Journal of Computer Science and Artificial Intelligence
ISSN: 3078-8242 (Print), ISSN: 3078-2309 (Online) | Vol. 4, No. 1, 2025

A Review of Research on Secure Time Synchronization Technology of Precision Time Protocol

Yanqing Xu

Southwest Minzu University, Chengdu 610000, China

Abstract: Precision Time Protocol (PTP) is the core implementation of the IEEE 1588 standard and is widely used in areas such as power, industrial Internet, financial transactions and communications that require extremely high time synchronization accuracy. However, with the deployment of PTP in an open network environment, the security mechanism it lacked at the beginning of its design gradually exposed serious vulnerabilities and became an important target for attackers. In recent years, the security research on PTP has been deepened, covering multiple directions such as attack classification, protection methods, key management mechanism, protocol optimization and standard updates. This article is based on more than 40 relevant research literatures at home and abroad in the past decade, and conducts a systematic review of PTP security issues. First, the threat types under different attack models are summarized, including delayed attacks, replay attacks, message tampering, spoofing and denial of service, etc.; then, existing protection measures are sorted out, from the message authentication code (MAC) scheme of IEEE 1588 Appendix K, to multicast authentication mechanisms such as TESLA, IPsec/MACsec-based link encryption, hardware trusted nodes, blockchain and quantum cryptographic enhancement schemes, etc.; then, various key management and distribution strategies are analyzed, including NTS4PTP, centralized and distributed key exchange, post-quantum key negotiation and other technologies. The review shows that the focus of future PTP security research will focus on four directions: lightweight, high security authentication, low-latency key update, anti-quantum attack mechanism, and cross-layer comprehensive protection, so as to provide end-to-end verifiable security guarantees while ensuring nanosecond synchronization accuracy.

Keywords: IEEE 1588, PTP, time synchronization security, multicast authentication, key management, anti-quantum cipher.

1. Introduction

High-precision time synchronization is the cornerstone of modern information infrastructure. In application scenarios such as power scheduling, 5G communication, financial high-frequency trading, and industrial automation, the nanosecond clock consistency not only determines the operating performance of the system, but also directly affects safety and stability. As an implementation solution of the IEEE 1588 standard, Precision Time Protocol (PTP) has become one of the mainstream time distribution technologies worldwide with its microsecond to nanosecond synchronization capabilities. However, PTP paid more attention to synchronization accuracy and implementation efficiency in the initial design stage, and lacked defense design for cyber-attacks, which gradually became a security risk after it was deployed to open network and industrial IoT environments.

In recent years, the number of attacks and vulnerabilities disclosed against PTP has continued to increase. For example, a Delay Attack can introduce time deviations without being detected; a Replay Attack can use historical messages to destroy synchronization stability; a Malicious Master Attack can inject error time information across the entire network. These attacks not only threaten the system's functions, but may also cause chain security accidents. With the release of IEEE 1588-2019 version, more security extensions have begun to be introduced at the standard level, but there are still shortcomings in key management, performance overhead, compatibility, etc.

Academic and industrial circles have proposed a variety of improvement solutions for this, including: symmetric message authentication code (MAC) scheme based on Appendix K, delayed key disclosure multicast authentication mechanisms such as TESLA, IPsec/MACsec-based link encryption, FPGA hardware accelerated authentication, blockchain decentralized trust management, and anti-quantum computing scheme combining quantum random numbers and post-quantum cryptography. At the same time, key management has become a key link, from the early static pre-shared key development to dynamic centralized distribution (such as NTS4PTP), distributed key negotiation and post-quantum secure key exchange.

This article aims to systematically sort out the research results and development trends in the field of PTP security in the past decade. The full text structure is arranged as follows: the second part introduces the evolution of the PTP protocol and its three major versions of security mechanisms; the third part reviews the main types of attacks and threat models facing PTP; the fourth part analyzes the progress of existing protection technologies and standardization; the fifth part explores the trade-off between key management solutions and synchronization accuracy; the sixth part reviews existing research and proposes future development directions.

2. Research Status

With the rapid development of industrial automation, power system intelligence, 5G communications and financial transaction networks, precise time synchronization has become an important basis for ensuring the reliable operation of these fields. Precision Time Protocol (PTP), or the IEEE 1588 protocol, has gradually become the mainstream solution for network clock synchronization with its high precision and low latency. The PTP protocol can achieve high-precision time synchronization at submicron seconds or even nanosecond levels, so it has been widely deployed and applied in scenarios with high real-time requirements.

However, the initial design of the PTP protocol focused primarily on synchronization accuracy without sufficient

security consideration. This design flaw makes the PTP protocol face many security risks in practical applications, including but not limited to message tampering attacks, replay attacks, delay attacks, and denial of service attacks. In recent years, as the importance of network security in the critical infrastructure field continues to increase, attacks and security vulnerabilities against the PTP protocol have gradually increased, making the security issues of the PTP protocol a focus of common attention in academic and industry. Once the security problems of the PTP protocol break out, it may lead to a serious reduction in the accuracy of time synchronization, which will lead to communication interruptions, data corruption and even more serious security accidents. Therefore, studying and analyzing the security threat model of the PTP protocol and exploring effective security protection mechanisms have become an important issue that needs to be solved urgently in the field of network synchronization.

2.1. PTP Protocol Version and Security Evolution

Precision Time Protocol (PTP) is a clock synchronization protocol used for the entire computer network with relatively high accuracy. In LANs, accuracy can reach submicron seconds, making it suitable for measurement and control systems. PTP is used to synchronize financial transactions, mobile tower transmissions, subsea acoustic arrays, and networks that require precise timing but cannot access satellite navigation signals.

IEEE 1588-2002 [1] (PTP v1) is the initial standard for PTP. The design goal of this version is to provide high-precision time synchronization capabilities for measurement and control systems, especially those industrial LAN environments that cannot afford the cost of GPS hardware. It defines core architectural elements such as master/slave clock, border clock, transparent clock, BMCA (optimal master clock algorithm). However, this version mainly focuses on synchronization accuracy and scalability, and does not introduce any built-in security mechanism in the standard. All messages are transmitted in plain text, and there is no authentication and encryption function. This means that as long as an attacker can access the network, he can easily listen, tamper with or even forge PTP messages, thereby destroying synchronization.

In order to cope with the higher requirements for time synchronization accuracy and security in the fields of industrial automation, energy and communications, IEEE released the second version of PTP, namely IEEE 1588-2008 (v2) [2] in 2008. This version has made significant improvements in synchronization performance, network adaptability and security. In terms of synchronization performance, v2 introduced new transparent clock mechanism, boundary clock, announce message (for BMCA operation), single-step and two-step timestamp modes and other improvements, optimizing the delay measurement mechanism, significantly improving accuracy and robustness; in terms of security, v2 introduced the protocol built-in message authentication mechanism in Appendix K (Annex K) for the first time. Annex K uses the HMAC-SHA1 algorithm based on symmetric keys to calculate the message authentication code (MAC) and append it to the end of the message with a TLV (Type-Length-Value) field. The master and slave parties need to pre-share the same symmetric key before synchronization. After receiving the message, the receiver uses the key to recalculate the HMAC and compare it with the authentication code in the message to verify whether the message has been tampered with or forged during transmission.

In the study of Annex K security extension in the IEEE 1588-2008 (PTP v2) standard, Hirschler and Treytl [3] first paid attention to the correctness verification problem of this mechanism in actual deployment in 2011, and proposed a systematic verification and testing framework, which divided the security functions defined by Annex K into four core areas: (1) Message integrity protection; (2) Group authentication; (3) Security association management; (4) Key and life cycle update process. Based on these four fields, the author designed 13 comprehensive test cases, including: location and length check of message format and authentication TLV, generation and verification of ICV (integrity check value), consistency and validity verification of KeyId, triggering and window management of replay attack protection mechanisms, correctness and timeout processing of challenge-response processes, establishment and switching of static and dynamic security associations, capacity limitation of security association tables (SA tables), and correct update of key and lifecycle IDs. This test method combines the idea of black and white boxes. On the one hand, it detects the security response of the protocol stack through external message interaction. On the other hand, it requires the device under test (TOE) to record and export internal security events during operation, so that the testers can independently verify the Annex K implementation on a platform composed of reference devices, secure transparent clocks and monitoring devices. This method has been verified in the PTP implementation of Oregano Systems, with good portability and low experimental conditions (no high clock synchronization accuracy required), and is suitable for security testing of both ordinary and transparent clocks.

In the same year, on this basis, Treytl and Hirschler [4] further proposed improvement solutions to Annex K's structural shortcomings in security. The author pointed out that the original Annex K relies on SHA-1-based HMAC for message integrity protection and group authentication, but still has hidden dangers in resisting replay attacks, message forgery, and widespread damage caused by key leakage, and overall security is highly dependent on the secure distribution and management of keys. To this end, the research proposes several implementation improvements, including the use of higher quality random number generators to enhance the unpredictability of keys and challenge values, tightening the playback window management strategy, and stricter verification of the format and location of the authenticated TLV. In order to quantify the performance and security differences of different message authentication code (MAC) algorithms under the Annex K framework, the author implemented and tested the HMAC scheme based on hash functions such as SHA-1, SHA-256, SHA-512, etc. on the experimental platform to compare its performance in calculation overhead, processing delay and security margin. Experimental results show that a stronger hash function (especially SHA-256) can significantly increase the security margin while introducing only limited delay overhead, so it can be used as a better choice in most PTP application scenarios.

IEEE 1588-2019 [5] is the third version of PTP, a compatibility upgrade to the 2008 version, aiming to improve time synchronization accuracy and protocol security, and

formally integrate security mechanisms into core standards.

In 2022, Chang Siqi and Chu Yingjun [6] systematically analyzed the optimization of the IEEE 1588-2019 (PTP v2.1) protocol in terms of high precision, security, flexibility and performance monitoring, and explained it in combination with typical vertical industries such as telecommunications, power, radio and television, finance, and industrial control. In terms of security, the paper pointed out that PTP has a long-term lack of security control. The 2019 edition has significantly enhanced its defense capabilities by introducing four types of security and protection mechanisms: (1) Integrated security mechanism: by extending TLV to carry symmetric key-based identity authentication and integrity verification value (ICV) in PTP messages, supporting instant or delayed verification, ensuring that the message is not tampered with and trustworthy source; (2) External security mechanism: using IEEE 802.1x MACsec or IPsec to establish a secure tunnel between PTP instances to resist external attacks, but the impact on delay and synchronization accuracy is required; (3) Network redundancy mechanism: prevent single point of failure or malicious nodes from disrupting synchronization through multi-master clocks, cross-domain majority voting, and redundant path distribution; (4) Monitoring and management mechanism: introducing standardized performance data interfaces to detect abnormal offsets or delay changes in real time to identify potential attacks. The author believes that these mechanisms improve the security and robustness of PTP networks, but in actual applications, it is necessary to optimize deployment in combination with industry configuration files and take into account the balance between security and precision.

2.2. Attack Model and Threat Analysis

2.2.1. Delay Attack

Delayed attacks are the most obscure and destructive type of attacks against PTP. The attacker does not need to tamper with the content of the message, but instead increases the delay of the message transmission path, so that the master and slave clocks can obtain error results when calculating the delay compensation, resulting in a synchronization offset. Attack methods can be divided into: fixed delay injection: the attacker artificially inserts fixed delays in the link, causing the slave clock to shift the overall time; random delay injection: randomly adds delays to each message, resulting in frequent clock adjustments, causing synchronization instability; asymmetric delay attack: injects different delays to the Sync and Delay_Req paths respectively, breaking the symmetric link assumptions of PTP.

2.2.2. Replay Attack

In a replay attack, the attacker captures historically valid PTP messages and resends them at some time later. This can cause the slave clock to synchronize with expired timestamps, thereby introducing bias. Replay attacks can be implemented without destroying message integrity, so even if Annex K is enabled, there is no complete defense.

2.2.3. False Master Attack

Fake master clock attacks exploit the flaw of PTP's lack of authentication. The attacker broadcasts fake Announce messages to the network, claiming that he is the highest priority master clock, thereby inducing the slave clock to switch the synchronization source. Once it becomes the main clock, the attacker can directly control the entire network time.

2.2.4. Denial of Service attack (DoS)

DoS attacks target the availability of PTP. Attackers can implement it in the following ways: message flooding: sending a large number of forged PTP messages to flood the processing queue; blocking key messages: filtering out Sync, Follow_Up or Delay_Resp messages to cause clocks to lose pace; resource exhaustion: defects implemented using PTP (such as memory leaks) cause device exceptions.

2.3. PTP Protection Technology

In 2021, Zhang Meng and Lu Bo [7] analyzed the main threats faced by the Precision Time Protocol (PTP) in untrusted networks in response to the security requirements of future information networks for high-precision and high-reliability time synchronization, and verified the harm of message tampering attacks and delayed attacks through experimental simulations. The results show that message attacks can significantly reduce synchronization accuracy by modifying the timestamp, while delay attacks use link asymmetric delay to continuously pull slave time without being noticed. In response to the shortcomings of traditional encryption that cannot effectively defend against delayed attacks, the author proposes a quantum enhanced secure time synchronization protocol: symmetric encryption is used in the PTP layer to ensure the confidentiality and integrity of packets, and an independent quantum channel is established in the key distribution layer, and the time deviation is compared with the PTP deviation through quantum measurement, and the delay attack warning and time source switching are triggered when the difference exceeds the threshold. Experimental analysis shows that this protocol can defend against message tampering and delay-type attacks at the same time, and its impact on synchronization accuracy is controllable (jitter remains at microseconds or submicrons).

In 2018, Wang Weizhao [8] designed a secure time synchronization method based on node identity recognition based on node identity recognition to detect illegal information using the timestamp correlation between nodes and the uniqueness of the node clock slope, rather than simply isolated suspicious nodes. During the detection process, each node determines whether the information is reliable and filters invalid information based on the relative clock slope relative to its common neighbor. NiSTS can resist witch attacks and information manipulation attacks, and is insensitive to the number of witch attackers in the network.

In 2023, Zhang Ying [9] et al. proposed a detection and recovery model combining Markov Logic Tree (MLT) and system brittleness analysis based on the problem that PTP and other time synchronization protocols are vulnerable to delay attacks in smart substations. This method first constructs an MLT model based on the communication logic and device dependency of the substation network, represents the event chain that may be caused by delayed attacks in the form of probabilistic logic, and introduces a system fragility analysis method to quantify the vulnerability of key devices or links under attack. By monitoring and historical baseline comparison of synchronization packet delay characteristics, the model can identify latency attack signs early and combine MLT inference to determine the affected synchronization path and devices. In order to achieve rapid recovery after attack, the author designed a path switching and clock resynchronization strategy, and preferred redundant link recovery synchronization services with low brittleness and normal latency. Experimental results show that this method

can effectively detect static and dynamic delayed attacks in the IEEE 1588 environment, with detection accuracy higher than 95%, and the recovery time is about 30% shorter than traditional methods.

In 2022, Waleed Alghamdi and Michael Schukat [10] proposed to enhance IEEE 1588 PTP security with trusted supervision nodes (TSN): TSN centrally collects offset, delay and key timestamp information (t1, correctionField, EMT, syncID) of slave clocks, reorganize according to the synchronization cycle and compare it with the baseline; designs two types of TSNs, Type-A (statistical method) and Type-B (local high-stable independent clock + PTP slave clock), and two algorithms "synchronous link attack detection/time source attack detection"; use threshold, continuous suspicious message count and LCA (lowest public ancestor) for abnormal judgment and attack location coarse position, and reinforce TSN through TPM/PKI With the reporting link, and do not have to rely on additional time reference. Experiments show that the system can detect tampering with packet content, delayed manipulation, playback/spoofing, and DoS, and can identify time-source degradation and BMCA attacks; among them, Type-B can find the "quietest" time-source attacks even if the slave parameters still fall into the normal range; this scheme serves as a monitoring layer to provide additional defense for PTP.

In 2021, Lei Peng et al. [11] proposed a secure clock synchronization device and method for the Industrial Internet of Things (IIoT) in his invention patent, aiming to enhance the quantum computing attack resistance and bidirectional authentication capabilities of the timing link based on NTP and PTP. Its core innovations include: embedding quantum random number generators in the clock synchronization hardware module, combining ID-based Signcryption and Ring-LWE-based post-Quantum KEX to achieve "one password at a time" message encryption, lightweight authentication and forward security. The device tames the clock with Beidou/GPS, and uses true random numbers to drive session key generation to avoid the predictability of pseudo-random numbers. During the synchronization process, the central master node acts as the trusted key generation center, and implements node identity and time slot control through IDA/IDB binding to the hierarchical absolute serial number; the handshake stage uses ciphertext compression and feature extraction to reduce traffic, and rejects sessions when the timestamp difference exceeds ΔT to prevent playback and delay attacks. On the premise of ensuring security, short messages and low computing complexity are used to meet the requirements of industrial sites for efficient authentication and forward security, and improve practicality and flexibility.

In 2020, Eyal Itkin and Avishai Wool [12] conducted a systematic study on the shortcomings of the existing security extension Annex K, the IEEE 1588 Precision Time Protocol (PTP), and firstly, starting from the threat model, it conducted an in-depth analysis of the vulnerability of PTP in the startup phase, key management, computing delay, and delayed attack defense, pointing out core issues such as Annex K lacks effective authentication before three handshakes, reliance on manual pre-sharing keys, low computational efficiency of HMAC-SHA1 and inability to detect latency manipulation. To this end, they proposed a revised PTP security extension solution: in terms of method, the improved security handshake protocol is used to implement dynamic security association (SA) establishment and key distribution, replace the original HMAC-SHA1 as a hardware-friendly AES-CMAC to reduce authentication delay, introduce a sequence number and timestamp binding mechanism to enhance playback attack detection, and add a dwell time authentication field in transparent clock mode to prevent intermediate nodes from tampering. Through the experimental platform, the performance of the original Annex K and the revised solution was compared, and the certification delay, synchronization accuracy and protection capabilities were measured. The results showed that the certification delay of the revised version dropped below half of the original solution with the support of hardware acceleration, which had negligible impact on synchronization accuracy, and significantly improved the anti-tampering and anti-playback capabilities.

In 2025, Zeba Idrees et al. [13] proposed a lightweight attack detection and mitigation framework for the security vulnerability of IEEE 1588 (PTP) in the industrial Internet of Things (IIoT) network: collecting slave clock synchronization status (SS/SSR) around monitoring nodes (MU), comparing the master station Sync and slave timestamps; when confirming that the master clock is attacked, the active transparent clock (ATC) participates in BMCA and takes over as a temporary master clock; expands the slave clock to report the above key timing. Methods The detection delay, synchronization error and network overhead are evaluated by comprehensively sorting out the attack surface and simulation under OMNeT++ multi-topology; the results show that the attack points such as GMC/BC/TC/link are covered, and the detection delay is inversely proportional to the SS frequency. In the worst case, the new traffic is about ~1 KB/s, and the attack accuracy is often 30–200 B/s without attacks, and the overall synchronization accuracy is not sacrificing.

In 2024, the robustness of Petrică Ciotirnae and Adrian Florin Păun [14] Time Reference Distribution Equipment (TSU) for Telecommunications Networks under GNSS spoofing/interference and PTP attacks, proposes a multimodal security monitoring architecture based on blockchain: in a tree PTP network, each TSU monitors the key parameters of GNSS reception, PTP module, optical port distribution and remote management for each TSU. If an exception occurs, it cannot be tampered with the link-on-winding and full-network association analysis through the "Hyperledger Fabric"; and is accompanied by GNSS OS-NMA (TESLA delay disclosure) and PTP AUTHENTICATION TLV (GDOI) Group key, instant processing)" authentication mechanism, the gateway isolates TSU and transmits alerts with TLS/WebSocket. The experimental results show that this solution can gather the alarm and operation data of the entire network without tamperingly, quickly identify GNSS spoofing/blocking, PTP and management channel security events at the TSU level, and judge whether it is a single point, regional or network-level attack based on the alarm timestamps and geographical distribution of different TSUs, and has the potential to scalability and adapt to smart contracts.

In 2021, Langer and Bermbach [15] proposed a PTP instant authentication key management solution based on NTS (RFC 8915), and are independent of NTP operation. Two types of key distribution modes are designed and standardized: the "group-based (including Go2 subgroup)" for multicast/mixed mode and the "ticket-based" mode for unicast and scalable "ticket-based" mode. The NTS-KE extension messages and fields such as PTP Key Request/Grant/Refusal, Registration Request/Success/Revoke, etc. are defined, and the secure

channel is required to be established through TLS 1.3 and X.509 bidirectional authentication, giving the operation process and parameters for key rotation and transparent clock participation. Extend message/record types on existing NTS-KEs, formally define state machines and timing (including update/authorization/certificate configuration, etc.), and discuss deployment constraints and security considerations (such as KE server redundancy, DoS risk, time during startup phase, and certificate dependencies). Experimental results show that the scheme provides automatic key management for PTP's AUTHENTICATION TLV, covering multicast and unicast scenarios without relying on NTP, making it easier to integrate with existing TLS/PKI infrastructure.

In 2022, Filip Rezabek et al. [16] system implemented and evaluated the PTP security extension based on IEEE 1588-2019 Annex P (Prong A), added AUTHENTICATION TLV/HMAC to linuxptp, accompanied by SPD/SAD, adopted instant processing, and quantified its impact on synchronization accuracy on reproducible laboratory bench with COTS hardware + open source toolchain; at the same time, a linear 4–9 jump topology was built, E2E, P2P and transparent clock (TC), and evaluated a variety of HMACs (SHA-512/256, BLAKE2b, BLAKE3) and "100 μs False delay", comparing the short/long path two-domain clocks, counting the mean and standard deviation, and examining the configuration of different logSyncInterval and the TC residence time distribution, the measurement system accuracy is about ±40 ns. Experimental results show that the safety expansion does not significantly degrade synchronization: the number of hops of E2E/P2P rises to about 118.6–571 ns, while the standard deviation after the introduction of TC is about 90–140 ns; the TC residence delay is only increased by a few microseconds compared to "no safety"; no additional jitter caused by the safety expansion is observed under different logSyncInterval combinations.

In 2019, Prasanth Kemparaj and S. Satheesh Kumar [17] proposed "Fully PTP Integrated Security (F-PTPIS)" against the threats listed in RFC 7384 [18]: by adding new PTP general messages and TLVs, encryption, authentication and key management are directly embedded into the protocol process, avoiding "out-of-band" protection that only relies on IPsec/MACsec. By giving end-to-end secure timing message exchange process and state machine, chain updates of the (message) correction field carry the next round of required keys/parameters for continuous protection. Experimental results show that F-PTPIS can cover the main attack surfaces such as tampering, forgery, playback, pseudo-master station and delay manipulation, and based on this, a "resolved" correspondence is given item by item to the RFC 7384 threat.

In 2010, Treytl and Hirschler [19] systems analyzed the feasibility and impact on synchronization accuracy of using IPsec tunnels, and pointed out that its motivation is to reduce key and connection maintenance costs across applications with unified tunnels. IPsec (AH/ESP, transmission/tunnel mode) and 1588 native security extension were analyzed, and the "Security Processing-Timestamp-Protocol Stack" coupling model was established. Based on Linux/IP stack inserts, the delay and jitter of the transceiver paths under different security configurations were measured, and the architectural trade-off between one-step/two-step clock and hardware timestamp was discussed. At the same time, the key kernel functions are calculated and the end-to-end processing time of AH/ESP in transmission/tunnel mode is counted, and the baseline (pure IP) comparison and 10,000 sample statistics are given. The experimental results show that the reception path introduces additional jitter of about 2–3 μs due to the interaction between the security processing and the protocol stack, while the transmission path is almost non-incremental (about 0.02 μs). Low-precision applications can "directly fit IPsec", while high-precision applications need to be targeted to modify hardware and algorithms. The "two-step clock" can basically eliminate the impact of the security layer on the timestamp accuracy, but the cost is the increase in bandwidth and implementation complexity. If you pursue the nanosecond accuracy of the one-step clock, you need to focus on ICV/AD in the MAC, and even overclock the encryption unit to catch up with the line speed, which increases the difficulty and cost of implementation.

In 2014, Naiara Moreira et al. [20] proposed the idea of using SHA-3/KECCAK to build PTP message MAC on programmable hardware to reduce the delay and area overhead brought by Annex K using HMAC-SHA1/256, and is aimed at high-precision secure timing for smart grid IEC 61850/IEC 62351 scenarios. Main work: Implement KECCAK [400] (capacity 256 bits) on the FPGA core on Xilinx Virtex-5 (supports K round expansion), and compare it with the open-source AES-128 CMAC core in three aspects: resource occupation, frequency and packet processing delay (clock cycle), and supplement the analysis of the performance shortcomings of Annex K design and HMAC and its impact on TC residence delay/key management. The Annex K/ICV verification process and HMAC structure were analyzed, the KECCAK hardware architecture was designed and the round expansion implementation of K=1…5 was implemented. After unifying the comprehensive options, the number of cycles, maximum frequency and LUT/FF/BRAM usage of the two types of cores under different K were measured, and the embedibility of the TC architecture was discussed. Experimental results show that at the same security level, KECCAK[400] achieves a time delay comparable to AES-128 with higher hardware efficiency (no S-Box and Boolean operations as the main one), and has a better overall area when K≥3; it is recommended that the future IEEE 1588 version consider SHA-3 based on MAC to reduce the cost of security to synchronization performance.

In 2021, Mino Sharkhawy [21] proposed the Secure Time-PTP integration solution to solve the bottleneck problem of IEEE 1588 protocol's resistance to delay attacks. DTLS-based session initialization and NTS-inspired cookie-type round-trip delay measurement authentication are designed to avoid saving slave states on the master clock and suppressing large-scale attacks; then prototyped on Linux PTP, and built a "two Beagle bone Black+GPS" measurement platform and a configurable delay attack device based on DPDK, and compared and evaluated the accuracy and attack resistance of "standard PTP vs. SecureTime-PTP". Methodically, the public key signature protects synchronization packets, serial number/session key management, as well as the upper bound constraints on RTD and maximum synchronization intervals, and clarify the key points and limitations of coexisting with transparent clock/hybrid networks. Experimental results show that under the correct parameter configuration, SecureTime will not reduce the synchronization accuracy of PTP and can detect and limit multiple types of delayed attacks.

3. Literature Review

Focusing on the security reinforcement of IEEE 1588, recent work is roughly divided into three paths: outer

transmission encryption (such as IPsec/MACsec), message authentication and management optimization endogenous to protocols, and a lightweight security framework that can identify delay attacks on PTP. Overall, these three types of solutions have their own choices between "deploy ability-precision-resistance-resistance attacks".

First, the representative analysis of IPsec used to protect PTP points out that IPsec (AH/ESP, transmission/tunnel mode) can unify a variety of services, including PTP without changing the application. However, it inevitably introduces encryption and decryption and ICV recalculation in the sending path, amplifying the coupling between the timestamp generation and the message is sent, thereby increasing jitter; if the hardware timestamp is used for the receiving path, the impact can be minimized. Actual measurement and modeling show that IPsec can be "out of the box" for low-precision synchronization; while high-precision (nanosecond/sub microsecond) scenarios require dedicated hardware and algorithms to cooperate, and two-step clocks are preferred to decouple timestamps from authentication calculations, otherwise the timestamp of one-step clocks will be directly affected by the security module delay. It should also be noted that end-to-end encryption will limit the update of the clear clock to the correctionField, further affecting the accuracy and compensation ability for asymmetric delays.

Second, for "hard real-time" scenarios such as power substations, the academic community has made performance analysis and replacement attempts for PTP's built-in symmetric key scheme (Annex K). Annex K uses HMAC-SHA1/SHA256 to implement source authentication and playback protection, but in large-scale deployment, problems such as startup congestion, complex key/session management, and longer transparent clock residence time are exposed. In particular, the area and delay overhead of HMAC on FPGA/ASIC are not friendly to real-time. To this end, some work has proposed a MAC with SHA-3/KECCAK as the core, and implemented it on FPGA to reduce latency and resource usage, and to match the requirements of the IEC 61850 process bus for sub microsecond synchronization and low jitter; actual measurement comparison shows that compared with traditional HMAC/AES-CMAC implementations, KECCAK-MAC has more advantages in hardware efficiency and delay, thereby improving authentication throughput and scalability without sacrificing synchronization accuracy.

Third, for the "selective delay" type of attack that cannot be blocked by encryption, the SecureTime idea superimposed on PTP has emerged: using fast elliptic curve signatures for data source authentication, and at the same time, applying "hard boundary" and handshake/measurement authentication to the message delay through the protocol side to significantly improve the detectability of delayed attacks. The engineering transformation for PTP includes: completing session initialization with DTLS, authenticating round-trip measurements with reference to NTS cookies, trying to avoid maintaining the slave clock status on the master clock side, and analyzing the compatibility of transparent clocks and hybrid nodes when coexisting. Prototypes based on LinuxPTP and rigorous GPS benchmarking measurements show that under correct parameterization, SecureTime will not significantly degrade PTP accuracy and can identify multiple delay attacks.

In summary: If "fast online and unified protection" are first, IPsec is suitable for medium accuracy and edge/wide-area interconnection, but it needs to fully evaluate its impact on one-step clock and transparent clock, and give priority to the combination of two-step and hardware timestamps; if "end-to-end real-time" is first, a more efficient PTP endogenous MAC (such as SHA-3/KECCAK) can complete source authentication while maintaining microsecond/sub microsecond accuracy, reducing the implementation overhead of Annex K; and in high-confrontation scenarios where "must confront time delay manipulation" (financial matchmaking, protection control, etc.), superimposing the measurement authentication and delay boundaries of SecureTime class is the key to making up for the shortcomings of "unable to block delay attacks by encryption alone", but it requires a certain amount of protocol stack transformation and operation and maintenance complexity. A pragmatic route is: two-step PTP+hardware timestamps are used as the base, efficient MAC is used for source authentication within the protocol, IPsec is used for channel reinforcement across domain links, and monitoring and alarms of measurement authentication/delay thresholds are introduced in key segments to achieve a more robust balance between accuracy, deployment cost and offensive and defense capabilities.

4. Conclusion

Overall, PTP security technology is transforming from single-point reinforcement to systematic protection, from static keys to dynamic multi-party security negotiation, and from single algorithm to multi-mechanism fusion. This evolution path is not only driven by security threats, but is also closely related to the strategic position of high-precision time synchronization in the fields of electricity, communications, finance, industrial control, etc. The core of future research will be how to achieve end-to-end, cross-domain, and cross-layer verifiable security protection while ensuring sub-microsecond or even nanosecond synchronization accuracy.

References

[1] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," in IEEE Std 1588-2002 vol., no., pp.1-154, 31 Oct. 2002.

[2] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," in IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002), vol., no., pp.1-269, 24 July 2008.

[3] B. Hirschler and A. Treytl, "Validation and verification of IEEE 1588 Annex K," 2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication, Munich, Germany, 2011, pp. 44-49.

[4] C. Önal and H. Kirrmann, "Security improvements for IEEE 1588 Annex K: Implementation and comparison of authentication codes," 2012 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication Proceedings, San Francisco, CA, USA, 2012, pp. 1-6.

[5] Institute of Electrical and Electronics Engineers - IEEE Standards Association, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Standard 1588-2019, 2019.

[6] Chang Siqi, Chu Yingjun. Features and applications of Precision Time Synchronization Protocol IEEE 1588-2019 version [J]. Communications and Information Technology, 2022, (S2): 10-13.

[7] Zhang Meng, Lu Bo. Research on quantum enhanced secure time synchronization protocol [J]. Optical Communication Research, 2021, (04): 21-25+49.

[8] Wang Zhaowei. Research on high-precision, high-safe time synchronization method for industrial wireless sensor networks [D]. University of Chinese Academy of Sciences, 2018.

[9] Zhang Ying, Shen Xi, Li Qihao, et al. Smart substation protocol delay attack detection and recovery model based on Markov logic tree and system brittleness analysis [J]. Power System Protection and Control, 2020, 48(03):113-121.

[10] Alghamdi W, Schukat M. A Security Enhancement of the Precision Time Protocol Using a Trusted Supervisor Node. Sensors (Basel). 2022 May 11;22(10):3671.

[11] Shanghai Electric Group Co., Ltd. A device that realizes the synchronization of the secure clock of the industrial Internet of Things and its function implementation method [P]. 2021-12-17.

[12] E. Itkin and A. Wool, "A Security Analysis and Revised Security Extension for the Precision Time Protocol," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 1, pp. 22–34, 2020.

[13] Z. Idrees, S. Latif, H. Tahir, and L. Zheng, "Enhancing IEEE 1588 PTP security for IIoT networks: A lightweight attack detection and mitigation framework," Internet of Things, vol. 33, p. 101669, 2025.

[14] P. Ciotirnae and A. F. Păun, "Increasing the Robustness of the Time Reference Distribution Equipments using Multimodal Security Methods Based on Blockchain Implementations," in Proc. 2024 IEEE 15th International Conference on Communications (COMM), 2024.

[15] M. Langer and R. Bermbach, "NTS4PTP—Key Management System for the Precision Time Protocol Based on the Network Time Security Protocol," Internet-Draft (draft-langer-ntp-nts4ptp-02), IETF/Network Time Protocol WG, Work in Progress, Aug. 20, 2021.

[16] F. Rezabek, M. Helm, T. Leonhardt, and G. Carle, "PTP Security Measures and their Impact on Synchronization Accuracy," in Proc. IFIP/IEEE International Conference on Network and Service Management (CNSM), 2022.

[17] Kemparaj, P.; Kumar, S. S. Secure precision time protocol in packet switched networks. In: 2019 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), Portland, OR, USA, Sept. 2019, pp. 1–6.

[18] T. Mizrahi, "Security Requirements of Time Protocols in Packet Switched Networks," RFC 7384, Oct. 2014.

[19] M. Treytl and B. Hirschler, "Securing IEEE 1588 by IPsec tunnels—An analysis," in Proc. 2010 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2010.

[20] N. Moreira, A. Astarloa, U. Kretzschmar, J. Lázaro, and E. Molina, "Securing IEEE 1588 messages with message authentication codes based on the KECCAK cryptographic algorithm implemented in FPGAs," in Proc. IEEE Int. Symp. on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS), 2014.

[21] M. Sharkhawy, "Attack Detection and Mitigation for High-Precision Clock Synchronization: The Precision Time Protocol (PTP) Case Study," Diploma thesis, Faculty of Informatics, TU Wien, Vienna, Austria, May 18, 2021.