of the various functions and explain the inner workings below.

Frame Replication provides the generation of packet sequence numbers for a given stream and encoding it in each packet. This sequence generation function adds an IEEE 802.1CB specific header to provide packet identification. This header allows other network components to detect duplicate packets. After adding the sequence number to a packet, the packet propagates through multiple network paths and, if configured, multiple streams on the same path.

Frame Elimination provides the elimination of duplicate packets. It keeps track of the received sequence numbers and only relays the first packet for each received sequence number. This functionality ensures that no loops or exact duplicates will be relayed and delivered to the next component along the path.

After elimination, each network component can replicate the packet again on separate paths if configured.

Latent Error Detection provides a detection mechanism for an unexpected number of packets either due to network failure, invalid network configuration, or an attacker. This detection assumes that the number of discarded packets per sequence number should always stay the same if everything works well. A configurable threshold ensures that there is some leeway for naturally occurring packet loss, which is very rare [13], but should not cause an alarm when this event occurs. However, if it detects that a significantly lower number of packets is received suddenly, it raises an alarm to indicate that a network link has gone down. In contrast, if it detects a significantly higher number of packets, there is a possibility that an attacker is spoofing packets.

Implementation of this IEEE 802.1CB standard can be gradually rolled out within a network as it is backwards compatible with non-supporting systems. Different network configurations provide different guarantees and loss rates depending on their support for this standard and the actual topology [14]. For example, an existing ring topology network with the end devices connected to a ring of switches can already upgrade reliability by only updating the switches. This partial upgrade will ensure that the message will go both clockwise and counterclockwise, resulting in a higher resilience against link failure (hard error). Another example is if we only update the end devices in this topology. This upgrade will cause the packets to be sent twice through the same route and eliminated at the end device. While this does not protect against link failure, it does protect against soft errors such as a CRC mismatch. Partially upgrading a combination of switches and devices will already result in a much more reliable delivery, even if not all devices support this feature. See Fig. 1 for a graphical overview of the variations.

4 Possible Security Risks

In this section, we use the threat modelling framework STRIDE [15] to analyse the possible security attacks and effects on IEEE 802.1CB. This framework covers **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege threats against system components. As IEEE 802.1CB has no built-in security, the protection against possible threats is nonexistent. For example, there is no mitigation against the misuse of the elimination function and the latent error detection function. Therefore, an adversary can target the network communication to disrupt it. In addition, an incorrect network configuration could also prevent it from delivering its service. We describe these threats in the following sections.

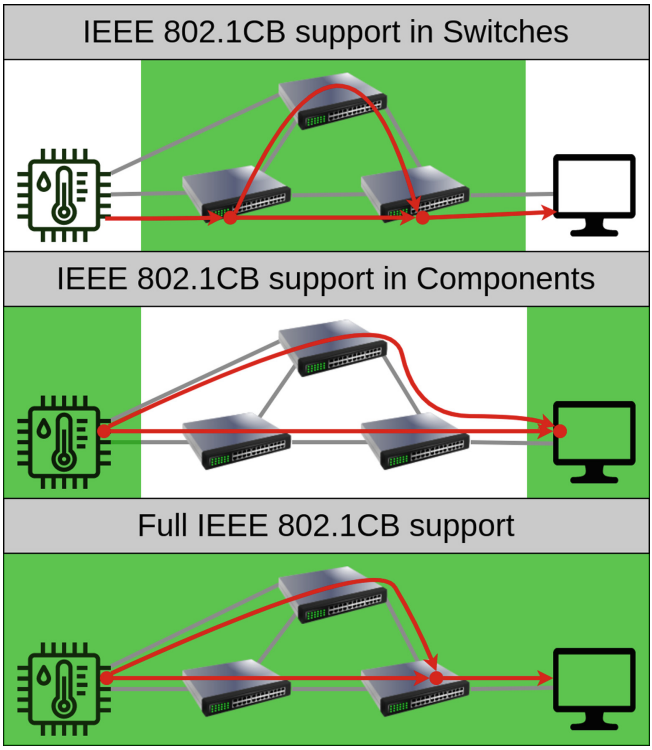

Fig. 1. Different implementation configurations showing support for seamless redundancy by enabling 802.1CB

4.1 Sequence Numbering

As the elimination of packets is done based on the sequence number, changes to this value could have adverse effects on the reliability. For the above mentioned attacks, we focus on the sequence number part of the FRER header as shown in Fig. 2.

If an attacker can intercept packets to modify them, or if the attacker can create new packets within the network, the following attacks are feasible.

- The attacker uses **spoofing** to create new packets within the network with existing sequence numbers that arrive earlier than the correct packets. This attack causes the elimination function to drop the original packets resulting in a **denial of service**.
- The attacker uses **spoofing** to create new packets within the network with existing sequence numbers that arrive later than the correct packets. This attack causes the Latent Error Detection function to trigger a warning signal as too many packets are delivered, resulting in the mission-critical system taking unnecessary precaution measures. In addition, if the network has a

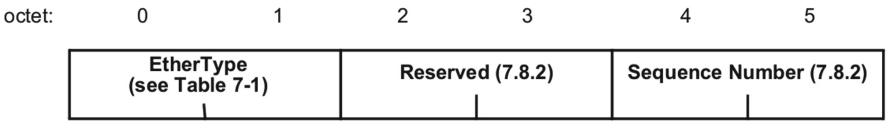

Figure 7-4—R-TAG format

Fig. 2. IEEE 802.1CB header format (from [17])

failure, the attacker can spoof enough packets so that the latent error detection function does not notice this, and it generates no warning signal, creating the illusion that the system is reliable.
- The attacker uses **tampering** by modifying existing packets to have random sequence numbers. This attack causes unexpected packets to drop and delivery of out-of-order packets. This effect will result in a **denial of service**.
- The attacker uses **tampering** by modifying the sequence number of replicate packets. This attack causes the same packet to arrive multiple times at the end destination without a way of detecting it. An adversary can use this to perform a replay attack.

4.2 Path Configuration

As some parts of the network are configurable during run-time, specific protocols enable the configuration of redundant paths and streams that could be abused. While this is not caused by IEEE 802.1CB as it does not provide this configuration, it affects the performance and reliability. These attack threats are described as follows.

- The attacker changes the network configuration to add multiple paths of redundant streams on the same link or multiple redundant streams on different links. This attack causes extra bandwidth usage and possibly higher latency due to this increased computing and throughput that is now required. Additionally, this attack will cause degradation in QoS and could lead to a **denial of service**.
- The attacker changes the network configuration to add intersecting paths. All packets will now go through switches that have received packets with the same sequence number earlier. These packets will be dropped and never delivered to the destination. This attack will result in a **denial of service**.

5 Existing Solutions

All the above mentioned attacks are widely known in the general networking community, and therefore there exist solutions to mitigate them. While not all of these solutions are designed explicitly for TSN, as this is a very recent technology, they are all designed for automotive networks and other related applications. In this section, we describe how these solutions work and analyze their effects on the KPIs required for TSN.

5.1 MACsec - 802.1AE-2018

MACsec is an IEEE standard that works at the medium access control layer. It works just below the IEEE 802.1CB standard as they both provide functionality to the data link layer. There has been research on the specific application of this standard to automotive Ethernet backbones and their performance and reliability [18]. Although this solution does not explicitly describe the security improvements of IEEE 802.1CB, it does ensure the confidentiality, integrity and authenticity of data within Ethernet frames resulting in mitigation of most attack threats described above. It replaces the existing Ethernet frames and encapsulates them into MACsec-compliant ones. The content is then encrypted and decrypted with symmetric keys by using AES-GCM. This solution depends on IEEE 802.1X for discovering network nodes and configuring and distributing the encryption keys and cryptographic parameters.

Ethernet frames consist of the destination address, source address and user data. MACsec makes the three following modifications to Ethernet frames.

- It adds a **SECTag** between the source address and the user data, which provides recognition of the MACsec frame and contains security information such as packet numbering, key length, and replay protection data. This section is 8 to 16 bytes long.
- If the packet requires confidentiality, the user data is optionally encrypted. The length of this section will be equally long as the original section.
- After the user data, it adds a 16 bytes long section for the Integrity Check Value. The **ICV** cover the integrity of the destination and source addresses and the integrity of the user data.

In [18], the authors provide a detailed descriptions of the actual hardware implementations and some design choices they have made regarding the automotive network environment. They also include performance tests of their implementation and conclude that their latency is smaller than 350 nanoseconds. This added latency is due to the increased packet size and the required calculations. Finally, they conclude that for a car driving 100 km/h, the physical delay will be less than a millimetre. Therefore this can even be used in safety-related systems such as a braking system.

5.2 MACsec - TSN-MIC

Another take at implementing MACsec for time-sensitive networking is called TSN-MIC [19]. This solution differs from other MAC-layer security schemes, such as the 802.1AE solution described in the previous section, as it only adds checking of the message integrity and no encryption of the payload data. Authors of [19] have first researched the performance of various lightweight cryptography solutions available. They decided on using Chaskey-12 as this is among the fastest algorithms available and is 7 to 15 times faster than AES-CMAC. In addition, this lightweight cryptography is provably secure, patent-free, and provides better

key agility than using a key schedule. For the configuration of encryption keys, they have decided on using a modified version of IEC 11770 over IEEE 802.1X. They conclude that their method is more efficient than IEEE 802.1X and more secure than IEC 11770.

This solution works just below the data link layer, and it would require no changes to the IEEE 801.1CB layer. They have implemented their solution and simulated the network to gain insight into the performance. The absolute added delay would be between 200 and 800 microseconds depending on the Ethernet frame size. This increase would cause a 35% delay to short frames and just a 1% delay to long frames. They conclude that their proposed security schema has a less significant impact on the delay than the frame payload size. Therefore, this will be a feasible solution to time- and mission-critical applications.

5.3 Chaos Cipher

The authors of [20] propose their Chaotic Cipher solution that ciphers the network traffic to hide the complete Ethernet traffic pattern without introducing overhead and throughput loss. For this, they use a stream cipher in combination with symmetric keys that are known to both end devices of a single network link. This solution provides a different approach as it implements a physical layer encryption method instead of a medium access control layer. One big gap in this paper is that they have no recommendation as to how keys should be shared and exchanged.

Their implementation works on the Physical Coding Sublayer (PCS) by directly encrypting the 8b10b symbol flow. This method provides physical layer encryption and obfuscates the traffic pattern as the control symbols such as start/end are also obfuscated. This layer consists of 256 data symbols and 12 control symbols, containing 268 possible symbols. It uses a symmetric key to generate a mapping of the original symbols to the ciphered symbols. This mapping can easily be reversed if the symmetric key is known. The keystream generation is based on the chaotic map method called Skew Tent Map (STM), which provides chaoticity and no periodic windows.

Finally, they conclude with a performance comparison related to other physical layer solutions. They show that their solution has the highest encryption throughput compared to other algorithms. Moreover, this is sufficient to support a Gigabit Ethernet connection without introducing additional delays.

5.4 KD and SC

The following solution proposes an application layer Key Distribution and Secure Communications module in [21]. This solution cannot prevent the security issues of IEEE 802.1CB as it works on a higher layer. However, it can detect possible attacks and encrypt the data so that attackers can not eavesdrop.

The Key Distribution Module works as a gateway during the start-up phase of the system by distributing the asymmetric keys to all legitimate end devices. The gateway has a database of identities and keys for each end device used to

exchange keys securely. Each end device has a hard-coded asymmetric key used only for this key exchange. This method ensures that an eavesdropping attacker cannot gain information about the encryption keys used for the subsequent communications.

Each supported end device should implement the Secure Communication Module, and it should provide the ability to encrypt, decrypt, and authenticate messages. For this, it uses DES and HMAC-MD5. In addition, it uses a sequence number to prevent replay attacks.

Finally, the authors provide a real-time performance evaluation of their proposed solution for both the key distribution and the impact on secure communication. This start-up delay is negligible because the key distribution is only done once on boot. However, the communication response time increases by 2 to 6 milliseconds depending on the CPU clock rate.

6 Evaluation of Attacks and Solutions

Table 1 shows a comparison of the different existing solutions in regards to the TSN KPIs and the discussed attack threats. Each attack scenario from Sect. 4 is shown with an indication if it can be prevented, detected, or if it is unaffected by the proposed solutions. This comparison is purely theoretical based on the description and details of the corresponding research paper.

Prevent means that the reviewed solution, in theory, has the ability to prevent these kinds of attacks from happening. Unaffected means that the reviewed solution has no effect on the attack feasibility. Detect means that the solution is able to notice that the network's communication has been tampered with, but is unable to prevent it from happening. Improve means that the reviewed solution has a positive effect on the amount of packet loss as it is able to filter out some malicious packets, therefore improving the number of legitimate packets that will arrive.

Table 1. Comparison of effectiveness for all reviewed solutions.

	802.1AE-2018 [18]	TSN-MIC [19]	Chaos Cipher [20]	KD & SC [21]
Latency	<350 ns	<800 μs	0	<6 ms
Jitter	–	–	–	–
Packet Loss	improve	improve	improve	–
Spoof DoS	prevent	prevent	prevent	unaffected
Spoof Error	prevent	prevent	prevent	unaffected
Tamper RND	prevent	prevent	prevent	detect
Tamper Replay	prevent	prevent	prevent	detect
Duplicate Paths	unaffected	unaffected	unaffected	unaffected
Intersect Paths	unaffected	unaffected	unaffected	unaffected

It is interesting to see significant differences in the introduced latency by the various solutions. The Chaos Cipher does not introduce any latency as it does not require any processing overhead because it merely shuffles the physical layer symbols according to a keystream generator. The KD & SC solution, on the other hand, introduces a significant latency of several milliseconds. It is expected from a higher-level solution to be slower, but this performance impact is several orders of scale slower than the other available mitigation solutions. Finally, the 802.1AE-2018 and TSN-MIC have only a slight latency impact. The main difference is that the TSN-MIC paper focuses explicitly on time optimization by picking the most performant encryption methods.

Jitter is one of the KPIs in Time-Sensitive Networking, but none of the reviewed solutions provides any information about the delay variation. We think including these measurements is essential to ensure the correct order of packet delivery within mission-critical systems. We assume the papers did not provide this information as they primarily provide theoretical solutions. The jitter should be measured by performing experiments on a hardware test-bed as many external variables could impact it.

Regarding packet loss, most papers can prevent some attacks and are therefore more resilient to accidental packet corruption or malicious actors trying to abuse the system. Unfortunately, they do not provide additional functionality to recover from link failures such as flipped bits. However, as the solutions provide detection of such failures, they can ensure to drop this incorrect packet to ensure that the correct packet travelling on a different path will continue. Therefore, by filtering bad packets, they can improve the number of correct packets arriving at the destination. For the KD & SC solution, they do not have an impact on the packet loss as it is an application layer solution.

Finally, as Table 1 shows, multiple solutions can prevent most attacks from happening. The physical and data link layer solutions can effectively prevent tampering with the packet and sequence number. However, they do not have an impact on malicious path configurations. If these solutions' limitations are resolved and implemented in a practical use case, they might provide proper mitigation.

7 Related Work

As TSN and especially IEEE 802.1CB are recent developments, there have not been widespread contributions to the research field. Especially concerning the security of these network standards, the current knowledge is limited. However, redundancy within industrial Ethernet networks has been an area of interest for quite some time. An excellent overview of available solutions has been provided by the authors of [22]. This paper describes the requirements of industrial networks and how they can be partially solved by using the Spanning Tree Protocol (STP) or the more recent Rapid Spanning Tree Protocol (RSTP). These protocols are currently implemented in many industrial networks. In addition, they provide an overview of 15 Ethernet redundancy solutions, and all of them have

a fail-over time ranging from 30ms to 30s. On the other hand, IEEE802.1CB has an instant fail-over time meaning that no packet loss will occur when one of the paths fails.

The authors of [11] provide an extensive overview of the recently published IEEE 802.1 TSN standards. It describes relevant applications for each standard, which aspects it focuses on, and how these standards can best be combined for optimal effect. The standards provide solutions related to Timing and Synchronization, Bounded Low Latency, Reliability, and Resource Management. A summary is given for all the introduced TSN standards, and finally, they conclude with some use cases to show their usefulness. It describes an industrial automation scenario and an automotive in-vehicle networking scenario. For both these scenarios, they recommend using IEEE 802.1CB to improve the reliability of the network communications.

However, security should be of the utmost importance for industrial networks, and therefore the authors of [16] provide an analysis of the security of IEEE 802.1 Time-Sensitive Networking. Just as in the previously mentioned paper, it categorizes the standards and provides a summary of each standard. The main contribution of this paper is its insights into the possible TSN threats. They theorize about threats such as Time Synchronization Threats, Scheduling Threats, Control and Orchestration Threats, and Policing and Redundancy Threats. This paper provided the starting point of our research into the Policing and Redundancy threats introduced by the IEEE 802.1CB standard. The paper concludes with the observation that security has not been one of the main design concerns for TSN as it prioritizes practicality and ease of use.

Finally, the authors of [7] provide a deep dive into the challenges and the limitations of IEEE 802.1CB. It identifies and theorizes possible challenges of this networking standard, such as Insufficient Buffer Dimensioning, Transmission Error Feedback, and Out-of-Order Delivery. In addition, when implementing this standard, there are certain limitations as each switch has to be configured individually. Furthermore, introducing redundant packets could create network inference, and this standard is still dependent on physical redundancy measures to provide disjoint paths. While this paper does not detail any security challenges or limitations, it provides interesting insights into the standard's limitations and suggests making a formal worst-case analysis framework to determine the possible impact.

8 Conclusion

As shown by the overview table in Sect. 6, there is significant overlap in the capabilities of most proposed solutions, and some interesting distinctions become apparent. One substantial similarity is that all these proposed solutions cannot prevent attacks based on the network configuration. This limitation is expected as the IEEE 802.1CB standard is not responsible for the routing and network configuration. Therefore, further research should be done to identify security measures to mitigate these threats.

The most significant difference between these algorithms is the latency impact they have. As the Chaos Cipher and TSN-MIC have a latency impact lower than 1ns, they can most likely be used for all mission-critical applications. On the other hand, the 802.1AE-2018 solution has a higher impact on the latency and is therefore limited in its applications. However, the paper ensured that it is sufficient for automotive networks. Finally, the KD & SC solution has a very high latency mainly due to its implementation in the application layer instead. In addition, this solution cannot prevent any attacks and only provides detection for a subset of the threats.

As these solutions provide no information about their effects on the jitter, we suggest that further research should be done to identify the impact.

This paper provides a threat overview by using the STRIDE model and we recommend further research to focus on a corresponding risk assessment to analyze the exact impact of these identified threats.

Finally, looking at the latency impact and the prevention of security threats, we can conclude that both the TSN-MIC solution and the Chaos Cipher would be feasible. While both solutions have certain drawbacks, further research can improve upon these proposed mitigations. Alternatively, combining them might provide a complete solution.

References

1. Finn, N.: Introduction to time-sensitive networking. IEEE Commun. Stand. Mag. **2**(2), 22–28 (2018)
2. Alcaraz, C., Roman, R., Najera, P., Lopez, J.: Security of industrial sensor network-based remote substations in the context of the internet of things. Ad Hoc Netw. **11**(3), 1091–1104 (2013)
3. Case, D.U.: Analysis of the cyber attack on the Ukrainian power grid. Electricity Inf. Sharing Anal. Center (E-ISAC) **388**, 1–29 (2016)
4. Lee, R.M., Assante, M.J., Conway, T., SANS Industrial Control Systems: ICS CP/PE (Cyber-to-Physical or Process Effects) Case Study Paper-Media report of the Baku-Tbilisi-Ceyhan (BTC) pipeline Cyber Attack (2014)
5. Slay, J., Miller, M.: Lessons learned from the maroochy water breach. In: International Conference on Critical Infrastructure Protection, pp. 73–82, March 2007
6. Farwell, J.P., Rohozinski, R.: Stuxnet and the future of cyber war. Survival **53**(1), 23–40 (2011)
7. Hofmann, R., Nikolić, B., Ernst, R.: Challenges and Limitations of IEEE 802.1 CB-2017. IEEE Embedded Syst. Lett. **12**(4), 105–108 (2019)
8. Teener, M.D.J., et al.: Heterogeneous networks for audio and video: Using IEEE 802.1 audio video bridging. Proc. IEEE **101**(11), 2339–2354 (2013)
9. Nasrallah, A., Thyagaturu, A.S., Alharbi, Z., Wang, C., Shao, X., Reisslein, M., ElBakoury, H.: Ultra-low latency (ULL) networks: the IEEE TSN and IETF DetNet standards and related 5G ULL research. IEEE Commun. Surv. Tutorials **21**(1), 88–145 (2018)
10. IEEE Standards Association. (2018). IEEE Standard for Local and Metropolitan Area Network-Bridges and Bridged Networks. IEEE Std 802.1 Q-2018 (Revision of IEEE Std 802.1 Q-2014): 1–1993 (2018)

11. Bello, L.L., Steiner, W.: A perspective on IEEE time-sensitive networking for industrial communication and automation systems. Proc. IEEE **107**(6), 1094–1120 (2019)
12. Ergenç, D., Fischer, M.: On the Reliability of IEEE 802.1 CB FRER. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications, pp. 1–10. May 2021
13. Prinz, F., Schoeffler, M., Lechler, A., Verl, A.: End-to-end redundancy between real-time I4. 0 Components based on Time-Sensitive Networking. In: 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), vol. 1, pp. 1083–1086, September 2018
14. Pannell, D., Navet, N.: Practical Use Cases for Ethernet Redundancy. In: 2020 IEEE Standards Association (IEEE-SA) (2020)
15. Shostack, A., Hernan, S., Lambert, S., Ostwald, T.: Uncover Security Design Flaws Using The STRIDE Approach. MSDN Magazine 2006.11, November 2006
16. Ergenç, D., Brülhart, C., Neumann, J., Krüger, L., Fischer, M.: On the security of IEEE 802.1 time-sensitive networking. In: 2021 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6, June 2021
17. Frame Replication and Elimination for Reliability, IEEE standard P802.1CB, 2017
18. Carnevale, B., Fanucci, L., Bisase, S., Hunjan, H.: Macsec-based security for automotive ethernet backbones. J. Circuits Syst. Comput. **27**(05), 1850082 (2018)
19. Watson, V., Ruland, C., Waedt, K.: 2021. MAC-layer Security for Time-Sensitive Switched Ethernet Networks, INFORMATIK (2020)
20. Pérez-Resa, A., Garcia-Bosque, M., Sánchez-Azqueta, C., Celma, S.: Using a chaotic cipher to encrypt Ethernet traffic. In: 2018 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1–5, May 2018
21. Wang, C.T., Qin, G. H., Zhao, R., Song, S.M.: An information security protocol for automotive ethernet. J. Comput. **32**(1), 39–52 (2021). International Symposium on Circuits and Systems (ISCAS), pp. 1–5
22. Prytz, G.: Redundancy in industrial Ethernet networks. In: 2006 IEEE International Workshop on Factory Communication Systems, pp. 380–385, June 2006