New Security Mechanisms for Network Time Synchronization Protocols

Karen O'Donoghue
Internet Society
Reston, Virgina, USA
odonoghue@isoc.org

Dieter Sibold
PTB
Braunschweig, Germany
dieter.sibold@ptb.de

Steffen Fries
Siemens AG, CT RDA ITS
Munich, Germany
steffen.fries@siemens.com

***Abstract*— As evolving security concerns have prevailed, the network time synchronization protocol community has been actively engaged in the development of improved security mechanisms for both the IEEE 1588 Precision Time Protocol (PTP) and the IETF Network Time Protocol (NTP). These activities have matured to the point where this year should see the finalization of the first new security mechanisms for time protocols in ten years. This paper provides an overview of the two solutions being developed, compares and contrasts those solutions, and discusses relevant use cases and deployment scenarios.**

Keywords—time synchronization protocols; PTP; IEEE 1588; NTP; NTS; security; authentication; integrity.

I. INTRODUCTION AND BACKGROUND

Network time synchronization protocols have been evolving for over thirty years. At the beginning, security was not a priority because the security of timestamps was not seen as an immediate need based on the requirements and use cases under consideration at the time. The protocols were lightweight and not deemed to put a burden onto the infrastructure. The perceived risk of attacks targeting clocks was quite low. This environment resulted in time synchronization protocols that did not include security functionality in the initial designs. In the intervening years synchronized time has become an important requirement not only in applications but also in security mechanisms themselves. Hence, as for other protocols and applications, security functionality has been identified as a necessary and integral part of network time synchronization approaches.

The Network Time Protocol (NTP) was published as RFC 958 [1] initially in 1985 with the current version being published as a standards track RFC (RFC 5905 [2]) in 2010. These early versions of NTP provided a basic pre-shared key scheme for authentication of time servers by clients. However, the pre-shared key approach did not scale enough for large scale network deployments or the global Internet. Therefore, the Autokey Authentication Protocol (RFC 5906 [3]) was published in 2010 to address the scaling issue. With Autokey, clients authenticate time servers using public key infrastructure (PKI) mechanisms. Security analysis, however, has demonstrated a number of security issues with Autokey. [4] [5]. Because of the shortcomings of pre-shared key and Autokey, there is an ongoing effort in the Internet Engineering Task Force (IETF), to provide updated security mechanisms for NTP.

The Precision Time Protocol (PTP, IEEE 1588) was originally published in 2002 with a focus on precision synchronization for instrumentation, industrial automation, and military applications. The second version was finalized in 2008 [6] including more application use cases, such as telecom and enterprise environments. While the first version of PTP contained no security mechanisms, the second version was published with an Experimental Annex (Annex K). Annex K specified a security solution that provided group source authentication, message integrity, and replay attack protection. However, Annex K was not well adopted and implemented, and a number of studies were published regarding its weaknesses. Therefore, the ongoing effort to revise IEEE 1588 includes a plan to provide updated security mechanisms for PTP.

There has been growing recognition by the network time synchronization community that the operational environment and the application use cases have changed significantly, and security must now be addressed in a thorough and systematic manner. This evolution of time synchronization protocol security requirements and motivations is discussed in some detail in [7]. This paper goes on to discuss the resulting work in the IETF TICTOC working group and the IEEE PTP security subcommittee to identify time synchronization security requirements. RFC 7384 [8] documents the results of that analysis.

The security approaches discussed in this paper provide security counter measures addressing these requirements. It connects to the previous work and provides an overview about the current state of standardization of the two emerging time synchronization approaches, IEEE 1588 (PTP) with integrated security and the IETF Network Time Security (NTS). As of July 2017, the effort to address security in both the NTP and the PTP technical communities is still in progress; however, it has reached significant technical consensus over the past year. This paper is intended to provide the community with the technical highlights of both of the security approaches.

II. PTP SECURITY

The IEEE 1588 revision defines four solution classes (called prongs) to address the diversity of application requirements and considerations identified in [8]. These

solution classes can be used individually or in combination. These classes of solutions include: A) integrated PTP security mechanisms; B) external transport security mechanisms; C) architectural mechanisms; and D) monitoring and management. These classes are explained with more detail in the corresponding subsections. In addition to the four prongs, the IEEE 1588 revision provides some additional information on security practices and considerations that can be used to improve the security posture of the overall system.

A. Integrated Security Mechanism

The first solution class being defined by the IEEE 1588 Security Subcommittee is a security mechanism integrated into PTP itself. This solution class is intended to be deployable by any PTP system regardless of the underlying transport being used. It provides both authentication of the PTP entity and integrity protection of the PTP message. It does not aim to protect the confidentiality of the PTP message itself because of the non-secret nature of the included timestamps.

The foundation of the PTP integrated security mechanism is a Security TLV (Tag Length Value) that is added as an extension to the PTP message being secured. The content of the *securityTLV* depends on the PTP entity communicating and the key management protocol being utilized. The format of the newly defined *securityTLV* is shown in Figure 1 below. As shown, the *securityTLV* is added at the end of the PTP message and contains, beyond other information, an Integrity Check Value (ICV), which ensures the authenticity of the PTP information. The ICV is built using a hash function (HMAC-SHA-256-128) or AES in MAC mode (AES-GMAC-128). The secret key is provided by the associated key management. The current draft of the IEEE 1588 revision does not require a specific key management scheme, choosing instead to allow different key management approaches. There is an informative annex that suggests two specific approaches for different scenarios. These approaches are discussed in more detail below.

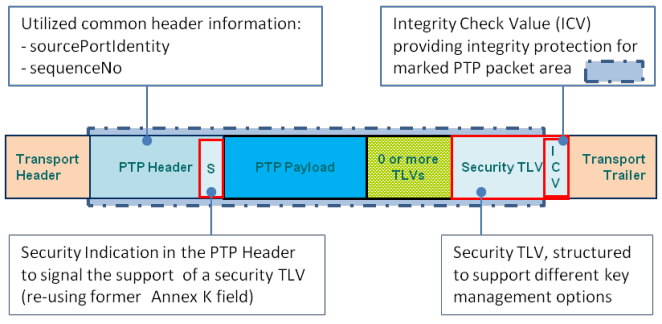

FIGURE 1: SECURITY TLV EMBEDDED IN PTP MESSAGE

With the current definition of the *securityTLV*, both unicast and multicast PTP communication can be secured. This degree of freedom was achieved by requiring an out-of-band key management mechanism. One of the primary challenges for the definition of the *securityTLV* in conjunction with key management was the need to provide the utilized key instantly or in a delayed manner.

Instant key sharing is typically achieved by group based key management protocols like the Group Domain Of Interpretation (GDOI) and specified in RFC 6407 [9]. The availability of the group key enables immediate security processing of the received PTP messages. An example for delayed key sharing is based on TESLA as specified in RFC 4082 [10]. Here, the key is shared after its active usage time and enables the security processing on the receiver side. The latter option requires the storage of the messages for later security checks but also enables source authentication directly. The first approach utilizes a group key and enables immediate actions, but only ensures that a member of the group has provided the message and not which member exactly.

The support of these various options stems from the nature of multicast communication. Here, source authentication is viewed in two different ways:

- The authentication source is a key distribution server resulting in a distributed group key or
- The authentication source is the receiver of a PTP packet directly resulting in a delayed key disclosure.

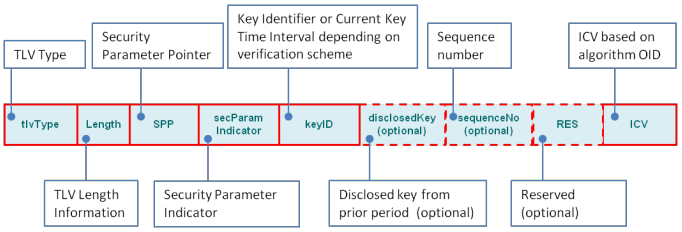

FIGURE 2: SECURITY TLV CONTENT

Figure 2 shows the general structure of the *securityTLV*. The detailed content is as follows:

- **Security Parameter Pointer (SPP)**: Together with information from the PTP header like the source port identity, the SPP is used to find the right security association containing necessary key management parameter
- **secParamIndicator**: indicates which of the optional fields are used
- **keyID**: identifies the currently used key
- **disclosedKey**: contains the disclosed key in the case of a delayed key sharing approach. This field is only used after a defined time period and is optional.
- **sequenceNumber**: is an optional field to extend the sequence number field as part of the original PTP header
- **RES**: is an optional reserved field for potential future use
- **ICV**: carries the integrity check value of the PTP packet for the packet content as marked in Figure 1

As stated above, PTP itself does not mandate any specific key management approach, but recommends two schemes, which are outlined in the following subsections.

1) Instant key sharing using GDOI

The first key management scheme suggested for PTP is GDOI. The Group Domain of Interpretation (GDOI) is specified in RFC 6407 [9] and supports the distribution of a symmetric group key (i.e., a Traffic Encryption Key – TEK) to all pre-configured or otherwise enrolled PTP Instances. This method requires a Key Distribution Center (KDC), which is the authoritative entity responsible for distributing symmetric session keys and security policy parameters to the involved PTP Instances. GDOI uses point-to-point communications between the KDC and each member of the group to distribute the symmetric group keys. The group key is distributed after successful authentication of the group members. The group key itself is then applied in ICV calculations of PTP messages within the specific group. A KDC failure will disrupt key updates, which may influence the group communication, so KDC redundancy is imperative. This approach is illustrated in the following Figure 3.

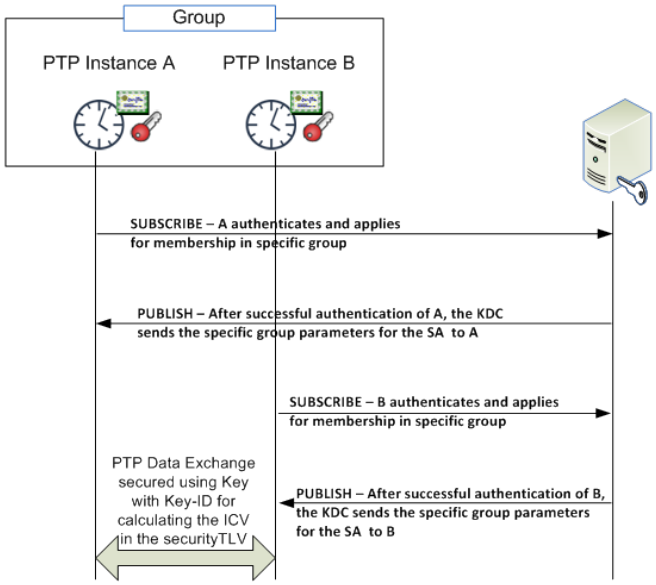

FIGURE 3: GDOI APPLICATION IN THE CONTEXT OF PTP

Note that the application of GDOI to IEEE 1588 will need further specification work as the current standard defines the distribution of group keys for IPSEC. However, the existing standard does allow for the definition of other security association payloads.

2) Delayed key sharing using TESLA

The second key management scheme suggested for PTP is based on TESLA. The Time Efficient Stream Loss-Tolerant Authentication (TESLA) method defined in RFC 4082 [10] enables a receiver of a message to validate its integrity and to authenticate its source after the associated key is disclosed by the sender. Hence, the TESLA scheme results in the delayed distribution of the source authentication key enabling delayed verification of PTP message integrity between a sender and a receiver.

As shown in Figure 4, an authoritative entity, which may also be a Key Distribution Center as shown for GDOI in the previous section, generates a key chain by using a random number generator to generate the hash chain anchor. This value is then hashed in an iterative process (i.e., X0 is hashed into X1, which is hashed into X2, etc.) Also, the intended usage time is split into intervals of uniform duration (in the example here, the validity time is one day), and each key is assigned to an interval in reverse order. All PTP instances utilizing TESLA securely obtain the last element of the key chain from the authoritative entity (anchor value). This value is typically digitally signed to ensure its integrity and source authentication. It may also be made publicly available. In the figure above, the authoritative entity is co-located with the master clock. Here, during each interval, the PTP messages are integrity protected using the current key, for instance X1. Once the time interval has ended (after one day), the master switches to the next key X2 and discloses X1. This enables all receiving PTP entities to validate the stored PTP messages. Note that the interval of one day was only taken as illustrative example. In real deployments, it is expected that the time interval will be much shorter.

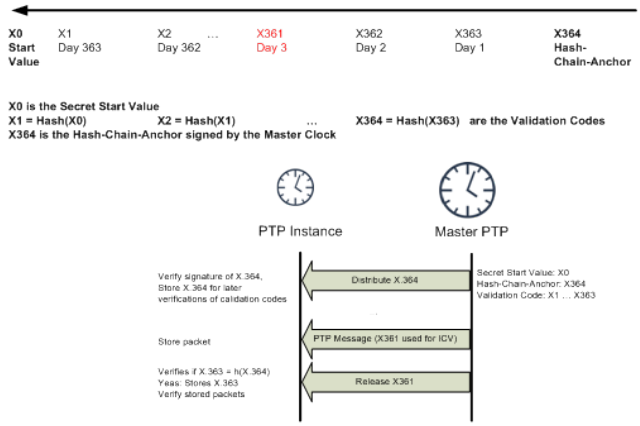

FIGURE 4: TESLA APPLICATION IN THE CONTEXT OF PTP

Note that when TESLA (or any other delayed disclosure scheme with scheduled disclosure times) is used to secure one-way time synchronization traffic, consideration should be given to tailored delay attacks as outlined in Ref. [11]. Such attacks employ small-step-big-step procedures to circumvent security by de-synchronizing participants just enough to cause vulnerabilities with regard to the disclosure schedule. Fortunately, appropriate use of periodical two-way packet delay measurements is sufficient to make the protocol resilient against this kind of attack [12], and PTP does offer mechanisms for this. But the issue is not trivial, and a deliberate look at the parameters and setup of the system in question is recommended for the sake of caution.

B. External Transport Security Mechanisms

The second solution class being specified for IEEE 1588 includes those security mechanisms that are external to PTP but may already be present in the system and therefore can be leveraged to also improve the security of the time synchronization infrastructure. There are two options currently identified for this solution class, MACSec and IPSec.

The first of these solutions, IEEE 802.1AE Media Access Control (MAC) Security (MACSec) [13], is defined for use on IEEE 802 based layer 2 networks. When using the MACSec mechanism, a secure association is established between two IEEE 802 ports. Integrity protection is provided to all data exchanged between those two ports including the PTP packets. The data path between the two ports may optionally also be encrypted. In order to establish a secure association between the two ports, some form of key management is required. This can be done with manual key configuration or using the MACsec Key Agreement (MKA) defined in IEEE 802.1X-2010 [14]. This solution is applicable to any PTP system that uses IEEE 802 layer 2 networks including PTP transported over IP over IEEE 802.

The second option, IP Security (IPSec) defined by the IETF, is applicable for PTP systems using IP based transport. The base architecture is defined in RFC 4301 [15], a protocol for node authentication and key exchange is defined in RFC 7296 [16], and a protocol for providing integrity checking and encryption of the data is defined in RFC 4303 [17].

Both of these mechanisms, MACSec and IPSec, can be used to provide authentication, integrity protection, and optionally encryption. If a PTP system is already operating in an environment where these mechanisms are present, it may make sense to utilize them as opposed to deploying a separate mechanism and the associated key management infrastructure needed for a PTP specific solution.

C. Architectural mechanisms

The third solution class being specified for IEEE 1588 is architectural mechanisms. In particular, architectural elements can provide some protection against DoS and replay attacks. Environments where this might be applicable include hybrid environments where there is not consistent deployment of the integrated or external security mechanisms discussed above.

The primary architecutural construct useful in the security context is redundancy. With redundancy, there are multiple points that an attacker must compromise in order to impact the overall PTP system. Three types of redundancy are being discussed in the IEEE 1588 context. Redundant timing systems provide a source of time outside of the PTP system. Redundant PTP grandmasters (implemented using multiple domains) can be deployed to reduce the vulnerability associated with having a single grandmaster as a potential target. And finally, redundant paths allows for multiple paths to get to the grandmaster. These redundancy mechanisms are reliant on the expansion of the use of domains to cover this case. The redundant time synchronization information can also be used for plausibility checks at the receiver side.

D. Monitoring and Management

The final solution class being specified for IEEE 1588 is monitoring and management mechanisms that provide the ability to observe PTP behavior and detect when attacks are potentially occuring. The IEEE 1588 revision defines parameters that could be used in this context. In addition to being able to detect problems with the PTP infrastructure, monitoring of the PTP system can also provide valuable insights into the overall security status of the system. This may be supported protocols like Simple Network Management Protocol (SNMP) and syslog. Note that both SNMP and syslog were defined long ago and were not originally designed with security in mind. Newer revisions and additional means to provide security for both of these protocols now exist to ensure the security of their transmitted data. While confidentiality may not always be the first objective here, source authentication and integrity protection of the communication is an important requirement.

III. NTP Security

The IETF NTP working group is focused on the development of a set of security measures for NTP, which are currently specified in the internet draft "Network Time Security for the Network Time Protocol" [18].

The main objectives of the Network Time Security (NTS) measures are to enable NTP entities to cryptographically identify their communication partner, to ensure authenticity and integrity of exchanged time synchronization packets, and to provide replay protection. A relatively new goal of NTS is to provide unlinkability, which ensures that NTS does not leak any data that would allow an attacker to track mobile NTP clients when they move between different networks. Although NTS is able to provide confidentiality for specific NTP extension fields, the NTP header itself will not be encrypted.

NTP provides different modes of operation. Besides the most utilized client-server mode, it also provides a mode for synchronization of symmetric peers, a mode for exchanging control messages, and a broadcast mode. The various modes have different security and performance requirements. The symmetric and control modes have more rigorous security requirements when compared to the client-server mode. However, the client-server mode requires more attention to resource utilization since NTP servers may be contacted by a high number of clients and may not able to maintain state information for each client. NTS provides different means to meet these different requirements.

A. Symmetric and Control Mode

NTP's symmetric and control modes are protected by encapsulating the corresponding packets as DTLS Applications Data, respectively. This provides mutual authentication and replay protection. It also provides confidentiality which is required by certain NTP control messages.

B. Client-Server Mode

There are two security related phases for client-server mode. In the first phase an NTP client verifies the authenticity of its time server and performs the key exchange. And in the second phase, the client and server exchange NTP messages. The first phase is performed only once during the establishment of an NTP association. The second phase is continually repeated as long as the NTP association is active.

1) First Phase: Authentication and Key Exchange

The current draft defines an NTS key exchange protocol that uses the TLS protocol to provide a secure and robust means for the initial authentication of the server and the subsequent exchange of the keying material. Since TLS

requires a TCP connection between client and server, an NTS enabled NTP server must not only listen to port 123/UDP but also to a TCP port, which will be assigned by IANA.

Note that earlier versions of this draft (up to version 6) defined a custom key exchange protocol in which the authentication and key exchange messages were encapsulated into NTP extension fields which were piggy-backed onto NTP packets. This key exchange protocol has been discarded because of potential security issues related to IP fragmentation.

2) Second Phase: Protection of the Time Synchronization

During the second phase, NTS introduces four new Extension Fields (EF) to satisfy the security objectives. The latencies introduced by cryptographic algorithms may impede the time synchronization performance. It is therefore imperative that the applied cryptographic primitives must be fast to calculate. This requirement is met by applying only symmetric cryptography. The four new extension fields are:

1. The NTS Unique-Identifier extension: This EF contains a 32-octet random value which serves as nonce and protects the client against replay attacks.
2. The NTS Cookie extension: This EF contains information that enables the server upon receipt to re-calculate keys. The server therefore does not have to keep per-client state. This EF is opaque to the client.
3. The NTS Cookie Placeholder extension: this EF is sent whenever the client wishes to receive a new cookie. The server has to send an NTS Cookie extension for each received NTS Cookie Placeholder extension. This EF enables NTS to fulfill the unlinkability requirement.
4. The NTS Authenticator and Encrypted Extensions extension: This EF contains the ICV which is computed over the NTP header and any preceding EF. It is calculated by applying the Authenticated Encryption with Associated Data approach [19].

C. Broadcast Mode

The current draft does not provide any cryptographic security measures to protect NTP's broadcast mode. This is due to the difficulty with specifying an appropriate mechanism that is resistant to packet delay attacks. As with PTP, the utilization of a TESLA-like mechanism is being considered. However, because NTP does not provide periodical two-way packet delay measurements, it is especially vulnerable against tailored delay attacks [11, 12]. Further countermeasures are discussed in Ref. [11], but additional study is required in order to specify any additional security measures for NTP's broadcast mode.

D. Best Current Practice

Beyond the specification of NTS, the NTP community is also addressing security concerns through corrections to the specification, improvements to the implementation, and the issuance of an NTP BCP. [20]

IV. Deployment examples

Security for time synchronization is increasingly important, as several applications also in the critical infrastructure domain depend on timing information. Examples for domain specific applications may be:

- Synchronization of Phasor Measurement Units in the energy transmission and/or distribution network. These devices provide information about voltage, current, and phase angle used to derive the current state of the electricity network. Security for the synchronization between these units is one corner stone in the reliable operation of the transmission/distribution networks
- Synchronization in substation automation networks to ensure the correct operation of protection devices (in conjunction with protocols like GOOSE (Generic Object Oriented Substation Event) or SV (Sampled Values).
- Synchronization of machine parts in motion control in the process industry, for instance in a rolling mill or for printing presses.
- Synchronization of logging information in distributed systems to enable error tracking and thus to contribute to system stability and system integrity.
- New regulations of the finance sector raise high demands on the time synchronization of business clocks in trading systems. This is especially true in the high frequency trading where a new EU legislation called Markets in Financial Instruments Directive (MiFID II) requires a timestamping granularity of 1 μs and a maximal divergence to UTC from 100 μs. Similar requirements are formulated by the US Securities and Exchange Commission (SEC Rule 613).
- Many national metrology institutes in Europe and in the US apply NTP for the dissemination of UTC.
- In general, security management, specifically the increasing usage of X.509 certificates, relies on time for validity checks. As this builds the base for many applications, security is a necessary prerequisite.

V. Next Steps

As of the completion of this paper, the work in both the IEEE 1588 Security Subcommittee and the IETF NTP working group has not been finalized. However, while it is true that the efforts are still evolving, they do appear to be converging towards consensus. It is hoped that there will be stable security solutions for both NTP and PTP in the 2018 timeframe.

Additional information on the IEEE 1588 Security Subcommittee and the overall IEEE 1588 effort can be found at [21]. Additional information and instructions on how to participate in the NTP working group is available at [22]. Efforts are being made to keep the two activities coordinated so that security expertise as well as development resources can be leveraged across both groups.

The next stage beyond completion of the specification is implementation. There has been some interest in implementation of PTP security. On a more concrete note, a preliminary implementation of NTS is underway, and additional implementations have been indicated. Interoperability testing, vulnerability research and analysis, and

operational testing will all be needed to ensure that the proposed solutions are robust and secure. While there is still much work to do, significant progress has been made in emerging security solutions for network time synchronization protocols.

VI. Acknowledgement

The authors wish to acknowledge the ongoing efforts of the IEEE 1588 Security Subcommittee, the IETF NTP working group, and the IETF TICTOC working group, all of whom play an active role in the work represented in this paper. In particular, Doug Arnold, Jeffrey Dunn, Daniel Franke, Sharon Goldberg, Aanchal Malhotra, Russ Housley, Mikael Johansson, Danny Mayer, Tal Mizrahi, Silvana Rodriguez, Opher Ronen, Stefano Ruffini, Harlan Stenn, and Kristof Teichel all deserve recognition for significant technical contributions and ongoing persistence and patience as the committee work in both IEEE 1588 and IETF edges towards completion. Special thanks to Kristof Teichel who carefully reviewed the paper. Any errors or ommissions in the representation of this work in this paper are the responsibility of the authors alone.

VII. References

[1] Mills, “Network Time Protocol”, RFC 958, DOI 10.17487/RFC0958, September 1985, <https://www.rfc-editor.org/info/rfc0958>.

[2] D. Mills, J. Martin, Ed., J. Burbank, and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, DOI 10.17487/RFC5905, June 2010, <https://www.rfc-editor.org/info/rfc5905>.

[3] B. Haberman, Ed., and D. Mills, "Network Time Protocol Version 4: Autokey Specification", RFC 5906, DOI 10.17487/RFC5906, June 2010, <https://www.rfc-editor.org/info/rfc5906>.

[4] D. L. Mills, “NTP security analysis”, May 2012 [Online] Available: https://www.eecis.udel.edu/~mills/security.html. [Accessed: 24-Jul-2017]

[5] S. Rottger, “Analysis of the NTP autokey procedures,” unpublished.

[6] IEEE 1588-2008, IEEE Instrumentation and Measurement Society. TC-9 Sensor Technology, "IEEE standard for a precision clock synchronization protocol for networked measurement and control systems", 2008.

[7] K. O'Donoghue, "Emerging Solutions for Time Protocol Security," presented at the 2016 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS 2016), ERICSSON, Stockholm, SWEDEN, 2016.

[8] T. Mizrahi, "Security Requirements of Time Protocols in Packet Switched Networks", RFC 7384, DOI 10.17487/RFC7384, October 2014, <http://www.rfc-editor.org/info/rfc7384>.

[9] B. Weiss, S. Rowles, T. Hardjono, “The Group Domain of Interpretation”, RFC 6407, October 2011, https://tools.ietf.org/html/rfc6407

[10] A. Perrig, D. Song, R. Canetti, J. D. Tygar, B. Briscoe, “Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction”, RFC 4082, June 2005, https://tools.ietf.org/html/rfc4082

[11] K. Teichel, D. Sibold, and S. Milius, "An Attack Possibility on Time Synchronization Protocols Secured with TESLA-Like Mechanisms," in *Information Systems Security: 12th International Conference, ICISS 2016, Jaipur, India, December 16-20, 2016, Proceedings*, I. Ray, M. S. Gaur, M. Conti, D. Sanghi, and V. Kamakoti, Eds. Cham: Springer International Publishing, 2016, pp. 3-22.

[12] R. Annessi, J. Fabini, and T. Zseby, "It's About Time: Securing Broadcast Time Synchronization with Data Origin Authentication," presented at the The 26th International Conference on Computer Communications and Networks (ICCCN 2017) Vancouver, Canada, July 31 -August 3, 2017, 2017.

[13] IEEE 802.1AE, IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Security, Aug 2006.

[14] IEEE 802.1X-2010, IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, Aug. 2010

[15] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <http://www.rfc-editor.org/info/rfc4301>.

[16] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <http://www.rfc-editor.org/info/rfc7296>.

[17] S. Kent, "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <http://www.rfc-editor.org/info/rfc4303>.

[18] D. Franke, D. Sibold, K. Teichel, " Network Time Security for the Network Time Protocol”, Work in Progress, draft-ietf-ntp-using-nts-for-ntp-08, March 2017, <https://datatracker.ietf.org/doc/draft-ietf-ntp-using-nts-for-ntp/>.

[19] D. McGrew, “An Interface and Algorithms for Authenticated Encryption”, RFC 5116, January 2008, https://tools.ietf.org/html/rfc5116

[20] D. Reilly, H. Stenn, D. Sibold, "Network Time Protocol Best Current Practices”, Work in Progress, draft-ietf-ntp-bcp-00, June 2017, <https://datatracker.ietf.org/doc/draft-ietf-ntp-bcp/>.

[21] "iMeet Central", Ieee-sa.imeetcentral.com, 2016. [Online]. Available: https://ieee-sa.imeetcentral.com/1588public/. [Accessed: 24- Jul- 2017].

[22] IETF NTP working group, https://datatracker.ietf.org/wg/ntp/about/, 2017. [Online]. [Accessed: 24 July 2017].

Presented at International IEEE Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS) in Monterey, CA, on September 1, 2017.