Requirements for Secure Clock Synchronization

Lakshay Narula, and Todd Humphreys, The University of Texas at Austin

Abstract—This paper establishes a fundamental theory of secure clock synchronization. Accurate clock synchronization is the backbone of systems managing power distribution, financial transactions, telecommunication operations, database services, etc. Some clock synchronization (time transfer) systems, such as the Global Navigation Satellite Systems (GNSS), are based on one-way communication from a master to a slave clock. Others, such as the Network Transport Protocol (NTP), and the IEEE 1588 Precision Time Protocol (PTP), involve two-way communication between the master and slave. This paper shows that all one-way time transfer protocols are vulnerable to replay attacks that can potentially compromise timing information. A set of conditions for secure two-way clock synchronization is proposed and proved to be necessary and sufficient. It is shown that IEEE 1588 PTP, although a two-way synchronization protocol, is not compliant with these conditions, and is therefore insecure. Requirements for secure IEEE 1588 PTP are proposed, and a second example protocol is offered to illustrate the range of compliant systems.

Index Terms—time transfer; clock synchronization; security.

I. INTRODUCTION

Secure clock synchronization is critical to a host of technologies and infrastructure today. The phasor measurement units (PMUs) that enable monitoring and control in power grids need timing information to synchronize measurements across a wide geographical area [1]. Wireless communication networks synthesize their base stations to enable call handoff [2]. Financial networks transfer time across the globe to ensure a common time for pricing and transaction time-stamping [3]. Cloud database services such as Google’s Cloud Spanner similarly require precise synchronization between the data stations to maintain consistency [4]. These clock synchronization applications have sub-millisecond accuracy and stringent security requirements.

Clock synchronization is performed either by over-the-wire packet-based communication (NTP, PTP, etc.), or by over-the-air radio signals (GNSS [2], cellular signals, LORAN [5], DCF77 [6], etc.); both wired and wireless clock synchronization are used extensively. Synchronization by GNSS is the method of choice in systems with the most stringent accuracy requirements. Equipped with atomic clocks synchronized to the most accurate time standards available, GNSS satellites can synchronize any number of stations on Earth to within a few tens of nanoseconds [7]. NTP is usually only accurate to a few milliseconds, but essentially comes for free whenever the host device is connected to a network.

One-way clock synchronization protocols are based on unidirectional communication from the time master station, A, to the slave station, B. In such protocols, A acts as a broadcast station and may send out timing signals either continuously or periodically. The principal drawback of one-way wireless clock synchronization protocols is their vulnerability to delay attacks in which a man-in-the-middle (MITM) adversary nefariously delays or repeats a valid transmission from one station to another. Cryptographic and other measures can improve the security of one-way protocols against delay and other signal- and data-level spoofing attacks [8]–[10], but, as will be shown, such protocols remain fundamentally insecure because of their inability to measure round trip time. They can be secured against unsophisticated attacks, but remain vulnerable to more powerful adversaries.

Two-way clock synchronization protocols involve bi-directional communication between stations A and B. Such protocols enable measurement of the round trip time of the timing signal, which is shown to be necessary for detecting MITM delay attacks. This measurement, however, is not by itself sufficient for provable security against such attacks.

This paper establishes a fundamental theory of secure clock synchronization. In contrast to the current literature on timing security [11]–[17], the problem is formalized with definitions, explicit assumptions, and proofs. The major contributions of this work are as follows:

1) One-way synchronization protocols are shown to be insecure against a MITM delay attack. Adversarial delay is shown to be indistinguishable from clock bias, and hence is unobservable without further assumptions.

2) A set of necessary conditions for secure two-way clock synchronization is presented and proved. Similar protocol-specific conditions have been previously proposed [11], [13], [18], but have not been generalized to apply to a universal clock synchronization model.

3) The proposed necessary conditions, with stricter upper bounds, are shown to be sufficient for secure synchronization in presence of a probabilistic polynomial time (PPT) adversary. Provably secure for clock synchronization has not previously been explored in the literature.

4) The two-way synchronization scheme of IEEE 1588 PTP is shown to violate a necessary condition for security. This is a known vulnerability of PTP for which a fix has been proposed [11]. Having established a theory for security, this paper is able to show that the proposed fix is sufficient but is not the minimal necessary modification. A more parsimonious security requirement for PTP is presented that is both necessary and sufficient for secure synchronization.

5) A generic construction of a secure two-way clock synchronization protocol is presented to illustrate the general applicability of the proposed necessary and sufficient conditions to a range of underlying protocols.

This paper is a significant extension of [19], by the same authors. The necessary conditions for security have been revamped to incorporate both continuous and packet-based
clock synchronization systems. A sufficiency proof for the security conditions has been formulated, and protocol-specific countermeasures presented in the literature have been unified with the proposed conditions.

Wired clock synchronization is inherently more secure than its wireless counterpart because physical access to cables is easier controlled than access to radio channels. This paper primarily focuses on the more challenging task of clock synchronization over a wireless channel; nonetheless, the attacks and security protocols discussed herein also apply to wireline clock synchronization protocols in the case where the adversary gets access to the channel. For example, if an adversary is able to hijack a boundary clock in a wireline PTP network, then the resulting vulnerabilities are equivalent to that of wireless synchronization where the adversary has open access to the radio channel. In fact, an adversarial boundary clock is even more potent than a wireless adversary since it can completely block the authentic signal from reaching B.

The rest of this paper is organized as follows. Previous works on secure clock synchronization, and their relation to this paper, are summarized in Section II. Section III presents a generic model for clock synchronization and shows that all possible one-way synchronization protocols are insecure. Section IV presents the set of security conditions for a wireless clock synchronization protocol, proving these to be necessary by contradiction. Section V presents a proof of sufficiency for the same set of conditions with stricter upper bounds. A construction of an example secure protocol is presented in Section VI along with the security requirements for IEEE 1588 PTP. Concluding remarks are made in Section VII.

II. RELATED WORK

GNSS, NTP, and PTP are the most widely used protocols for clock synchronization. A number of research efforts have been made to assess and improve the security of these protocols. This section reviews some of the notable efforts in the literature.

The GNSS jamming and spoofing threat has been recognized in the literature for more than a decade. A survey of the current state-of-the-art in spoofing and anti-spoofing techniques is presented in [8]. Recent works on GNSS anti-spoofing techniques have specifically focused on the case of timing security. Collaborative multi-receiver [16] and direct time estimation [17] techniques have been proposed for robust GNSS clock synchronization.

The growing popularity of IEEE 1588 PTP for synchronization in critical infrastructure has brought about concerns regarding its security [11]–[15]. The threats to IEEE 1588 PTP can broadly be categorized into data-level attacks (such as modification of time messages) and physical layer attacks (such as replay and delay attacks). While cryptographic protocols are able to foil data-level attacks against realistic adversaries, some signal-level attacks, such as the delay attack, remain open vulnerabilities. Unfortunately, their execution is relatively simple.

Ullman et al. [11] propose measuring the propagation delays during initialization of clock synchronization and monitoring the propagation delays during the normal operation of the time synchronization protocol. However, [11] does not prove that such a defense would be sufficient to prevent the delay attacks.

In [13], it is remarked that the clock offset computed between multiple master clocks over a symmetric channel must be zero, and thus, if multiple master clocks are available, they can detect any malicious delay introduced by an adversary. However, this defense does not consider the possibility that the adversary may only delay the packets sent to the slave nodes.

The work presented in [13] is perhaps in closest relation to the current paper. Annessi et al. upper bound the clock drift between subsequent synchronization signals using a drift model, and perform two-way exchange of timestamps such that the master clock is able to verify the time at the slave. Furthermore, given the maximum clock drift rate and the maximum and minimum propagation delay of the timing signal, they derive an upper bound on the adversarial delay that can go unnoticed. However, with conservative bounds on the maximum clock drift rate and the variation in path delays, the accuracy guarantees derived in [13] may be insufficient for certain applications. Moreover, as will be shown in this paper, they fail to take account of one the necessary conditions for secure synchronization.

This paper abstracts the clock synchronization model and assesses its security in a generic setting. It is shown that specialization of the generic security conditions to the particular protocols assessed in the aforementioned efforts leads to solutions similar or identical to those previously advanced. Thus, establishing the fundamental theory of secure clock synchronization also serves to unify the prior work in the literature.

III. SYSTEM MODEL

A general system model for clock synchronization is shown in Figure 1 The time seeker station, A, wishes to synchronize its clock to that of the time master station, B. For wireless synchronization applications, stations A and B are assumed to have known locations, xA and xB, respectively. Due to clock imperfections, the time at station B, tB, continuously drifts with respect to tA, the time at station A. Station B seeks to track the relative drift of its clock by an exchange of signals between A and B. Without loss of generality, this paper assumes tA is equivalent to true time (relative to some reference epoch), a close proxy for which is GPS system time.

It is assumed that A and B are able to exchange cryptographic keys securely, if required. This exchange may occur over a public channel via a protocol such as the Diffie-Hellman key exchange [20] or via quantum key exchange techniques [21], [22]. Alternatively, symmetric keys for neighboring stations may be loaded at the time of installation.

Station A sends out a sync signal, sA, having distinct features which can be disambiguated from one another by observing a window of the signal containing the feature. The transition in sA marking the beginning of a data packet is an example of such a signal feature. Furthermore, the system at A is designed such that the kth feature is transmitted at time tA,k. B either
known to vary with time as \( \tau_{k} \). The window captured by \( B \) containing the \( k \)th feature of \( s_{B} \) as it travels from \( A \) to \( B \). For line-of-sight (LOS) wireless communication, \( \tau_{k} \) is the sum of the free-space propagation delay over the distance \( \| x_{B} - x_{A} \| \) and additional delays due to interaction of the timing signal with the intervening channel.

\( S_{A}^{k} \) represents a window of \( s_{A} \) containing the \( k \)th feature.

\( S_{A}^{k} \) is modeled as zero-mean with variance \( \sigma_{x}^{2} \). The measurement itself, denoted \( s_{B}^{k} \), is modeled as

\[
s_{B}^{k} = t_{B}^{k} + w_{AB}^{k}
\]

\[
t_{B}^{k} = t_{A}^{k} + \tau_{AB}^{k} - \Delta t_{AB}^{k} + \bar{w}_{AB}^{k}
\]

where

\[
\Delta t_{AB}^{k} = t_{A}^{k} + \bar{w}_{AB}^{k} - t_{B}^{k}
\]

is the unknown time offset \( B \) wishes to estimate. As the bijection in (1) is known to \( B \), \( B \) can obtain \( t_{A}^{k} \) for the \( k \)th detected feature. If a prior estimate \( \bar{t}_{AB}^{k} \) of the delay \( t_{AB}^{k} \) is available to \( B \), then the desired time offset can be estimated as

\[
\Delta t_{AB}^{k} = t_{A}^{k} + \bar{w}_{AB}^{k} - z_{B}^{k}
\]

As a concrete example, consider the case of clock synchronization via GNSS in which \( B \) is a GNSS receiver in a known fixed location \( x_{B} \), and \( A \) is a GNSS satellite whose location is known to vary with time as \( x_{A}(t_{A}) \). On detection of the \( k \)th feature in a window of captured data, \( B \) determines \( t_{A}^{k} \) using (1) and also makes the measurement

\[
t_{B}^{k} = t_{A}^{k} + \tau_{AB}^{k} - \Delta t_{AB}^{k} + \bar{w}_{AB}^{k}
\]

\[
= t_{A}^{k} + \left[ \| x_{B} - x_{A}(t_{A}^{k}) \| + D_{\rho}^{k} \right] / c - \Delta t_{AB}^{k} + \bar{w}_{AB}^{k}
\]

where \( D_{\rho}^{k} \) is the sum of the excess delay caused by additive noise. The modeled excess delay is based on atmospheric models possibly refined by dual-frequency measurements [23]. An estimate of the time offset, \( \Delta t_{AB}^{k} \), can then be made using \( t_{A}^{k} \), \( \bar{w}_{AB}^{k} \) and \( z_{B}^{k} \) in (4).

It must be noted that, for one-way clock synchronization, any errors in the estimate of the distance between \( A \) and \( B \), and in the estimate of the excess channel delay, will appear as an error in the estimate of the time offset.

### B. Two-Way Clock Synchronization Model

As discussed above, if an estimate of \( \bar{t}_{AB}^{k} \) is available, then clock synchronization is complete after \( B \) receives the \( k \)th feature in \( s_{B} \). The response signal from \( B \) is typically used to either determine, or refine, the estimate of \( \bar{t}_{AB}^{k} \) with a measurement of the round trip time (RTT). The ability to measure RTT obviates the requirement that \( \| x_{B} - x_{A} \| \) be known a priori. In IEEE 1588 PTP, for example, RTT is measured to initially obtain, and periodically refine, the value of \( \bar{t}_{AB}^{k} \) used in deriving \( \Delta t_{AB}^{k} \) from (4).

In the system model considered in this paper, station \( B \) transmits a response \( s_{B} \) that is designed such that (1) there is a one-to-one mapping \( l(k) \) between the \( k \)th feature in \( s_{B} \) and the \( k \)th feature in \( s_{A} \), and (2) the \( l \)th feature’s index can be inferred by observation of a window containing it. Symbolically, if \( S_{B}^{l} \) is a window of \( s_{B} \) containing the \( l \)th feature of the response signal, then

\[
S_{B}^{l} \Longleftrightarrow l(k) \Rightarrow k
\]

On receipt of the \( k \)th feature in \( s_{A} \), at time \( t_{A}^{k} \) by \( B \)’s clock, but at \( t_{B}^{k} \) as measured by \( B \), \( B \) transmits the \( l \)th feature in \( s_{B} \) after a short delay, \( \tau_{BB} \) (in true time), hereon referred to as the layover time.

The layover time is introduced as a practical consideration. On receipt of \( A \)’s \( k \)th feature, \( B \) is physically unable to transmit its own \( l \)th feature with zero delay. Thus, \( B \) is allowed to specify a short layover time, \( \tau_{BB} \), after which it intends to launch its \( l \)th feature. It is important to note that the actual layover time, \( \tau_{BB} \), will not be the same as the intended layover time because the clock at \( B \) will not, in general, be frequency synchronized with true time. However, if the layover time
is sufficiently short, the difference $\bar{\tau}_{BB} - \tau_{BB}$ can be made negligible compared to the time synchronization requirement, with the actual value depending on the quality of B’s clock.

Station A receives the response signal as a delayed and noisy replica of $s_B$, denoted $r_A$. The delay experienced by the lth feature as it travels from B to A, in true time, is denoted $\tau_{BA}$. Station A captures a window $R_{BA}$ of $r_A$ that enables A to identify the lth feature in $s_B$ according to (5), and to infer that the received feature is in response to the lth feature transmitted by A. Furthermore, A makes a noise-corrupted measurement $z_A^l$ of the time-of-arrival of the lth feature in $s_B$, according to A’s clock. The noise, denoted $w_{BA}^l$, is again modeled as zero-mean with variance $\sigma^2_{w}$. The full measurement model is given by

$$z_A^l = t_A^l + w_{BA}^l = t_A^l + \tau_{AB} + \tau_{BB} + \tau_{BA}^l + w_{AB}^l + w_{BA}^l$$

Since $t_A^l$ is exactly known at A, a direct noisy measurement of the round trip time $\tau_{BA}^l + \tau_{BB} + \tau_{BA}^l$ can be made as

$$z_{\text{RTT}} = z_A^l - \tau_{BA}^l$$ (6)

Under the assumption of symmetric delays, i.e., $\tau_{BB} = \tau_{BA}$, and with knowledge of $\tau_{BB}$, the measured RTT in (6) can be exploited to improve the modeled propagation delay for future exchanges between A and B:

$$z_{\text{RTT}}^m = z_{\text{RTT}}^n = \frac{z_{\text{RTT}}^l - \tau_{BA}^l}{2}$$

where $m > k$ and $n > l$.

Since RTT will be play a central role in the discussion on secure synchronization later on, various definitions and assumptions concerning RTT are stated here for clarity:

- RTT for the kth feature in $s_A$ and the corresponding lth feature in $s_B$ is defined as

$$z_{\text{RTT}}^l = \tau_{AB}^k + \tau_{BB}^l + \tau_{BA}^l + \tau_{AB}^l$$

- Measured RTT includes, in addition to RTT, measurement noise at both A and B; it is modeled as

$$z_{\text{RTT}} = \tau_{AB}^k + \tau_{BB} + \tau_{BA}^l + w_{AB}^k + w_{BA}^l$$

- Modeled RTT, also called the prior estimate of RTT, is defined as

$$\hat{z}_{\text{RTT}} = \tau_{AB}^k + \hat{\tau}_{BB} + \hat{\tau}_{BA}^l$$ (7)

For example, in the case of wireless clock synchronization with LOS radio signals, a prior estimate of RTT is based on the distance between A and B and on models of channel delays in excess of free-space propagation between these.

- The modeled RTT, $\hat{z}_{\text{RTT}}$, can be refined with measurements of RTT in a two-way protocol. Alternatively, as will be discussed later, if an accurate modeled RTT is available, it and the measured RTT can be used to detect delay attacks.

- Unambiguous measurement of RTT requires that there exist a one-to-one mapping between the signal features in $s_A$ and $s_B$, as mathematically represented in (5). On detection of the lth feature in $s_B$, A must be able to deduce that this feature was transmitted approximately $\bar{\tau}_{BB}$ after B received the kth feature in $s_A$. This requirement is appropriately a part of the RTT definition since it enables A to unambiguously measure RTT.

C. Attack Model

The attack model in this paper considers a MITM adversary $M$. The available computational resources allow M to execute probabilistic polynomial time (PPT) algorithms. M can receive, detect, and replay signals from A and B with arbitrarily precise directional antennas. Additionally, M has precise knowledge of $x_A$ and $x_B$, and can take up any position around or between the two stations. It has unrestricted access to the signals that A and B exchange over the air, and has complete knowledge of their synchronization protocol save for the cryptographic keys.

Let $L$ denote the alert limit, defined as the error in time synchronization not to be exceeded without issuing an alert.

**Definition III.1.** Clock synchronization is defined to be compromised if $|\Delta t_{AB} - \Delta \tau_{BA}^k| \geq L$.

Note that, in the absence of an adversary, clock synchronization is not compromised so long as

$$|\tau_{AB}^k - \bar{\tau}_{AB}^k + w_{AB}^k| < L$$

However, in the presence of a MITM adversary, the sync signal is delayed or advanced such that

$$\tau_{AB}^k = \tau_{AB}^k + \tau_{BA}^k + \tau_{AB}^k$$ (8)

where $\tau_{AB}^k > 0$ is the natural or physical delay (equal to $\tau_{AB}^k$ in the absence of an adversary) and $\tau_{AB}^k \geq 0$ is the adversarial delay. In this case, if

$$|\tau_{AB}^k - \bar{\tau}_{AB}^k + w_{AB}^k| = |\tau_{AB}^k - \bar{\tau}_{AB}^k + \tau_{BA}^k + w_{AB}^k| \geq L$$ (9)

then clock synchronization is compromised.

D. Vulnerability of One-Way Clock Synchronization

One-way clock synchronization is fundamentally vulnerable to a delay attack because it provides no mechanism to measure RTT. The adversary $M$ can compromise any one-way wireless clock synchronization protocol by transmitting the authentic sync signal from A such that the retransmitted signal, $s_M$, overpowers or otherwise supersedes the authentic signal $s_A$. In the absence of additional assumptions beyond those underpinning the one-way protocol described earlier, $M$ can introduce an arbitrary delay $\bar{\tau}_{AB}^M$ in its retransmission, thereby compromising the synchronization process.

Note that whereas counterfeit signal attacks can be prevented by authentication and cryptographic methods [24], these techniques do not prevent delay attacks because the delayed or repeated signal has the same cryptographic characteristics as that of the genuine signal, the only difference being that it is received with a (possibly small) additional delay.

The delay introduced by $M$ is added to the natural delay, $\tau_{AB}^k$, of the signal between A and B. As a result, an error of
A laboratory demonstration of such nulling is reported. If $\bar{A} \rightarrow \bar{B}$, nulling of $\triangle t_{2AB}$ is indistinguishable from a clock offset of the same magnitude.

To be sure, measures can be taken to make a MITM delay attack harder to execute without detection. But, importantly, these measures cannot guarantee synchronization will remain uncompromised. Various measures proposed in the literature, and their shortcomings, are discussed below.

a) Received Signal Strength Monitoring: The adversary $\mathcal{M}$ might attempt to overpower the authentic signal in order to spoof the sync message, leading to an increase in the total signal power received at $\bar{B}$. Station $\bar{B}$ could monitor the received signal strength (RSS) to detect such an attack [25]. However, a potent adversary could transmit, in addition to its delayed signal, an amplitude-matched, phase-inverted nulling signal that annihilates the authentic sync signal $s_A$ as received at $\bar{B}$, thus preventing an unusual increase in received power at $\bar{B}$. If $\mathcal{M}$ is positioned along the straight-line path between $\bar{A}$ and $\bar{B}$, nulling of $s_A$ can be effected without prior knowledge of $s_A$. A laboratory demonstration of such nulling is reported in [26].

b) Selective Rejection of False Signal: If $\bar{B}$ receives both the authentic and false (delayed) sync signals, it may be able to apply angle-of-arrival or signal processing techniques to selectively reject the delayed signal [3]. [9]. However, discrimination based on angle-of-arrival fails if $\mathcal{M}$ is positioned along the line from $\bar{A}$ to $\bar{B}$, and, as conceded in [9], signal-processing-based techniques for selective rejection of false signals can be thwarted by an adversary transmitting an additional nulling signal, as described above.

c) Collaborative Verification: Multiple time seekers may attempt to synchronize to the same time master. In this scenario, the time seekers can potentially detect malicious activity by cross-checking the received signals [16]. In the simplest implementation, all time seekers can collaborate to verify that they are synchronized amongst each other. In case of an uncoordinated attack against a subset of time seekers, this verification would expose the attack since the time offset computed at the attacked subset would be different from that computed at the other stations. In principle, however, it is possible for an adversary to execute a coordinated attack against all the time seekers, thus concealing its presence.

IV. NECESSARY CONDITIONS FOR SECURE SYNCHRONIZATION

This section presents a set of conditions for secure two-way clock synchronization and proves these to be necessary by contradiction. In other words, it is shown that if a two-way clock synchronization protocol does not satisfy any one of these proposed conditions, there exists an attack that can compromise clock synchronization without detection.

It is important to note that the ability to measure RTT in a two-way protocol is necessary, but not sufficient, for provably secure synchronization. As an example, IEEE 1588 PTP is a two-way protocol that has been proposed as an alternative to GNSS for sub-microsecond clock synchronization in critical infrastructure such as the PMU network. But, despite the bidirectional exchange between stations, and hence the ability to measure RTT, recent work has shown that PTP is vulnerable to delay attacks in which a MITM introduces asymmetric delay between $\bar{A}$ and $\bar{B}$. Asymmetric delay breaks the assumption that $\bar{t}_{AB} = \bar{t}_{BA}$ and leads to an erroneous prior for $\bar{t}_{AB}$ and $\bar{t}_{BA}$ for future exchanges. This vulnerability is documented in both the literature [11], [13], [18] and the IEEE 1588-2008 standard. Thus, a secure two-way clock synchronization protocol must satisfy additional security requirements beyond the ability to measure RTT.

The conditions introduced below are not tied to any specific protocol, unlike some measures proposed in the current literature [11]–[17]. They are generally applicable to any two-way protocol (e.g., PTP) for which the foregoing two-way synchronization model applies.

Assuming the time master $\bar{A}$ initiates the two-way communication, the necessary conditions for secure clock synchronization are as follows:

1) Both $\bar{A}$ and $\bar{B}$ must transmit unpredictable waveforms to prevent the adversary $\mathcal{M}$ from generating counterfeit signals that pass authentication. In practice, this implies the use of a cryptographic construct such as a message authentication code (MAC) or a digital signature.

2) The propagation time of the signal must be irreducible to within the alert limit $L$ along both signal paths. For terrestrial stations and wireless clock synchronization, this condition implies synchronization via LOS radio signals as $L \rightarrow 0$.

3) The RTT between $\bar{A}$ and $\bar{B}$ must be known to $\bar{A}$ and measurable by $\bar{B}$ to within the alert limit $L$. The RTT must include the delays internal to both $\bar{A}$ and $\bar{B}$, in addition to the propagation delay. Station $\bar{A}$ must know of any intentional delay introduced by $\bar{B}$, such as the layover time $\bar{t}_{BB}$ introduced earlier.

A. Proof of Necessity of Conditions

1) Stations $\bar{A}$ and $\bar{B}$ must transmit unpredictable signals: To prove this condition is necessary, two scenarios are considered: a) station $\bar{A}$ transmits a signal waveform $s_A$ that is predictable, and, b) station $\bar{B}$ transmits a signal waveform $s_B$ that is predictable.

a) $s_A$ is predictable: $\mathcal{M}$ can compromise synchronization without detection as follows:

i) $\mathcal{M}$ takes up a position between $\bar{A}$ and $\bar{B}$ along the line joining the antennas at the two stations.

ii) $\mathcal{M}$ initially transmits a replica of $s_A$, such that $\bar{B}$ receives identical signals from both $\bar{A}$ and $\mathcal{M}$. Subsequently, $\mathcal{M}$
increases its signal power or otherwise supersedes $s_A$ (e.g., via signal nulling, as discussed earlier) such that $B$ tracks $s_M$, the signal transmitted by $M$. (Hereafter, whenever signals from $M$ compete with those from $A$ or $B$, it will be assumed that those from $M$ exert control.) iii) Exploiting the predictability of $s_A$, $M$ advances its replica $s_M$ with respect to $s_A$ by $|\tau_{AB,M}^k|$, where $\tau_{AB,M}^k < 0$. $B$ tracks the advanced signal, resulting in an error of $\tau_{AB}^k$ in the computed $\Delta t_{AB}^k$, as shown in (10).

iv) $B$ transmits the unpredictable response $s_B$ compliant with the pre-arranged layover time $\bar{\tau}_{BB}$. $M$ intercepts this signal from $B$, and replays it to $A$ with a delay of $\tau_{BA}^k - \tau_{AB,M}^k > 0$, causing $A$ to track the delayed signal. As a result, the RTT is $\tau_{AB}^k + \bar{\tau}_{BB} + \tau_{BA}^k$ as $A$ expects. In summary:

\[
\begin{align*}
\tau_{AB}^k &= \tau_{AB,M}^k + \Delta t_{AB,M}^k \\
\tau_{BA}^k &= \tau_{BA,M}^k + \Delta t_{BA,M}^k = \tau_{BA,M}^k - \tau_{AB,M}^k \\
\Rightarrow \tau_{AB}^k + \bar{\tau}_{BB} + \tau_{BA}^k &= \tau_{AB,M}^k + \Delta t_{BA,M}^k
\end{align*}
\]

Thus, $M$ undoes the effect of its sync advance, preventing $A$ from detecting the attack.

b) $s_B$ is predictable: $M$ can compromise synchronization without detection by replicating $B$’s behavior:

i) $M$ takes up a position between $A$ and $B$ along the line joining the antennas at the two stations.

ii) $M$ receives the sync signal and generates a valid response with a delay

\[
\bar{\tau}_{BB} + \frac{\|x_M - x_B\|}{\|x_A - x_B\|} (\tau_{AB}^k + \tau_{BA}^k) \tag{11}
\]

such that the RTT is $\bar{\tau}_{BB} + \tau_{BB} + \tau_{BA}^k$, as $A$ expects.

iii) $M$ records the unpredictable signal from $A$ and replays it to $B$ with an arbitrary delay $\tau_{AB,M}^k > 0$. This results in an error of approximately $\tau_{AB}^k$ in the computed $\Delta t_{AB}^k$ at $B$, as shown in (10).

2) Propagation time must be irreducible to within $L$: If there exists a channel that reduces the propagation time from $A$ to $B$ or from $B$ to $A$ by more than $L$ as compared to the channel used by $A$ and $B$, then $M$ can compromise synchronization without detection. The following attack assumes the propagation time from $A$ to $B$ is reducible by more than $L$; a similar attack exploits the situation in which the propagation time from $B$ to $A$ is reducible by more than $L$.

i) $M$ records the sync signal $s_A$ going from $A$ to $B$.

ii) $M$ makes the recorded signal reach $B$ advanced by $|\tau_{AB,M}^k|$ compared to $s_A$, where $\tau_{AB,M}^k < -L$. An error of $\tau_{AB,M}^k$ is introduced in the time offset value computed at $B$ as shown in (10).

iii) $M$ records the response signal $s_B$, which has the expected pre-arranged layover time $\tau_{BB} \approx \bar{\tau}_{BB}$. $M$ replays this signal to $A$ with a delay of $\tau_{BA,M}^k = -\tau_{AB,M}^k$ such that the RTT is consistent with what $A$ expects.

3) RTT known to and measurable by $A$ to within $L$: Synchronization can be compromised without detection if $|z_{\text{RTT}}^{kl} - z_{\text{RTT}}| > L$ with non-negligible probability even in the absence of an adversary. This condition can be met if a) the prior estimates $\tilde{\tau}_{AB}^k$, $\tilde{\tau}_{BA}^k$, or $\tilde{\tau}_{BB}$ are not accurate to the corresponding true values to within $L$, or b) the magnitude of the measurement error sum $|w_{\text{BB}}^k + w_{\text{BB}}^l|$ is larger than $L$. Note that the condition $|w_{\text{BB}}^k| > L$ compromises synchronization even absent an adversary. An adversary $M$ can exploit the condition $|z_{\text{RTT}}^{kl} - z_{\text{RTT}}^{k+1}| > L$ as follows:

i) $M$ initially transmits a replica of $s_A$ such that $B$ receives identical signals from both $A$ and $M$. Subsequently, $M$ introduces a delay $\tau_{AB,M}^k > 0$ in the replayed signal $s_M$. As assumed earlier, $s_M$ exerts control and introduces an error of approximately $\tau_{AB,M}^k$ in the computed $\Delta t_{AB}^k$ at $B$, as shown in (10).

ii) Station $B$ transmits the response signal with the pre-arranged layover time $\tau_{BB} \approx \bar{\tau}_{BB}$ with respect to the delayed signal.

iii) In the received signal $r_B$, $A$ identifies the expected feature $l(k)$. The RTT, if measurable, includes the delay $\tau_{AB,M}^k$ introduced by $M$.

iv) However, $A$ is unable to definitively declare an attack, since the errors in the modeled RTT and/or the measurement of RTT are possibly larger than $L$. In other words, it is not possible to claim that $|z_{\text{RTT}}^{kl} - z_{\text{RTT}}^k| > L$ only in the presence of adversarial delay.

V. PROOF OF SUFFICIENCY

This section presents a sufficiency proof for the set of security conditions proposed in the previous section. A sufficiency proof guarantees secure synchronization under the considered system and attack models. This paper draws inspiration from the literature on modern cryptography and formalizes the problem of secure clock synchronization with explicit definitions, assumptions, and proofs.

A. Assumptions

This proof assumes that the system under consideration strictly complies with the set of necessary security conditions. Specifically,

1) Both $A$ and $B$ use an authenticated encryption scheme to generate unpredictable and verifiably authentic signals in the presence of a probabilistic polynomial time (PPT) adversary.

2) The difference between the RTT along the communication channel between $A$ and $B$ and the shortest possible RTT is negligible as compared to $L$.

3) The difference between the modeled delays $\tilde{\tau}_{AB}^k$ and $\tilde{\tau}_{BA}^k$ and the true delays $\tau_{AB}^k$ and $\tau_{BA}^k$, respectively, is negligible as compared to $L$.

\[
|\tilde{\tau}_{AB}^k - \tau_{AB}^k| \ll L \tag{12}
\]

and

\[
|\tilde{\tau}_{BA}^k - \tau_{BA}^k| \ll L \tag{13}
\]

Furthermore, $A$ and $B$ agree upon a fixed layover time $\bar{\tau}_{BB}$, and the difference between this and the true layover time is negligible: $|\tau_{BB} - \bar{\tau}_{BB}| \ll L$. 

4) The standard deviation of the noise corrupting the measurements \( t_{b}^{k} \) and \( t_{\lambda}^{k} \) is negligible compared to the alert limit:

\[
\sigma_{\epsilon} \ll L
\]  

(14)

Notice that the above assumptions are the same as the necessary conditions in Section [IV] but with stricter upper bounds on the conditions.

If symmetric keys are exchanged prior to synchronization, then private-key cryptographic schemes such as Encrypt-then-MAC \([29]\) can be used for authenticated encryption. Alternatively, if the keys must be exchanged over a public channel, then digital signatures \([30]\) can be used to authenticate the encrypted messages. Cryptographic authentication schemes like MAC and digital signatures generate a tag associated with a message. Qualitatively, a MAC or digital signature scheme is secure if a PPT adversary, even when given access to multiple valid message-tag pairs of its own choice (as many as possible in polynomial time), cannot generate a valid tag for a new message with non-negligible probability. Irrespective of the cryptographic scheme used, this proof assumes that the probability of \( M \) generating a new valid sync or response signal is a negligible function of the key length \( n \).

\[
\mathbb{P}[\text{Valid}] < \negl(n)
\]  

(15)

To detect an attack before the synchronization error exceeds \( L \), \( \Lambda \) must select a threshold lower than \( L \) beyond which an attack is declared. Consider the modeled RTT, \( \tilde{t}_{\text{RTT}} \), as defined in (7), and the measurement \( z_{\text{RTT}}^{k} \) as defined in (6). A threshold less than \( L \), say \( L - \delta \) with \( 0 < \delta < L \), is set by station \( \Lambda \) such that if \( \left| z_{\text{RTT}}^{k} - \tilde{t}_{\text{RTT}}^{k} \right| > L - \delta \), then an attack is declared.

### B. Definitions

**Definition V.1.** A PPT adversary \( M \) succeeds if clock synchronization is compromised (Definition [11,12]) and

\[
\left| z_{\text{RTT}}^{k} - \tilde{t}_{\text{RTT}}^{k} \right| \leq L - \delta
\]

**Definition V.2.** Faster-than-light is defined to be hard if \( M \) cannot propagate a signal at a speed higher than the speed of light with non-negligible probability. Under hardness of faster-than-light

\[
\mathbb{P}[\text{Superluminal}] \approx 0
\]

**Definition V.3.** A clock synchronization protocol is defined to be secure if, under the hardness of faster-than-light assumption,

\[
\mathbb{P}[\text{Success}] < \negl(n)
\]

where Success for \( M \) is defined in Definition V.1

### C. Proof

In the presence of an adversary \( M \), the measurement \( z_{\text{RTT}}^{k} \) is modeled as

\[
z_{\text{RTT}}^{k} = r_{AB}^{k} + r_{BA}^{k} + r_{BA}^{l} + r_{BB}^{l} + \tau_{BB} + w_{AB}^{k} + w_{BA}^{l}
\]

(16)

Let \( \tilde{r}_{AB}^{k} \) and \( \tilde{r}_{BA}^{k} \) denote the error in the modeled signal delay due to natural/physical phenomenon. Also, let \( \tilde{\tau}_{BB} \) be the difference between the intended layover time \( \tilde{\tau}_{BB} \) and the actual layover time \( \tau_{BB} \). Note that these might be positive or negative.

\[
\tilde{r}_{AB}^{k} = r_{AB}^{k} - \tilde{r}_{AB}^{k}
\]

(17)

\[
\tilde{r}_{BA}^{k} = r_{BA}^{k} - \tilde{r}_{BA}^{k}
\]

(18)

\[
\tilde{\tau}_{BB} = \tau_{BB} - \tilde{\tau}_{BB}
\]

(19)

From (7), (16), (17), (18), and (19) it follows that

\[
z_{\text{RTT}}^{k} = \tilde{r}_{RTT}^{k} + \tilde{r}_{AB}^{k} + \tilde{r}_{BA}^{k} + \tilde{r}_{BA}^{l} + \tilde{r}_{BB}^{l} + w_{AB}^{k} + w_{BA}^{l}
\]

Following the assumptions in (12) and (13), the residual delays are negligible in comparison to \( L \):

\[
\left| z_{AB}^{k} \right| \ll L
\]

(20)

\[
\left| z_{BA}^{l} \right| \ll L
\]

(21)

This assumption is reasonable since otherwise the system could not confidently meet the accuracy requirements even in the absence of an adversary. Also, if \( \tilde{\tau}_{BB} \) is a short time interval, it is reasonable to assume that

\[
\left| \tilde{\tau}_{BB} \right| \ll L
\]

(22)

Note that \( M \) can advance the signal by (a) forging a valid message/tag pair, or (b) propagating the signal faster-than-light. The assumptions of secure MAC and hardness of faster-than-light enforce that

\[
\mathbb{P}[r_{AB}^{k} < 0] < \mathbb{P}[\text{Valid}] + \mathbb{P}[\text{Superluminal}] \approx \negl(n)
\]

(23)

In order to stay undetected, the adversary must ensure

\[
L - \delta \geq \left| z_{\text{RTT}}^{k} - \tilde{t}_{\text{RTT}}^{k} \right|
\]

\[
= \left| \tilde{r}_{AB}^{k} + \tilde{r}_{BA}^{k} + \tilde{r}_{BA}^{l} + \tilde{r}_{BB}^{l} + w_{AB}^{k} + w_{BA}^{l} \right|
\]

(25)

At the same time, in order to compromise time transfer, from (9), \( M \) must ensure

\[
L \leq \left| \tilde{r}_{AB}^{k} + r_{AB}^{k} + w_{AB}^{k} \right|
\]

\[
\leq \left| \tilde{r}_{AB}^{k} + w_{AB}^{k} + r_{AB}^{k} \right|
\]

\[
\Rightarrow \left| r_{AB}^{k} \right| \geq L - \left| \tilde{r}_{AB}^{k} + w_{AB}^{k} \right|
\]

(26)

The probability of success for \( M \) is evaluated as

\[
\mathbb{P}[\text{Success}] = \mathbb{P}[(\text{Success}) \cap (r_{AB}^{k} < 0)] + \mathbb{P}[(\text{Success}) \cap (r_{AB}^{k} \geq 0)]
\]

\[
= \mathbb{P}[(\text{Success}) \cap (r_{AB}^{k} < 0)] + \mathbb{P}[(\text{Success}) \cap (r_{AB}^{k} \geq 0)]
\]

\[
\leq \mathbb{P}[r_{AB}^{k} < 0] + \mathbb{P}[(\text{Success}) \cap (r_{AB}^{k} \geq 0)]
\]

\[
< \negl(n) + \mathbb{P}[(\text{Success}) \cap (r_{AB}^{k} \geq 0)]
\]

(27)

In the case where \( r_{AB}^{k} \geq 0 \), (26) simplifies to

\[
r_{AB}^{k} \geq L - \tilde{r}_{AB}^{k} + w_{AB}^{k}
\]
Substituting the least possible value of $\tau_{AB, M}^k$ into (25), it follows that

$$|\tau_{AB, N}^k + L - |\tau_{AB, N}^k| + \tau_{BA, N}^l + \tau_{BA, M}^l + \tau_{BB}^l + w_{BB}^l + w_{BA}^l| \leq L - \delta$$

Notice that from the assumptions made in (14), (20), (21), and (22), all terms except $L$ and $\tau_{BA, M}^l$ on the left-hand side of the inequality are negligible compared to $L$; thus,

$$|L + \tau_{BA, M}^l| \leq L - \delta$$

Since both $L$ and $L - \delta$ are defined to be positive, the above inequality simplifies to

$$\tau_{BA, M}^l \leq -\delta$$

where $\delta > 0$. Thus, for $M$ to succeed in the case where $\tau_{AB, M}^k \geq 0$, we must have that $\tau_{AB, M}^l < 0$. As a result

$$\mathbb{P}[(\text{Success}) \cap (\tau_{AB, M}^k \geq 0)] < \text{negl}(n)$$

Thus, from (27)

$$\mathbb{P}[(\text{Success})] < \text{negl}(n)$$

Qualitatively, the proof presented here argues that for the adversary to succeed, it needs to either advance the sync signal ($\tau_{AB, M}^l < 0$), or advance the response signal ($\tau_{BA, M}^l < 0$). With the use of a secure MAC (or digital signature) and the hardness of faster-than-light, the adversary can only succeed with a negligible probability.

VI. SECURE CONSTRUCTIONS

This section specializes the necessary and sufficient conditions for secure clock synchronization to IEEE 1588 PTP. In addition, it presents an alternative to PTP for wireless synchronization—a compliant synchronization system with GNSS-like signals.

A. Secure IEEE 1588 PTP

The necessary and sufficient conditions for secure synchronization, as adapted to IEEE 1588 PTP, are as follows:

1) Stations $A$ and $B$ must use an authenticated encryption scheme to prevent $M$ from generating valid message/tag pairs.

2) The difference between the path delays between $A$ and $B$ and the shortest possible path delays must be negligible as compared to $L$. For wireless PTP (31), (32), this implies communicating over the LOS channel. For traditional wireline PTP, $A$ and $B$ must attempt to communicate over the (nearly) shortest possible path.

3) The path delay, which is usually estimated from the RTT measurements, must be accurately known a priori for secure synchronization. The RTT measurements must be verified against the expected RTT. This implies that the layover time $\tau_{BB}$ must also be known to $A$.

The first condition has already been proposed in the IEEE 1588-2008 standard. The second condition, however, has not been considered in any of the earlier works in the literature. The third condition is similar to the proposal of measuring the path delays during initialization and monitoring the delays during normal operation in (11). However, (11) requires that $B$ respond to $A$ with zero delay during initialization to enable measurement of the reference delays. This condition is sufficient, but not necessary for secure synchronization. The system is in fact secure even if $B$ is allowed a fixed layover time.

The third condition, however, does not resemble the proposed defense in (13), that enforces an upper bound on the synchronization error accumulated between sync messages and recommends that $B$ send its timestamps to $A$ periodically for verification. As explained next, this condition is equivalent to the condition of known and measurable RTT, when adapted according to the system model considered in (13).

Note that the requirement of a zero delay in (11), or a short layover time in this paper, enables $A$ to measure the RTT since the transmit time of the $t^k$ feature in $s_B$, that is $t^k_B$, can be approximately traced back to $A$’s clock to within the alert limit as $t^k_A + t^k_B + \tau_{BB}$. Enforcing the synchronization error to within $L$ and transmitting $B$’s timestamp to $A$ achieves the same objective for the defense in (13), since the transmit time from $B$ can be traced back to $A$’s clock with the assumed approximate synchronization. Therefore, the proposed countermeasures in (11) and (13) are two different incarnations of the third security condition proposed in this paper. Of course, the failure of both (11) and (13) to address the second necessary condition makes their proposed defenses vulnerable to an adversary that can communicate along a shorter time path between $A$ and $B$.

B. Alternative Compliant System

This section describes an alternative wireless clock synchronization protocol that satisfies the set of necessary and sufficient conditions presented in Section IV. The proposed protocol involves bi-directional exchange of GNSS-like pseudo-random codes for continuous clock synchronization, in contrast to discrete packet-based synchronization techniques such as NTP and PTP. It is offered here to illustrate the general applicability of the proposed necessary and sufficient conditions to a range of underlying protocols.

The time master $A$ and the time seeker $B$ communicate wirelessly over the LOS channel between the nodes. To simplify the analysis, it is assumed that $A$ and $B$ securely share long sequences of pseudo-random bits prior to synchronization. These sequences of bits will later enable generation of unpredictable signals. The pseudo-random sequence for $A$ has the form

$$b_A = \{b_A^k\}_{k=0}^N, \quad b_A^k \in \{0, 1\}$$

The pseudo-random code $C_A(t_A)$ for $A$ is then generated as

$$C_A(t_A) = 2b_A^k - 1, \quad t_A \in [t^{k-1}_A, t^{k+1}_A]$$

where $t^{k-1}_A$ denotes the time according to $A$ at which the $k$th feature in $A$’s signal is transmitted. The pseudo-random nature of $b_A$ ensures that $C_A(t_A)$ has good cross-correlation properties, which enables an accurate measurement of the time-of-arrival of A’s signal at B, that is, $\sigma_e \ll L$. Station
A modulates a carrier with the code $C_A$ and transmits a signal $s_A(t_A)$ whose complex baseband representation is given as

$$s_A(t_A) = C_A(t_A) \exp(j\theta_A(t_A))$$

This signal is received at $B$ as

$$r_B(t_B, \tau_{AB}) = s_A(t_A - \tau_{AB}) + w_{AB}(t_A) = C_A(t_A - \tau_{AB}) \exp(j\theta_A(t_A - \tau_{AB})) + w_{AB}(t_A)$$

where all symbols have their usual meanings as detailed in Section III. Station $B$ captures a window $R^k_B$ of $r_B$ and correlates it with a local replica of $C_A$. The result of the correlation enables $B$ to detect the start of the $k$th bit of $C_A$ in the window, and provides a measurement

$$z^k_B = r^k_B + w^k_{AB}$$

of the time-of-arrival of the $k$th bit at $B$. Furthermore, the relationship between the start of the $k$th bit and $t^k_{AB}$ enables $B$ to infer the latter.

If a prior estimate $\bar{\tau}^k_{AB}$ of $\tau^k_{AB}$ is available, then $B$ estimates the clock offset $\Delta t^k_{AB}$ as in (4).

Similar to the pseudo-random sequence and code construction for $A$, $B$ generates its unpredictable code $C_B(t_B)$. $A$ and $B$ agree on a one-to-one mapping between $C_A$ and $C_B$ such that $B$ responds with the $l$th bit of $C_B$ on reception of the start of the $k$th bit of $C_A$. Furthermore, $A$ and $B$ agree that the start of the $l$th bit of $C_B$ will have a code-phase offset of $\bar{\tau}^l_{BB}$ with respect to the start of the $k$th bit of $C_A$. Station $B$ transmits the response signal as

$$s_B(t_B) = C_B(t_B) \exp(j\theta_B(t_B))$$

such that

$$t^l_{BA} = z^l_B + \bar{\tau}^l_{BB}$$

according to the time at $B$. In true time, the epoch $t^l_{BA}$ corresponds to

$$t^l_{BA} = t^k_A + \bar{\tau}^k_{AB} + w^k_{AB} + \tau^l_{BB}$$

Station $A$ receives the response as

$$r_A = s_B(t_A - \tau_{BA}) + w_{BA}(t_A)$$

and captures a window of the signal $R^l_A$. $A$ correlates $R^l_A$ with a local replica of $C_B$ to detect the start of the $l$th bit of $C_B$. This enables $A$ to measure the time-of-arrival

$$z^l_A = t^l_{BA} + w^l_{BA}$$

Moreover, the detection of the $l$th bit indicates that it was transmitted in response to the receipt of the start of the $k$th bit of $C_A$. Since $A$ knows the start time of the $k$th bit as $t^k_A$, it measures the RTT as described in (6).

Note that the exchange of one-time pad sequences enables the proposed system to satisfy the first security condition. Wireless LOS communication satisfies the second security condition, and the knowledge of the code-phase layover offset enables $A$ to make an accurate prior estimate of the RTT within the alert limit, thereby satisfying the third security condition. Thus, the proposed system complies with all three necessary and sufficient conditions for secure clock synchronization.

VII. CONCLUSIONS

A fundamental theory of secure clock synchronization was developed for a generic system model. The problem of secure clock synchronization was formalized with explicit assumptions, models, and definitions. It was shown that all possible one-way clock synchronization protocols are vulnerable to replay attacks. A set of necessary conditions for secure two-way clock synchronization was proposed and proved. Compliance with these necessary conditions with strict upper bounds was shown to be sufficient for secure clock synchronization, which is a significant result for provable security in critical infrastructure. The general applicability of the set of security conditions was demonstrated by specializing these conditions to design a secure PTP protocol and an alternative secure two-way clock synchronization protocol with GNSS-like signals.

ACKNOWLEDGMENTS

This project has been supported by the National Science Foundation under Grant No. 1454474 (CAREER), by the Data-supported Transportation Operations and Planning Center (DSTOP), a Tier 1 USDOT University Transportation Center, and by the U.S. Department of Energy under the TASQC program led by Oak Ridge National Laboratory.

REFERENCES

[1] A. Phadke, B. Pickett, M. Adamiak, M. Begovic, G. Benmouyal, R. Burnett Jr, T. Cease, J. Goossens, D. Hansen, M. Kezunovic et al., “Synchronized sampling and phaser measurements for relaying and control,” IEEE Transactions on Power Delivery, vol. 9, no. 1, pp. 442–452, 1994.
[2] J. G. McNeill, “The global positioning system,” IEEE Transactions on Microwave Theory and Techniques, vol. 50, no. 3, pp. 645–652, 2002.
[3] J. J. Angel, "When finance meets physics: The impact of the speed of light on financial markets and their regulation," Financial Review, vol. 2, no. 49, pp. 271–281, 2014.
[4] J. C. Corbett, J. Dean, M. Epstein, A. Fikes, C. Frost, J. J. Furman, S. Ghemawat, A. Gubarev, C. Heiser, P. Hochschild et al., "Spanner: Google globally distributed database," ACM Transactions on Computer Systems (TOCS), vol. 31, no. 3, p. 8, 2013.
[5] L. D. Shapiro, “Time synchronization from Loran-C,” IEEE Spectrum, vol. 8, no. 5, pp. 46–55, 1968.
[6] A. Bauch, P. Hetzel, and D. Piester, “Time and frequency dissemination with DCF77: From 1959 to 2009 and beyond,” PTB-Mitteilungen, vol. 119, no. 3, pp. 3–26, 2009.
[7] D. W. Allan and M. A. Weiss, Accurate time and frequency transfer during common-view of a GPS satellite. Electronic Industries Association, 1980.
[8] M. L. Psiaki and T. E. Humphreys, “GNSS spoofing and detection,” Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, 2016.
[9] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, “GNSS signal authentication via power and distortion monitoring,” IEEE Transactions on Aerospace and Electronic Systems, 2018, to be published.
[10] D. Chou, L. Heng, and G. Gao, “Robust GPS-based timing for phasor measurement units: A position-information-aided approach,” in Proceedings of the ION GNSS+ Meeting, 2014.
[11] M. Ullmann and M. Vogeler, “Delay attacks — Implication on NTP and PTP time synchronization,” in Precision Clock Synchronization for Measurement, Control and Communication, 2009. ISPCS 2009. International Symposium on. IEEE, 2009, pp. 1–6.
[12] T. Mizrahi, “A game theoretic analysis of delay attacks against time synchronization protocols,” in Precision Clock Synchronization for Measurement Control and Communication (ISPCS), 2012 International IEEE Symposium on. IEEE, 2012, pp. 1–6.
[13] B. Moussa, M. Debbabi, and C. Assi, “A detection and mitigation model for PTP delay attack in an IEC 61850 substation,” IEEE Transactions on Smart Grid, 2016.
[14] Q. Yang, D. An, and W. Yu, “On time desynchronization attack against IEEE 1588 protocol in power grid systems,” in Energytech, 2013 IEEE. IEEE, 2013, pp. 1–5.

[15] J.-C. Tournier and O. Goerlitz, “Strategies to secure the IEEE 1588 protocol in digital substation automation,” in Critical Infrastructures, 2009. CRIS 2009. Fourth International Conference on. IEEE, 2009, pp. 1–8.

[16] S. Bhamidipati, Y. Ng, and G. X. Gao, “Multi-receiver GPS-based direct time estimation for PMUs,” in Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016), Portland, OR, 2016.

[17] Y. Ng and G. X. Gao, “Robust GPS-based direct time estimation for PMUs,” in Position, Location and Navigation Symposium (PLANS), 2016 IEEE/ION. IEEE, 2016, pp. 472–476.

[18] R. Annessi, J. Fabini, and T. Zseby, “SecureTime: Secure multicast time synchronization,” arXiv preprint arXiv:1705.10669, 2017.

[19] L. Narula and T. E. Humphreys, “Requirements for secure wireless time transfer,” in Proceedings of the IEE/IION PLANs Meeting, Savannah, GA, 2016.

[20] R. C. Merkle, “Secure communications over insecure channels,” Communications of the ACM, vol. 21, no. 4, pp. 294–299, 1978.

[21] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” 1984.

[22] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Physical review letters, vol. 67, no. 6, p. 661, 1991.

[23] P. Misra and P. Enge, Global Positioning System: Signals, Measurements, and Performance, revised second ed. Lincoln, Massachusetts: Gangan-Jumana Press, 2012.

[24] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, “A proposed navigation message authentication implementation for civil GPS anti-spoofing,” in Proceedings of the ION GNSS Meeting. Portland, Oregon: Institute of Navigation, 2011.

[25] D. M. Akos, “Who’s afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC),” Navigation, Journal of the Institute of Navigation, vol. 59, no. 4, pp. 281–290, 2012.

[26] T. E. Humphreys, Springer Handbook of Global Navigation Satellite Systems. Springer, 2017, ch. Interference, pp. 469–504.

[27] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, “Robust joint multi-antenna spoofing detection and attitude estimation using direction assisted multiple hypotheses RAIM,” in Proceedings of the 25th Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2012). ION, 2012.

[28] D. Borio, “PANOVA tests and their application to GNSS spoofing detection,” IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 1, pp. 381–394, Jan. 2013.

[29] M. Bellare and C. Namprempre, “Authenticated encryption: Relations among notions and analysis of the generic composition paradigm,” Advances in Cryptology ASIACRYPT 2000, pp. 531–545, 2000.

[30] S. Goldwasser, S. Micali, and R. L. Rivest, “A digital signature scheme secure against adaptive chosen-message attacks,” SIAM Journal on Computing, vol. 17, no. 2, pp. 281–308, 1988.

[31] A. Mahmood, G. Gaderer, H. Trsek, S. Schwalowsky, and N. Kerô, “Towards high accuracy in IEEE 802.11 based clock synchronization using PTP,” in Precision Clock Synchronization for Measurement Control and Communication (SPCS), 2011 International IEEE Symposium on. IEEE, 2011, pp. 13–18.

[32] T. Cooklev, J. C. Eidson, and A. Pakdaman, “An implementation of IEEE 1588 over IEEE 802.11b for synchronization of wireless local area network nodes,” IEEE Transactions on Instrumentation and Measurement, vol. 56, no. 5, pp. 1632–1639, Oct. 2007.