Causality Re-Ordering Attacks on the IEC 60870-5-104 Protocol

Alessio Baiocco
Department of Information Security and Communication Technology
Norwegian University of Science and Technology
N-2815 Gjøvik, Norway
alessio.baiocco@ntnu.no

Stephen D. Wolthusen
Department of Information Security and Communication Technology
Norwegian University of Science and Technology
N-2815 Gjøvik, Norway
and
School of Mathematics and Information Security
Royal Holloway, University of London
Egham, Surrey TW20 0EX, UK
Email: stephen.wolthusen@rhul.ac.uk

***Abstract*—The ISO/IEC 60870-5-104 standard for sending telecontrol messages first published in 2000 does not include security features, although the ISO/IEC 62351 standard adds features such as integrity protection and authentication even if this is not yet widely used.**

However, in this paper we argue that even in the presence of such security extensions, it is still possible to realise attacks by subverting the temporal relation between APDUs which implementations assume to be correct. To this end we have investigated attacks against the Network Time Protocol (NTP) used for clock synchronisation in most implementations and demonstrate that Master and Slave entities or other entities including intrusion detection sensors can be made to obtain messages with different time-stamps. This can lead to the assumption of causality reversal and will affect both control loops and process reconstruction by auditing, monitoring, and intrusion detection system. We demonstrate these results analytically and in a scenario based on a simulation framework allowing the study of different topologies and their varying effects on the visibility of messages and time synchronisation before proposing a mitigation mechanism.

I. Introduction

The ISO/IEC 60870-5-104 standard is an extension of the ISO/IEC 60870-5-101 that allows the protocols for power system monitoring and telecontrol based on open TCP/IP standards. This permits the deployment of far more flexible telecontrol topologies including interconnections over wide-area networks, but also opens up two problem domains which the present paper seeks to demonstrate are closely linked.

The security of ISO/IEC 60870-5-101 communications relies on the assumption of closed communication links that can be point-to-point or multidrop mechanisms and has explicit time-synchronisation; for this purpose the standard defines time and synchronisation in clause 6.8 of IEC-60870-5-4 and is used in IIEC 60870-5-101, IEC-60870-5-102, IEC-60870-5-103, and IEC-60870-5-104, respectively. Whilst typically not required the maximum resolution possible in the ISO/IEC 60870 for clocks and time tags is $1ms$.

In the case of ISO/IEC 60870-5-104 communication, particularly when operating over wide-area networks, time synchronisation is more critical since one cannot assume that messages are obtained by master and slave stations at the time of receipt. Instead, *telemetry skew* caused by communication delays or scan rates will result in even the same operation being processed in different locations to be associated with different time stamps. To obtain correct baseline timestamps, and also to *preserve causality relations*, robust synchronisation is essential, and for interoperability and regulatory purposes must be linked to a recognised source such as recommended by NERC [14].

Whilst synchronisation against GNSS sources such as GPS is possible in a decentralised manner, multiple endpoints would not only be required to still distribute the signal from a receiver, but as civilian GPS signals are susceptible to spoofing and jamming also from inexpensive equipment [20], this is in itself problematic as has particularly been demonstrated for IEEE C37.118 synchrophasors [17]; analogous arguments hold for unprotected DCF77 and IRIG-B signals.

Hence most configurations will, even if atomic clocks or GNSS time references are used, or where the native ISO/IEC 60870-5-101 or -104 mechanisms are employed, rely on the Network Time Protocol (NTP) or a simplified variant (SNTP), currently in version 4 [5], [12], but originally designed in 1985. Although authentication mechanisms exist [6], these are currently not used widely in public systems which are subject to attacks against protocol and implementations [2], [9] including *on path* and *hijacking* attacks where it is not required to interpose an attacker in the path between an NTP time source and its consumer. Moreover, further attacks have been proposed also for authenticated variants [10], limiting the utility of current authentication mechanisms.

In this paper we argue that an attacker can achieve *desynchronisation between the observed time tags of events between master and (multiple) slave nodes* by altering the NTP synchronisation of target nodes, thereby achieving objectives such as *causality reversal* that may harm control loops and further rendering auditing and intrusion detection more difficult.

The remainder of this paper is structured as follows: Section II briefly defines the problem and current approaches before

discussing related work in section III. To demonstrate the feasibility of attacks, we outline underlying assumptions and describe the attack in section IV before describing the effect in a simulation environment in section V, proposing a mitigation mechanism in section VI, and giving conclusions in section VII.

II. Problem Statement

The NTP protocol specifies a hierarchical relation among numbered server *strata* where lower strata are acting as sources, although lateral peer-to-peer configurations among servers in the same stratum are permitted. Stratum 0 is taken to have a synchronisation source such as a high-precision atomic clock or an augmented GNSS receiver.

Clients will retrieve estimated times and error intervals from pre-configured lists of servers, and synchronises to a time interval on which at least half of the queried servers can agree. In a general network context this offers some protection, but power systems may not always be configured with sufficient diversity for this mechanism to be effective.

The ISO/IEC 60870-5-104 protocol must rely on either local synchronisation against high-precision time sources, typically a GPS receiver, or on (S)NTP as the ISO/IEC 60870-5-5 synchronisation mechanism is not available unless the configuration is sufficiently compact that the maximum network delay will be less than the required accuracy of the receiving station.

Master and slave nodes must hence generally rely on NTP for synchronisation, and although within power systems the use of authenticated NTP is feasible and desirable [6], we argue that weaknesses in currently deployed security mechanisms make attacks possible even in the presence of these security mechanisms whilst more recent developments considered by the IETF Network Time Security (NTS) working group are still in train. This, however, results in current standards for authentication having to be considered ineffective as the relevant cryptographic primitives have been demonstrated as inadequate. While a number of *identity schemes* for proving remote system identity and preventing man-in-the-middle attacks are proposed, the Autokey schema has long been known to be weak, while MAC calculations in pre-shared key environments rely on the obsolete MD5 hash algorithm.

This allows attackers able to inject messages visible by ISO/IEC 60870-5-104 stations to induce a mis-synchronisation. We propose to target systems such that in a given master/slave pair (or correspondingly for multiple slaves), this will result in a different *ordering of events or causality*.

III. Related Work

Although widely used in telecontrol of power systems particularly in Europe, research on security and vulnerabilities of the ISO/IEC 60870-5-104 protocol and its supporting protocols has been limited when compared to e.g. DNP3 (IEEE 1815) [3], [18]. The basic variant of the protocol does not incorporate (data origin) authentication or integrity verification and is hence vulnerable to straightforward man-in-the-middle attacks [11]; at the same time current implementations are less robust than desirable [8]. However, the basic issues found related to DNP3 documented in [3] such as susceptibility to replay and spoofing attacks in addition to man-in-the-middle scenarios are well-documented.

However, although at present not widely deployed, the integration of security mechanisms found in ISO/IEC 62351 addresses the majority of these vulnerabilities in the baseline protocol. What is not covered by this additional security are the supporting protocols, particularly time synchronisation. Here [25] identifies the main mechanisms in which desynchronisation attacks can be achieved, namely direct modification of time values, masqerading as the master clock, replaying old messages, denial of service, and delay of synchronisation. In particular, delay attacks have gained attention [13], [16] Surprisingly, the IEEE 1588 Precision Time Protocol used more commonly in closed network segments has received more attention in this regard [15], [21], [22]. We note that the use of authentication mechanisms no longer protects against attacks considered as mitigated by Ullmann et al. [25], but that synchronisation mechanisms are susceptible regardless, allowing *attackers to skew client clocks relative to the referenced master clock*. Whilst the so-called *panic threshold* in NTP is $1000s$ that would result in a client abandoning a given server, this is far more than the round-trip time required to influence control loops in power systems. As shown by Malhotra et al. [9], moreover, the NTP *Kiss of Death* mechanism can also be misused to temporarily interrupt legitimate synchronisation.

Most recent research into the security of ISO/IEC 60870-5-104 focuses on intrusion detection [26], but we note that regardless of whether signature-based [24], anomaly-based [23], or specification-based systems [1], all depend on correct message ordering as well.

IV. Assumptions and Considerations

In the following sections we explore how the time seen by ISO/IEC 60870-5-104 nodes can be shifted relative to one another, causing desynchronisation and second-order effects such as mis-compensation in control loops. A number of request types (PID) in the standard explicitly make reference to time tags in request and response APDUs (e.g. 30,31,58, and 63), allowing straightforward targeting.

For this to be successful, it is *immaterial if the protocol is protected by ISO/IEC 62351-5 as the attack is against the time referenced by endpoints rather than communication channels*. However, several assumptions must hold:

Authentication Current NTP as specified in RFC 5905 [12] relies on MD5 HMACs for messages, which is susceptible to chosen prefix collision attacks [19].

Access The proposed attack assumes that the attacker is able to read and write messages on the target network; the exact mechanism used for such an attack is beyond the scope of this paper.

Topology The proposed attack assumes a non-flat network topology such that NTP traffic for a given master and

slave combination is not visible at the same time to a monitoring entity.

V. Analysis and Scenario

We have choice to recreate a plausible research framework (named CHAOS) which contains SCADA IEC104 clients and one IEC104 server,the NTP servers and a storage server as showed in 1.

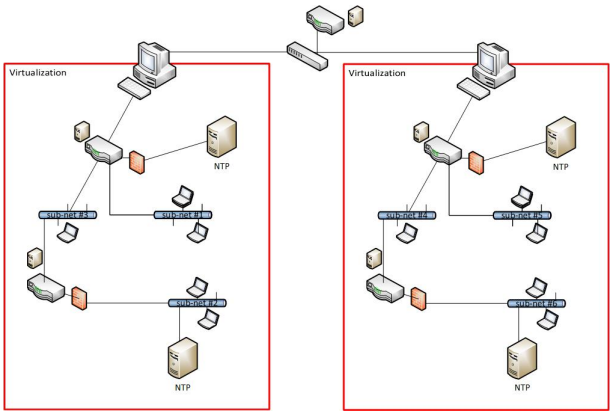

Fig. 1. CHAOS Framework Network Topology

Three bare metal PC are used as hosts using linux Ubuntu 16.04 LTS and Virtualbox is the chosen hypervisor. The networking service is performed by PFsense, an open source BSD based firewall-router software which is hosted by some virtual machine spreader inside the whole framework. A PFsense bare metal installation PC works as both peripheral firewall and central router for interconnecting the whole host PCs. Other virtualized PFsense based routers operate in the network providing network stratification and further data traffic security by implementing PFsense routers at each sub-network branch.

CHAOS framework can both works as a standalone platform and even connected to a real SCADA RTU simply by reconfiguring the border router: when the framework works in standalone mode the main peripheral router/firewall isolates all sub-networks blocking the IN/OUT communications, especially the NTP UDP port 123 (proper of NTP service). We choice to run the framework as standalone platform with its own time source provided by one of the PC. Even if using the local PC time as time source, we wanted our system isolated from the real stratus 1 (e.g. google time servers) in order to have full control over the timing infrastructure. The whole framework NTP infrastructure is represented in figure 2:

where a physical PC provides the time to the other levels (stratum 2 and stratum 3) up to stratus 4 which represents the NTP client of the IEC104 client/server units. The NTP infrastructure (figure 2) also has some peer-to-peer link in order to guarantee a certain degree of redundancy. Also, in order guarantee the max flexibility we used Ubuntu server OS based virtual machine as NTP client/server for both the stratum 2 and stratum 3. Also PFsense offers an NTP client-server daemon which we used for providing time reference to the sub-networks we connected to.

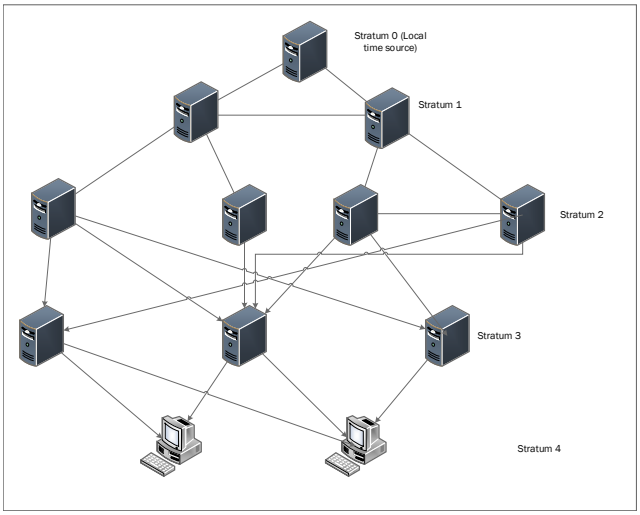

Fig. 2. CHAOS framework NTP Structure

In our simulation framework the NTP client/servers implements the MD5 symmetric authentication assuming that an attacker has already performed a collision attack against one or more NTP servers which allowed him to connect to the other NTP servers. How the collision attackto the MD5 authentication happen is not part of this work.

We decided to tamper two different NTP servers at stratum 2 ad stratum 3 in order to see how the ”malicious” time settings propagate across the NTP network. BY manipulating the time source we introduce a consistent time jitter which can be interpreted by lower level NTP server like as the time source server has lost synchronization, hence the NTp time source with a minor time jitter can be used putting the other time sources on a *candidate mode* state. However, this scenario might hot happen when the attacked NTP server is set as *prefer* with respect to the other ones.

The IEC 60870-5-104 client - or even server - by receiving the ”malicious” time from the external sources, starts to use the malicious time on the IEC 60870-5-104 APDUs timestamps. The receiving server might identifies wrong timing and wait for any packets source synchronization or, in the worst scenario, uses receiver’s local time for updating the the received time packet’s time stamp. Anyway, when time gap between the sent command request and the relative command answer becomes too wide, also when the NTP server resynchronize itself with a not tampered higher level time source, the IEC request-reply historian becomes ambiguous and hard to determinate which particular request has produces a subsequent answer from the IEC 104 server.

The figure 3 is the visual representation of the timing shift described above on a modified Minkowski graphic: $y - axes$ represents the IEC PID request sent to a server and on $x-axes$ there’s its relative response. Since the communication time delay is random the curve represents the time flow and the projections to the respective axes the represents respectively the correlation request-response.

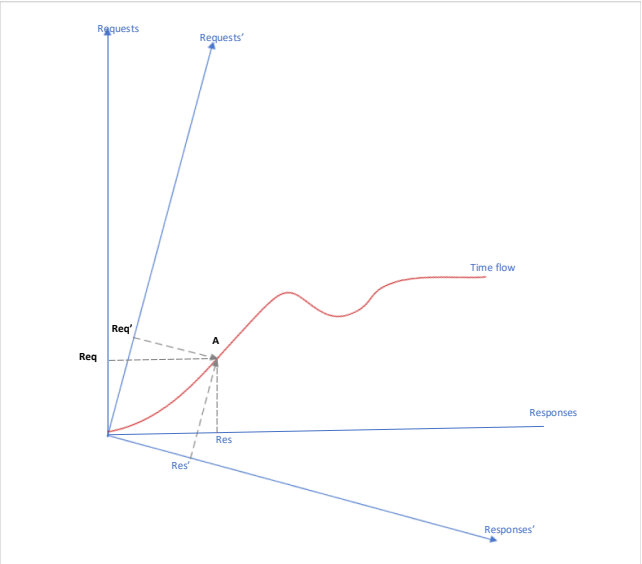

Fig. 3. Minkowsky Graphic Representation of time variance and relative effects on request-response timing

Using a different reference system for evaluating the same sequence of request-response is to be considered in the presence of attacks as the temporal sequence of events is completely distorted. It is deduced that several responses-required can be superimposed if we change the adopted time reference.

A. Mitigating the Attacks Effects

Both in section III and in the section V we have seen the ease with which any hacker can tamper with the global timing system NTP, whose his security concerns relies on the MD5 authentication procedure, also evaluating its impact on time-dependent protocols IEC 60870-5-104.

In order to mitigate the time drift effect and the consequent causality re-ordering attack we suggest the following strategies:

APDU Sequence numbering: sequencing the APDUs exchanged between the client and the server 60870-5-104 in such a way that, besides making an eventual replay attack more difficult to success, they allow to identity the correct packets reception whenever the time synchronism is lost due to hardware failures or even attacks). It is important to point out that no support or any procedure for correcting the random packet re-ordering phenomenon is provided nor implemented by the NTP protocol or even the IEC-60870-5-104 protocol: packet sequencing is entrusted to the TCP or to the NTP transport protocol if the time stamp NTP is taken as a reference. The APDUs should be numbered and the sequential number should be included in the packet before being sent over the network. Further, to ensure greater data integrity, the packets sent should contain part, also the numbering sequence, of the sent message processed by a hash function.

Reinforced MD5 Authentication: Authentication with MD5 hashing functions should be replaced or made more robust by adding a secret sequence of a reasonable length to the packet on which to do hashing, that is the salt/pepper hashing method. Among the two techniques we believe that pepper is the best solution as the secret sequence is not stored. However, we discourage the reuse of pepper/salt sequences to process other packets or data sequences to encrypt.

Partial Traffic Buffering: The sequence number is also useful to handle packets whenever these are buffered. We also count on the ability of both client and server to recompute the missing/damaged packets; this means client or server does not have to re-compute starting from the beginning of a sent packet series.

VI. Mitigation

Create mechanism to enforce shared view of message sequence per originator with partial ordering over messages at synchronisation points.

APDUs are to be associated with a sequence number where a station may start a sequence at a random number on startup or crash fault.

Each APDU is to be combined with the sequence number and subjected to a HMAC – assuming a suitable key distribution mechanism beyond the scope of this paper as this reflects trust relationships, but may use a schema such as the one proposed in [4], which creates an effective *one-way hash chain* [7].

This can be computed efficiently and distributed out of band relative to the ISO/IEC 60870-5-104 protocol, resulting in a partial order for each station that can be verified without having to assume either correct ordering guaranteed by the transport mechanism or synchronised time (tags).

VII. Conclusions

This paper has demonstrated that at present the best practice of securing the ISO/IEC 60870-5-104 protocol with the ISO/IEC 62351-5 protection profile remains insufficient if an attacker can gain access to a telecontrol network and is able to inject delayed or modified NTP messages. Attackers may de-synchronise control loops, causing undesirable behaviour, and may invert or distort causality relations seen by observers. Whilst mitigation by the introduction of multiple independent synchronisation sources may be possible, this implies considerable cost for both deployment of sources and requisite network topology-based isolation. Instead, we have proposed an out-of-band mechanism that does not require the modification of the underlying protocol but which can be used to validate causality relations.

Ongoing and future work will include a study of the effectiveness of currently-proposed extensions to the NTP

protocol and mechanisms for the detection of delay and desynchronisation attacks.

REFERENCES

[1] M. Caselli, E. Zambon, J. Petit, and F. Kargl, "Modeling Message Sequences for Intrusion Detection in Industrial Control Systems," in *Critical Infrastructure Protection IX: Proceedings of the Ninth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (ICCIP 2015)*, ser. IFIP Advances in Information and Communication Technology, M. Rice and S. Shenoi, Eds., vol. 466. Arlington, VA, USA: Springer-Verlag, Mar. 2015, pp. 49–71.

[2] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir, "Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks," in *Proceedings of the 2014 Conference on Internet Measurement Conference (IMC 2014)*. Vancouver, BC, Canada: ACM Press, Nov. 2014, pp. 435–448.

[3] S. East, J. Butts, M. Papa, and S. Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," in *Critical Infrastructure Protection III: Proceedings of the Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection (ICCIP 2009)*, ser. IFIP Advances in Information and Communication Technology, C. Palmer and S. Shenoi, Eds., vol. 311. Hanover, NH, USA: Springer-Verlag, Mar. 2009, pp. 67–81.

[4] R. Gennaro, S. Halevi, H. Krawczyk, T. Rabin, S. Reidt, and S. Wolthusen, "Strongly-Resilient and Non-Interactive Hierarchical Key Agreement in MANETs," in *Proceedings of the 13th European Symposium on Research in Computer Security (ESORICS 2008)*, ser. Lecture Notes in Computer Science, S. Jajodia and J. Lopez, Eds., vol. 5283. Málaga, Spain: Springer-Verlag, Oct. 2008, pp. 49–65.

[5] B. Gerstung, C. Elliott, and B. Haberman, "Definitions of Managed Objects for Network Time Protocol Version 4 (NTPv4)," IETF Request for Comments 5907, Jun. 2010.

[6] B. Haberman, D. Mills, and U. Delaware, "Network Time Protocol Version 4: Autokey Specification," IETF Request for Comments 5906, Jun. 2010.

[7] Y.-C. Hu, M. Jakobsson, and A. Perrig, "Efficient Constructions for One-Way Hash Chains," in *Proceedings of the Third International Conference on Applied Cryptography and Network Security (ACNS 2005)*, ser. Lecture Notes in Computer Science, J. Ioannidis, A. Keromytis, and M. Yung, Eds., vol. 3531. New York, NY, USA: Springer-Verlag, Jun. 2005, pp. 423–441.

[8] M. Kerkers, "Assessing the Security of IEC 60870-5-104 Implementations using Automata Learning," Master's thesis, University of Twente, Twente, The Netherlands, Apr. 2017.

[9] A. Malhotra, I. E. Cohen, E. Brakke, and S. Goldberg, "Attacking the Network Time Protocol," in *Proceedings of the 2016 Network and Distributed System Security Symposium (NDSS 2016)*. San Diego, CA, USA: Internet Society, 2016, pp. 1–15.

[10] A. Malhotra and S. Goldberg, "Attacking NTP's Authenticated Broadcast Mode," *Computer Communication Review*, vol. 46, no. 2, pp. 12–17, Apr. 2016.

[11] P. Maynard, K. McLaughlin, and B. Haberler, "Towards Understanding Man-In-The-Middle Attacks on IEC 60870-5-104 SCADA Networks," in *Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2014)*. St. Pölten, Austria: BCS, Sep. 2014, pp. 30–42.

[12] D. Mills, U. Delaware, J. Martin, J. Burbank, and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification," IETF Request for Comments 5905, Jun. 2010.

[13] T. Mizrahi, "A Game Theoretic Analysis of Delay Attacks against Time Synchronization Protocols," in *Proceedings of the 2012 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS 2012)*. San Francisco, CA, USA: IEEE Press, Oct. 2012, pp. 1–6.

[14] NERC, "Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs," North American Electric Reliability Corporation, Washington D.C., USA, Tech. Rep., Apr. 2009, Version 0.995, originally published in 2009 and approved in 2013.

[15] Y. Pathan, A. Dalvi, A. Pillai, and D. Patil, "Analysis of Selective Packet Delay Attack on IEEE 1588 Precision Time Protocol," University of Colorado at Boulder, Boulder, CO, USA, Technical Report TLEN-5710, Apr. 2014.

[16] A. Sargolzaei, "Time-Delay Switch Attack on Networked Control Systems, Effects, and Countermeasures," Ph.D. dissertation, College of Engineering and Computing, Florida International University, Miami, FL, USA, May 2015.

[17] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3–4, pp. 146–153, Dec. 2012.

[18] T. Sommestad, M. Ekstedt, and L. Nordstrom, "Modeling Security of Power Communication Systems Using Defense Graphs and Influence Diagrams," *IEEE Transactions on Power Delivery*, vol. 24, no. 4, pp. 1801–1808, Sep. 2009.

[19] M. Stevens, A. Lenstra, and B. De Weger, "Chosen-Prefix Collisions for MD5 and Applications," *International Journal of Applied Cryptography*, vol. 2, no. 4, pp. 322–359, Jul. 2012.

[20] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun, "On the Requirements for Successful GPS Spoofing Attacks," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*. Chicago, IL, USA: ACM Press, Oct. 2011, pp. 75–86.

[21] A. Treytl and B. Hirschler, "Security Flaws and Workarounds for IEEE 1588 (Transparent) Clocks," in *Proceedings of the 2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS 2009)*. Brescia, Italy: IEEE Press, Oct. 2009, pp. 1–6.

[22] J. Tsang and K. Beznosov, "A Security Analysis of the Precise Time Protocol," in *Proceedings of the 8th International Conference on Information and Communications Security (ICICS 2006)*, ser. Lecture Notes in Computer Science, P. Ning, S. Qing, and N. Li, Eds., vol. 4307. Raleigh, NC, USA: Springer-Verlag, Dec. 2006, pp. 50–59.

[23] R. Udd, "Anomaly Detection in SCADA Network Traffic," Master's thesis, Department of Computer and Information Science, Linköping University, Lund, Sweden, Nov. 2015.

[24] R. Udd, M. Asplund, S. Nadjm-Tehrani, M. Kazemtabrizi, and M. Ekstedt, "Exploiting Bro for Intrusion Detection in a SCADA System," in *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security (CPSS '16)*. Xi'An, China: ACM Press, May 2016, pp. 44–51.

[25] M. Ullmann and M. Vögeler, "Delay Attacks: Implication on NTP and PTP Time Synchronization," in *Proceedings of the 2009 International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS 2009)*. Brescia, Italy: IEEE Press, Oct. 2009, pp. 1–6.

[26] Y. Yang, K. McLaughlin, S. Sezer, Y. Yuan, and W. Huang, "Stateful Intrusion Detection for IEC 60870-5-104 SCADA Security," in *Proceedings of the 2014 IEEE PES General Meeting*. National Harbour, MD, USA: IEEE Press, Jul. 2014, pp. 1–5.