

Requirements for Secure Wireless Time Transfer

Lakshay Narula

Electrical and Computer Engineering
The University of Texas at Austin
Email: lakshay.narula@utexas.edu

Todd E. Humphreys

Aerospace Engineering and Engineering Mechanics
The University of Texas at Austin
Email: todd.humphreys@mail.utexas.edu

Abstract—Time transfer is the backbone of all technologies that require synchronization between stations. Wireless time transfer protocols generally employ simple and convenient one-way communication for synchronization of different nodes. However, it is argued that all one-way wireless time transfer protocols are fundamentally vulnerable to replay attacks that compromise timing information. Necessary conditions for security of a two-way time transfer protocol are proposed and proved by contradiction. Furthermore, an example compliant system is presented in detail. The uncertainty in estimation of tropospheric delay using common climatological models is studied and its effect on the accuracy of one-way time transfer and security of two-way time transfer is presented. Analysis of these models suggest that they are adequate for nanosecond-level accurate time transfer over links that are shorter than 10 km, but more sophisticated weather estimation techniques are needed if this accuracy is to be achieved over long distances.

Keywords—time transfer; security; tropospheric delay.

I. INTRODUCTION

Secure time transfer is critical to a host of technologies and infrastructures 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 use time transfer to synchronize their base stations, and time-stamping of financial transactions also requires a way to distribute a common time reference across the globe [2]. Many time transfer applications have stringent accuracy and security requirements.

Wireless transfer of time is a popular technique owing to its convenience and affordability as compared to wireline time transfer. However, wireless time transfer is inherently less secure than wireline time transfer because the physical security of the signal path is worse. Accurate wireless time transfer has traditionally been achieved using Global Navigation Satellite Systems (GNSS) such as Global Positioning System (GPS) [2], which have satellites equipped with atomic clocks that are corrected and synchronized to the most accurate time standards available. Using GNSS, any number of stations on Earth can be synchronized to a common time reference within a few tens of nanoseconds [3].

Wireless time transfer using GNSS, and other protocols such as LORAN (Long Range Navigation) [4], DCF77 [5] or MSF, is based on one-way communication between the time master station, A, and the time seeker station, B. In this mode of time transfer, A acts as a broadcast station and may send

out timing signals either continuously or periodically. The principal drawbacks of one-way wireless time transfer are as follows:

- All possible wireless one-way protocols for time transfer are insecure, as they are vulnerable to meaconing attacks. A meaconing attack is a form of man-in-the-middle attack in which an adversary fraudulently delays or repeats a valid transmission from one station to another station. Measures can be taken to improve the security of one-way protocols against meaconing and other signal and data-level spoofing attacks [6], but, as will be shown later, they remain fundamentally insecure to such threats. For example, the system may be made secure against attacks that involve a less sophisticated spoofer, but remain vulnerable to more powerful adversaries.
- In one-way wireless time transfer systems, the propagation delay of the communication channel either remains uncompensated or has to be estimated using some sort of model. For example, in the case of GPS, the propagation delay is estimated based on the distance between satellite and receiver, ionospheric delay models possibly aided by dual-frequency signals, and tropospheric delay models [7]. The latter is hardest to estimate due to non-dispersive and volatile nature of the tropospheric layer. The term tropospheric delay is often used to refer to the neutral atmospheric delay as a whole, as troposphere is by far the greatest contributor to the delay caused by neutral atmosphere. In applications where the accuracy and security requirements of time transfer are stringent, the error in estimation of tropospheric delay becomes a concern. In contrast, the overall propagation delay can be measured directly in case of two-way time transfer [8].

In two-way time transfer protocols, both A and B transmit and receive signals to perform time synchronization. Two-way time synchronization can overcome the major limitations of one-way time transfer. In a wireless two-way timing protocol, it is possible to measure the round trip delay of the timing signal. This offers a gain in accuracy as the delay is directly measured rather than estimated [8]. Additionally, as will be shown later, wireless two-way time transfer can be made highly robust against man-in-the-middle spoofing attacks.

The focus of this paper is on the security of wireless time transfer with nanosecond-level accuracy requirements. The contributions of this paper are as follows:

- One-way time transfer is shown to be fundamentally insecure against a man-in-the-middle meaconing attack. A set of necessary conditions for secure two-way time transfer are presented and proved.
- An example two-way wireless time transfer communication protocol that satisfies the necessary conditions is proposed.
- Analysis of uncertainty in the estimation of tropospheric delay for wireless time transfer is presented, and its impact on the accuracy of one-way timing and security of two-way time transfer is studied.

The reader is invited to devise an attack against any system that follows all the necessary conditions mentioned in this paper, or alternatively, determine whether the necessary conditions presented are sufficient for a time transfer system to be secure.

The rest of this paper is organized as follows. Section II presents a generic model for wireless time transfer and shows that one-way timing is fundamentally insecure. In Section III, the set of conditions for a wireless time transfer protocol to be secure are presented, and are proved to be necessary by contradiction. A realization of a protocol that satisfies the above necessary conditions is proposed in Section IV. Section V discusses the analysis of uncertainty in the estimation of tropospheric delay and its impact on the accuracy and security of time transfer systems. Concluding remarks are made in Section VI.

II. SYSTEM MODEL

A general system model for wireless time transfer is shown in Figure 1. The time master station, A, holds the timing information to be distributed, and the time seeker, B, wishes to synchronize its clock to the clock at A. For most time transfer applications, the stations A and B have fixed locations, \mathbf{r}_A and \mathbf{r}_B respectively. The time at the high quality clock at A is t_A , and the time at station B, t_B , continuously drifts with respect to the stable clock at A. Station B seeks to track the drift of its clock by an exchange of signals between A and B. A secure data channel may exist between the two stations for secure communication of data packets, if required.

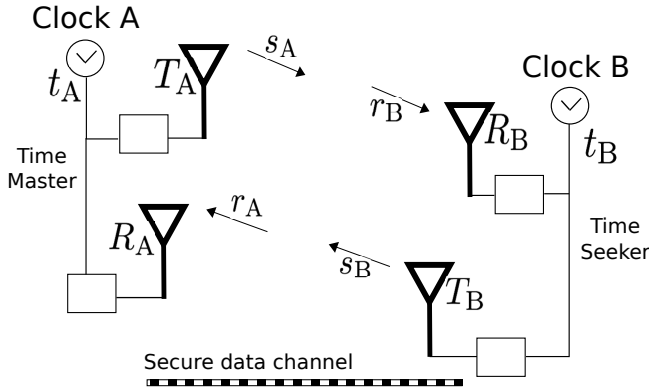


Fig. 1. Abstract model of a time transfer system with a time master station A and a time seeker station B.

Station A sends out a signal whose baseband complex envelope is given as

$$s_A(t_A) = A(t_A) \exp(j\theta_A(t_A)) \quad (1)$$

where j is $\sqrt{-1}$. The signal features in s_A are uniquely tied to the time t_A . Station B receives this signal as

$$r_B(t_A) = A(t_A - \tau) \exp(j\theta_A(t_A - \tau)) \quad (2)$$

where τ is the delay experienced by the signal in going from A to B. This delay depends on the known distance, $\|\mathbf{r}_B - \mathbf{r}_A\|$, and other delays that occur due to interaction of the timing signal with the intervening atmosphere. This expression for r_B ignores noise and fading as these play only a minor role in a security analysis.

A. One-Way Time Transfer Model

In a one-way time transfer system, the exchange of signals between A and B terminates with the reception of r_B at B. Station B is provided information about the signal features in s_A and their dependence on t_A in order to extract the timing information from the received signal. Station B uses these known signal features to measure the pseudorange between A and B as

$$\rho(t) = \|\mathbf{r}_B - \mathbf{r}_A\| + c(t_B - t_A) + T_\rho(t) + I_\rho(t) + w_\rho(t) \quad (3)$$

where t is the true time, t_A is the time at clock at A, t_B is the time at clock at B, T_ρ and I_ρ are the tropospheric and ionospheric delay in distance units, w_ρ is the measurement noise in distance units, and c is the speed of light. Using the known inter-station distance and estimates of other delays, B measures the offset between its clock and the clock at A. It must be noted that any errors in the estimate of the distance between A and B, and in the estimate of the tropospheric or ionospheric delays, will appear as an error in the estimate of the time offset along with the measurement noise error w_ρ . However, the distance between stations can be determined accurately, and the ionospheric delay may also be measured directly if multiple frequencies are used for timing. Tropospheric delay estimation is a challenge, and will be the subject of study later in this paper.

B. Two-Way Time Transfer Model

In a two-way timing protocol, station B may combine the received signal with its own signal, and transmit the combined signal back to A as

$$s_B(t_A, t_B) = A(t_A - \tau) \exp(j\theta_A(t_A - \tau)) + B(t_B) \exp(j\theta_B(t_B)) \quad (4)$$

Station A can measure the round trip time using the returning signal r_A by observing the delay in the signal features it had initially transmitted. The signal received by A can be expressed as

$$r_A(t_A, t_B) = A(t_A - 2\tau) \exp(j\theta_A(t_A - 2\tau)) + B(t_B - \tau) \exp(j\theta_B(t_B - \tau)) \quad (5)$$

where it has been assumed that the propagation delay is symmetric for the onward and return trip of the signal between A and B. The practical implications of this assumption are that the tropospheric parameters remain constant over the round trip. In addition to measuring the round trip time, A might make other measurements to ensure authenticity of time transfer. In case of two-way time transfer, the measured round trip time helps to obtain a better estimate of the propagation delay, that can aid the accuracy of the time transfer process.

It must be noted that in a two-way time transfer system, it is also possible that the time seeker B initiates the two-way protocol. In such a design, B measures both the pseudorange to A and the round trip time of the signal it initiates. However, as will be shown in the next section, this variant of two-way time transfer is vulnerable to man-in-the-middle spoofing attacks.

C. Attack Model

The attack model considered in this paper constitutes of a man-in-the-middle attacker M. It is assumed that M has strong directional antennas with no cost-related limitations. Additionally, M is provided as much computational power as it might need. M knows the locations of A and B, and can take up any position around or between the two stations. It can listen to signals that A and B exchange over the air, and has complete knowledge about their protocol.

A one-way time transfer system is fundamentally vulnerable to a meaconing attack because of its inability to measure the round trip time. As explained earlier, a meaconing attack involves a man-in-the-middle attacker delaying and replaying a valid transmission from one station to another station. This type of attack is extremely effective against a time transfer system as an undetected delay in the propagation of a timing signal from A to B can lead to a direct error in the timing information decoded at B. Furthermore, while counterfeit signal attacks can be prevented by using authentication and cryptographical methods [9], these techniques do not, in general, prevent meaconing attacks because the delayed or repeated signal has the same characteristics as that of the genuine signal that originated at A.

The hostile man-in-the-middle attacker M can hack any wireless time transfer process that uses a one-way protocol by initially retransmitting the authentic timing signal from A with infinitesimally small delay and gradually taking over the tracking loops of the receiver at B by increasing its signal power. Once in control of the communication, the attacker can introduce arbitrary delay in its retransmission, thereby tampering with the time transfer process. Although B might receive both the authentic and delayed signal in some cases, a clever attacker can potentially null the authentic signal from A by amplitude-matched phase-inverted destructive interference, and convince B to accept the timing information in the delayed signal [10]. The delay that the attacker introduces is added to the measured clock offset between A and B.

$$\tilde{\rho}(t) = \|\mathbf{r}_B - \mathbf{r}_A\| + c(t_B - (t_A + \Delta t_M)) + T_\rho(t) + I_\rho(t) + w_\rho(t) \quad (6)$$

where Δt_M is the delay introduced by the man-in-the-middle attacker.

Previous work has shown that if GPS is used for time transfer and the position of B is already known, a meaconing attack can be detected [6]. Also, if multiple receivers participate in a collaborative timing system then it can be hard to perform some of the man-in-the-middle spoofing attacks [6], but fundamentally it is always possible to spoof each receiver separately and compromise the timing of the system.

III. NECESSARY CONDITIONS FOR SECURE TIMING

Given that all one-way time transfer protocols are vulnerable to man-in-the-middle attacks, this paper proposes a set of necessary conditions that a wireless two-way time transfer system can follow in order to be secure. As described in the previous section, the time master A holds the timing information to be distributed, and the time seeker B wishes to synchronize its clock to the clock at A. Assuming a design where A initiates the two-way protocol, the necessary conditions for secure time transfer are as follows:

- 1) The round trip time for a radio wave to travel to and back from station B must be known to within the unpredictable variations introduced by the channel. This must include the constant or modeled delays internal to both A and B, in addition to the propagation delay. Station A must be able to measure the round trip time that the timing signal actually takes to travel to and back from B.
- 2) The round trip time of the timing signal must be irreducible. For terrestrial stations, the practical implementation of this implies use of line of sight radio waves.
- 3) Both A and B must inject unpredictability into their transmitted signals to prevent an intruder M from generating and transmitting counterfeit signals on its own.
- 4) The phasing between the unpredictability injected by A and B must be pre-arranged securely, and A must verify that the phasing of the unpredictable codes in the returning signal is as was decided upon.

In addition to the necessary conditions presented above, a functional requirement for a secure time transfer system is that a secure data channel must exist between A and B. It is important to make a distinction between a secure data channel and a secure timing channel: many protocols for securely transferring data over a channel already exist, but these cannot be used for time transfer because of the uncertain latency of data channels. These secure data channels can be leveraged for exchanging data packets securely when stable propagation delay is not a requirement. For example, in a system where A and B generate unpredictable signals using their public keys, they may exchange the keys over this secure data channel. Also, in case A detects a spoofing attack, it may indicate this condition to B over the secure data channel.

A. Proof of Necessity of Conditions

This section proves that a secure wireless two-way time transfer system must comply with the set of necessary conditions proposed above. The proof presented here uses the

method of contradiction: a potential attack scheme is devised against the time transfer protocol that does not follow either one of the four conditions that are necessary for a secure time transfer process. In all cases, it is assumed that the time seeker B is continuously tracking its clock offset with respect to the clock at time master station A, that is, B only searches for the updated clock offset within a small search region around the current estimate.

1) *Round trip time must be measured and its expected value be known:* To prove that this condition is necessary, two scenarios are considered: (1) Station A does not know the expected round trip time, and, (2) The round trip time is not measured by A. For wireless time transfer systems using radio waves, this implies that A is unaware of its distance to B and other propagation delays. One of the attack strategies that intruder M can take is:

- i) M initially records and replays the unpredictable signal s_A from A without any delay, but with a higher transmit power to capture the tracking loops at B. Gradually, it introduces a delay in the replayed signal, and this results in a delay in the waveform being received at B.
- ii) B estimates an incorrect time offset with respect to the clock at A. However, it still has to maintain the pre-arranged phasing between the two unpredictable signals in the returning signal.
- iii) In the returning signal r_A , A is able to find the expected combined signal with pre-arranged phasing, but the round trip time, if measured, includes the delay introduced by the attacker.
- iv) If station A is unaware of the nominal round trip time that the signal should have taken, it cannot raise an alarm indicating a possible spoofing attack. Also, if the round trip time is not measured, a spoofing attack cannot be detected.

2) *Round trip time must be irreducible:* If there exists a path or channel through which the signal takes less time to travel than the path that the authentic signal takes, then the attacker can take the following approach to disrupt timing operations:

- i) M intercepts the signal s_A going from A towards B.
- ii) As the time of flight of authentic signal is reducible, M can make the intercepted signal reach B before the authentic signal, such that the delay is within the search space of B. M uses a higher transmit power so that B tracks its spoofed signal, and not the authentic signal.
- iii) B decodes the timing information from this spoofed signal, but the estimated propagation delay used is incorrect as it was calculated according to the slower path that the authentic signal takes. This leads to an error in the timing information that B decodes.
- iv) M again intercepts the returning signal s_B that has the expected pre-arranged phasing between the unpredictable signals of A and B. This signal is played back to A, making sure that the round trip time seen by A is according to the slower path it expects the signal to follow.

- v) No alarm is raised by A as both the round trip time and the pre-arranged phasing are as expected. M increases the delay gradually to introduce large error in the timing information.

3) *Stations A and B must inject unpredictability:* To prove that this condition is necessary, two scenarios are considered: (1) Station A transmits a signal waveform s_A that is predictable, and, (2) Station B combines r_B with a waveform that is predictable.

a) *Station A does not inject unpredictability:* In the scenario where A transmits a predictable signal that is tied to its clock, a possible strategy that the attacker M can follow is:

- i) Using the predictable nature of waveform s_A , M can generate a local replica and measure the phase of s_A at A.
- ii) Initially M transmits its local replica of s_A such that the signal received at B from both A and M is the same. Then, M gradually increases the signal power to capture the tracking loops at B.
- iii) At this point, using the predictability of spreading code of A, M slightly advances the phase of its replica by Δt_M . Due to higher signal strength of signal from M, B tracks this spoofed signal. This causes an error of Δt_M in the decoded timing information.
- iv) Further, B combines r_B with an unpredictable signal taking care of the pre-arranged phasing that A would expect. M records this signal from B, and plays it to A with a delay such that the round trip time measured by A is as expected. Station A, thus, cannot notice any sign of a spoofing attack.

b) *Station B does not inject unpredictability:* Consider a scenario where B combines a predictable signal with the received signal r_B and sends the combined signal back to A. In such a setting, the adversary M takes the following approach:

- i) M records the signal s_A as it goes from A towards B. Furthermore, it also records the returning signal s_B that goes from B towards A.
- ii) Knowing the location of B, M combines the two recordings such that s_A is removed from s_B , and it is left with a recording of the predictable signal that B generates.
- iii) Now using a local replica of B's predictable signal and the above recorded data, M figures out the current phase of s_B at B.
- iv) From this point on, M can generate the B's predictable waveform into the future and having obtained the current phasing of s_B , it can maintain the pre-arranged phasing that A expects to see. However, as M cannot track the unpredictable signal from A, it is required that M has a stable clock that does not drift with respect to A. Round trip timing requirement can be met easily.
- v) Using the above steps, M has effectively short-circuited the signal path using a local replica of B's predictable waveform. M can now conveniently delay the signal going

from A to B and disrupt the timing operations between A and B.

4) *Pre-arranged phasing of codes in returning signal:*

Station A knows the round trip time of the signal to within the uncertainty in the propagation delay, and expects to find the unpredictable waveforms from both A and B in the returning signal. However, it has no information about the relative phasing between the two waveforms. An attacker can spoof falsified timing information at B while keeping A unaware of the attack as follows:

- i) M records the signal s_A as it goes from A towards B. Furthermore, it replays s_A with a slight delay and higher transmit power, such that B starts to track the spoofed signal from M. B decodes timing information using this delayed signal and thus, an error is introduced in the time transfer process.
- ii) Also, B combines the spoofed signal with its own unpredictable waveform and sends it back. If A were to track this signal from B, it would measure a longer round trip time due to the introduced delay, and detect the attack. But M has a recording of the signal from A that it can play back in accordance with the expected round trip time. M, however, needs to combine that recording with B's unpredictable waveform.
- iii) M combines the recorded s_A with the returning s_B such that s_A is removed from the returning signal, and the resulting output has the unpredictable waveform from B.
- iv) M can now fabricate a spoofed returning signal using recorded waveforms of A and B, while taking care of the round trip time of the signal as observed at A.
- v) The phasing between the two spreading codes in the spoofed returning signal is different than that in the authentic returning signal, but A does not have any information about the expected phasing, and thus cannot detect the attack.

It must be noted that the final necessary condition for secure time transfer precludes the use of a design where time seeker B initiates the two-way protocol, because if time master A tries to align the waveforms in the pre-arranged phasing, the timing information contained in the phase of A's waveform will be lost.

In this section it was proven that the mentioned conditions are necessary for a wireless two-way time transfer system to be secure. The authors believe that a system that follows these conditions is robust to any kind of spoofing attack by a man-in-the-middle. The reader is invited to invent an attack against a compliant system, or prove the sufficiency of these conditions.

IV. EXAMPLE OF A COMPLIANT SYSTEM

This section proposes a time transfer system that follows the set of necessary conditions presented in Section III. The proposed system uses unpredictable orthogonal spreading codes to allow multiple time seekers to interface with one time master. As explained in the previous section, the two-way timing protocol is initiated by the transmitter at time master

station A. The inter-station distance is known to A and B, and stations communicate via line-of-sight radio waves.

Station A generates an unpredictable spreading code C_A using its public key [11]. This code is tied to A's clock, that is, the code-phase of the spreading code used by A is determined uniquely by the time at clock A. Station A uses this spreading code to modulate a carrier at frequency f_A . The signal transmitted is thus given as

$$s_A(t) = \sqrt{2P_A}C_A(t_A) \cos(2\pi f_A t + \theta_A) \quad (7)$$

where P_A is the power of the signal transmitted by A, t is the true time, and t_A is the time at A. This signal travels to station B and assuming a unit channel gain it is received there as

$$r_B(t) = \sqrt{2P_A}C_A(t_A - \tau_A(t)/2) \cos(2\pi f_A t + \theta_A^{AB}(t)) \quad (8)$$

where $\tau_A(t)$ is the delay of the spreading code that A sees after the round trip of its signal to B, and $\theta_A^{AB}(t)$ is the carrier phase of $s_A(t)$ as received at B. The medium between A and B is assumed to be symmetric for the onward and return journey of the signal, which is reasonable because of the extremely short time that a radio wave takes to make the round trip. This assumption implies that the delay in the spreading code of A as observed in the $r_B(t)$ is $\tau_A/2$.

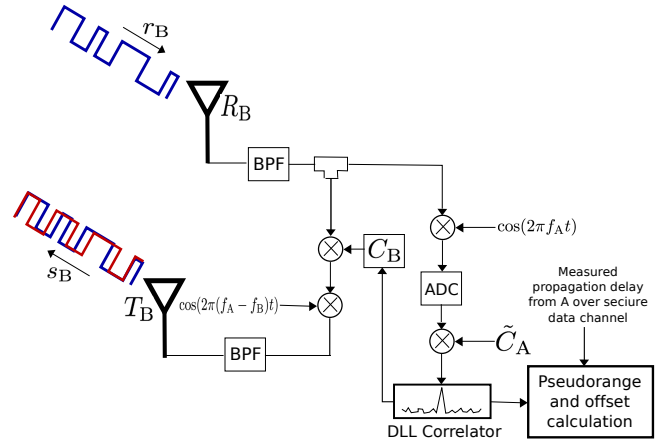


Fig. 2. Transceiver design at time seeker B for the proposed compliant system.

On reception of this signal, B first needs to measure its pseudorange to A so that it can decode the timing offset between its clock and the master clock at A. The design of the transceiver at B is shown in Figure 2. Station B mixes the incoming signal with a phase-matched tone of frequency f_A . A delay-lock loop (DLL) is then set up to measure the code-phase of the resulting baseband signal. Using the public key of A, B locally generates a replica of C_A . Station B tries to align the locally generated code with the incoming code by delaying or advancing the local replica. Let $\tau_A^B(t)$ be the shift with respect to t_B that gives highest correlation between the local and incoming code. At this point of highest correlation, the local replica is the same as the received spreading code and is given by

$$C_A^B(t) = C_A(t_B - \tau_A^B(t)) \quad (9)$$

From equation (8) it is seen that the received code-phase must be $(t_A - \tau_A/2)$. Thus, from equations (8) and (9) it can be concluded that

$$\tau_A^B(t) = t_B - t_A + \tau_A(t)/2 \quad (10)$$

which can be multiplied by the speed of light, c , to get the pseudorange as follows:

$$\rho(t) = \|\mathbf{r}_B - \mathbf{r}_A\| + c(t_B - t_A) + T_\rho(t) + I_\rho(t) + w_{\rho A}^B(t) \quad (11)$$

where $T_\rho(t)$ and $I_\rho(t)$ are the true tropospheric and ionospheric delays experienced by the radio wave, and $w_{\rho A}^B(t)$ is the measurement noise in the pseudorange at B. At this point, B can estimate the clock offset between the clocks at A and B, $t_B - t_A$, because all other terms in equation (11) except noise are either known or can be estimated. It must be noted that up to this point, the proposed system behaves exactly like a one-way time transfer system. As a result, the propagation delay needs to be estimated and is not actually measured. As will be shown later, A can provide periodic measurements of the propagation delay to B to improve the accuracy of the timing system.

Once B locks on to the correlation peak at the DLL, it continuously tracks the clock at A. The value of τ_A^B does not change abruptly because of the smooth drift of the clock and frequent measurements made by B. As a consequence, B only searches for the correlation peak in a narrow region close the current estimate of τ_A^B .

In accordance with the necessary conditions, B must send a signal back to A for verification of the authenticity of timing information. The verification process by A is two fold:

- 1) Station A measures the round trip time of the timing signal to ensure that an intruder M did not delay the signal in between.
- 2) Station A verifies the pre-arranged phasing of spreading codes of A and B in the returning signal.

Station B now needs to modulate the received signal with its unpredictable spreading code C_B in accordance with the pre-arranged phasing between the codes of A and B. An example of pre-arranged phasing might be that B must perfectly align the n^{th} chip of its code with the n^{th} chip of A's code. Assume, without loss of generality, that spreading codes of A and B have the same chipping rate. In such a scenario, C_A and C_B must have the same code-phase in combined signal. Using the code-phase of C_A from the DLL, B modulates the received signal with C_B such that the pre-arranged phasing is maintained. Finally, B mixes the signal with a tone of frequency $(f_A - f_B)$ and passes the resulting signal through a band-pass filter to get

$$s_B(t) = \sqrt{2P_B} C_A(t_A - \tau_A(t)/2) C_B(t_A - \tau_A(t)/2) \cos(2\pi f_B t + \theta_B(t)) \quad (12)$$

where P_B is the power of the signal transmitted by B, and $\theta_B(t)$ is the resulting carrier phase of the signal after mixing. It must be noted that even though the signal has to be digitized to measure the code-phase of A, all the modulation and mixing

occurs in an analog RF front end, which is desirable because of the stable RF delays.

The combined signal transmitted by B is then received at A as

$$r_A(t) = \sqrt{2P_B} C_A(t_A - \tau_A(t)) C_B(t_A - \tau_A(t)) \cos(2\pi f_B t + \theta) \quad (13)$$

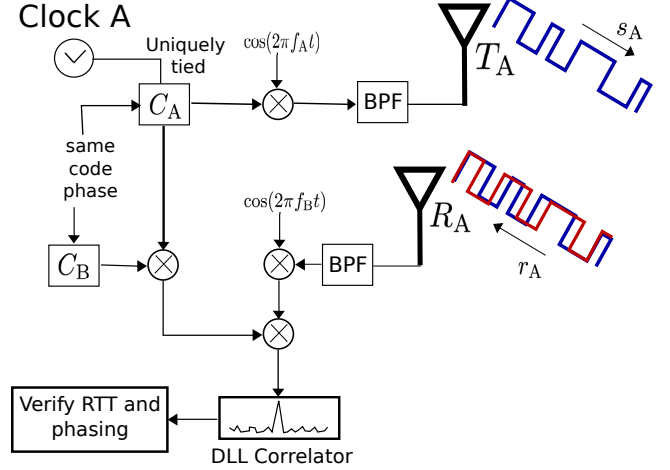


Fig. 3. Transceiver design at time master A for the proposed compliant system. Time master tracks each time seeker individually in separate tracking loops.

The design of the transceiver at A is shown in Figure 3. Station A first converts the received signal to a baseband signal. Station A can generate both C_A and C_B using the keys exchanged over the secure data channel. Once the relative phasing of these codes in the returning signal is agreed upon, A can locally generate the combined code it expects to see in the returning signal. The code-phase of this combined code depends on the round trip time of the signal. Station A expects to see a round trip time $\tilde{\tau}_A(t)$ given by

$$c \cdot \tilde{\tau}_A(t) = 2\|\mathbf{r}_B - \mathbf{r}_A\| + 2\tilde{T}_\rho(t) + 2\tilde{I}_\rho(t) \quad (14)$$

where $\tilde{T}_\rho(t)$ and $\tilde{I}_\rho(t)$ are the expected tropospheric and ionospheric delays. Thus, A generates a local replica of the combined code as

$$\tilde{C}_{AB} = C_A(t_A - \tilde{\tau}_A(t)) C_B(t_A - \tilde{\tau}_A(t)) \quad (15)$$

Station A then aligns the returning code and the local combined code by advancing or delaying the local replica. The measured round trip delay τ_A is indicated to B over the secure data channel periodically. Station B uses this information to improve the accuracy of the timing information decoded, as instead of estimating the tropospheric delay it can now use the measured value.

However, A only searches a small region around the expected code-phase τ_A . If A does not find a correlation peak within the search range, it concludes that either the phasing between the two spreading codes in the returning signal is not as decided upon, or the round trip time is abnormally deviant

from the expected value. In this scenario, A indicates to B over the secure channel that the timing information exchanged is not trustworthy.

The kind of man-in-the-middle meaconing attack that lead to failure of one-way time transfer is ineffective against two-way timing systems such as the one proposed above. Station A has the means to measure the round trip time that the signal actually takes to go to B and back, and it has prior knowledge about the round trip time that the signal must take, to within the uncertainties of the propagation delay of the signal. Station A can detect any discrepancy between the expected and measured value of τ_A and can reject the spoofed signal.

The accuracy of time transfer using this compliant system depends on the chip duration T_c of the spreading codes used by the two stations:

$$T_c = 1/f_c \quad (16)$$

where f_c is the frequency of the spreading code. A good rule of thumb is that a system using chip duration T_c can achieve a timing accuracy of $T_c/100$ at high signal-to-noise ratio. Thus, using a spreading code of frequency 10 MHz can provide an accuracy of 1 nanosecond.

V. TROPOSPHERIC DELAY ESTIMATION

Estimating the tropospheric delay is essential for highly accurate and secure wireless time transfer between stations. The motivation behind estimating this delay is two-fold:

- As explained earlier, unlike the physical distance between stations and ionospheric delay, the tropospheric delay cannot be measured directly in a one-way communication link [8]. An error in the estimate of the tropospheric delay degrades the accuracy of the timing information. For example, an error of 100 nanoseconds in the estimate of tropospheric delay leads to an error of 100 nanoseconds in the measured time offset between A and B. Thus, for highly accurate timing requirements, it is required that the troposphere is modeled accurately.
- In a two-way time transfer system, the tropospheric delay is measured by observing the round trip time of the timing signal and assuming that the delay is equal for the onward and return journey of the signal [8]. This eliminates the inaccuracy introduced by possibly erroneous estimation of the delay. However, as seen in Section III, the security of time transfer hinges on prior knowledge of expected time that the signal must typically take to make the round trip. Uncertainty in the estimate of the tropospheric delay, and consequently in the round trip time, provides a window for the attacker to delay or advance timing signal without being detected by the round trip time check.

The degree to which troposphere must be modeled accurately depends on the accuracy and security requirements of the time transfer system. For instance, if timing errors of 10 microseconds are permissible for some application, then modeling of the troposphere might not be required at all. However, this paper explores the limits of tropospheric delay estimation as nanosecond accurate time transfer is of interest.

A. Delay Model

The speed at which a radio wave travels through a medium is characterized by the index of refraction of the medium. The index of refraction is defined as the ratio of the speed of the radio wave in vacuum to the speed of radio wave in the medium of interest. The index of refraction of vacuum is unity. However, the index of refraction of the troposphere is a little greater than unity, typically close to 1.0003 at standard temperature and pressure (STP) [12]. This implies that a radio wave takes a longer time to cover a given distance within the troposphere than it would in vacuum. This excess time taken is known as the tropospheric delay. As mentioned earlier, troposphere is by far the greatest contributor to the neutral atmospheric delay experienced by radio waves, and the term tropospheric delay is often used to refer to the delay introduced due to the neutral atmosphere.

The refractive index of the troposphere depends on the local meteorological conditions. Given the parameters ρ (total mass density of air in kg/m^3), e (partial pressure of water vapor in mb), and T (temperature in Kelvin), the refractivity can be calculated as [13]

$$N = k_1 R_d \rho + k_2' (e/T) Z_w^{-1} + k_3 (e/T^2) Z_w^{-1} \quad (17)$$

where N is the refractivity, k_1 is equal to $77.604 \text{ K}\cdot\text{mbar}^{-1}$, k_2' is equal to $17 \text{ K}\cdot\text{mbar}^{-1}$, k_3 is equal to $377600 \text{ K}^2\cdot\text{mbar}^{-1}$, and Z_w^{-1} is a factor close to unity that accommodates for non-ideal gas behavior of air.

The tropospheric delay is then given by the path integral of refractivity:

$$\Delta = 10^{-6} \cdot \int_{\text{path}} N(l) \cdot dl \quad (18)$$

B. Existing Methods for Tropospheric Delay Estimation

Tropospheric delay estimation is done commonly in most GNSS receivers. For the case of satellite-based navigation, the transmitter is outside Earth's atmosphere, whereas the receiver is within the atmosphere. As a result, the models for estimating tropospheric delay in GNSS first estimate the delay directly upwards from the receiver to the top of the troposphere, and then map this delay to the elevation of each satellite using a mapping function [7]. Clearly, this kind of scheme would not work for terrestrial time transfer systems as both the transmitter and the receiver may be within the troposphere. The zenith delay as seen by the receiver, in itself, is inconsequential in measuring the delay along the path of the timing signal.

Emerging applications such as pseudolite-based positioning and Ground-Based Augmentation System (GBAS) have prompted the formulation of tropospheric delay estimation models that are applicable to intra-troposphere communication links. One such model proposed by Radio Technical Commission for Aeronautics (RTCA) estimates the delay by taking into account the refractivity of the troposphere at the receiver, and the slant path length and altitude difference between the transmitter and the receiver [14]. However, it has been shown that the estimate of the delay is not reliable when the altitude

difference between the transmitter and receiver is large [15]. Moreover, the refractivity might change along the path of the signal and deviate from the value at the receiver.

Another method proposed for estimating tropospheric delay involves imagining a virtual GNSS satellite in outer space along the line joining the transmitter and the receiver [15]. The idea is to estimate the tropospheric delay to the virtual satellite as seen individually by the two stations and then differencing them to obtain the delay experienced in going from one station to the other. This involves estimating the zenith delay and mapping it to the required elevation for both stations. Saastamoinen model and Niell mapping function (NMF) are the commonly used mapping functions [16], [17]. However, these functions do not provide reliable estimates of delay at low elevation. In particular, the Saastamoinen model and NMF are only accurate above elevation angles of 10° and 4° , respectively. In terrestrial applications it might be very common to have the transmitter and receiver at almost the same altitude. In such cases, the elevation angle would be close to 0° and this approach would not be reliable.

A network of reference GNSS stations at known locations has previously been used to estimate the tropospheric delay and to provide this estimate to a rover station in the local region [18]. However, as shown in Section II, GNSS receivers being one-way communication links are fundamentally insecure and thus the tropospheric delay estimates derived from such a system might be falsified by an attacker.

Recent research work has focused on using Numerical Weather Models (NWM) to estimate the tropospheric delay seen by GNSS receivers [19]. Moderately accurate results have been shown in the estimation of GNSS tropospheric delay using a high resolution Weather Research and Forecast (WRF) model at 1 kilometer grid spacing [20]. Although no results have been published for intra-troposphere communication links, the method seems to be promising. However, these numerical models demand very high computational power at high resolution. When dealing with terrestrial links that are only a few hundred kilometers or shorter, the resolution of such NWMs can become a bottleneck. As such, the objective of NWMs is to forecast the weather parameters into the future, whereas estimation of tropospheric delay only requires the current values of weather parameters. So even though NWM based delay estimation looks promising, a reasonable first step would be to explore an alternate method for estimating the weather parameters.

Instead of using one of the approximate models above, the tropospheric delay can be accurately determined by retracing the curved path followed by the radio wave through the non-homogenous medium and taking account of the additional distance travelled by the wave as well as the speed with which the wave would travel through each point on the way. This is known as the ray-tracing technique, and forms the basis of the approximated mapping functions. The only information required for implementation of ray-tracing is the refractivity field in space through which the ray travels. In view of equation (17) this implies that ρ , e , and T be known at each

point along the path of the ray.

Surface measurements of meteorological parameters are available from the large number of weather stations all over the globe. Determination of the 3-dimensional refractivity field is thus a matter of interpolating and extrapolating the meteorological parameters from the weather station locations to the surrounding 3-dimensional space accurately. This is the subject of the remainder of this paper.

C. Interpolation and Extrapolation of Meteorological Data

To generate this refractivity field, the meteorological parameters obtained from weather stations need to be interpolated horizontally along the surface and extrapolated vertically upwards. In this sub-section, a simple technique using existing climatological models is presented, and its limitations are outlined. Additionally, the concept behind an improved data driven approach is explained. The results obtained using this improved approach are being studied, and require further analysis.

1) *Interpolation Along Earth's Surface*: The wide network of ground weather stations all over the world can be leveraged to obtain the true value of meteorological parameters at the station locations. For example, the National Oceanic and Atmospheric Administration (NOAA) provides Quality Controlled Local Climactic Data (QCLCD) for over 2000 weather stations in the USA [21]. Similar databases exist for many other geographical locations on the globe. In addition, a very dense network of Personal Weather Stations (PWS) that update weather data in real-time is also available on the Weather Underground service. The 3-dimensional locations of these weather stations can be indexed by latitude, longitude, and altitude. A simple technique for interpolating the meteorological parameters to any location between the weather stations is to fit a surface through the given data points using a spline-based technique, such as thin plate interpolation. This surface can then be used to query the parameter values at any latitude-longitude pair within the limits of the weather station locations. It must be noted that along with the meteorological parameters, the surface altitude must also be interpolated to uniquely index the location at which the estimated meteorological parameter values are valid. This technique is very simplistic in the sense that it does not take into account any historical correlations between station data, and only interpolates within a snapshot of data points.

To evaluate the performance of this technique, a set of experiments were conducted and the error in the interpolated values of meteorological parameters was analyzed. The experiments used quality controlled data provided by NOAA. For the first experiment scenario, snapshots of surface meteorological conditions were taken at three major cities with a good density of weather stations: Dallas-Fort Worth (DFW), TX; Minneapolis (MIN), MN; and Chicago (CHI), IL. Four snapshots of data were taken for each city between 11:00 and 14:00 on 01/01/2015. The second experiment scenario used the same set up, except that the data snapshots were taken

from 07/01/2015. Each of the cities had around 15 weather stations that provide QCLCD data.

For each snapshot of meteorological data, a smooth surface was fit through all but one of the data points for the three parameters of interest: ρ , e , and T . The stations to which the surface was fit were called training points, and the one station that was left out was called the test point. The interpolated values at the location of the test point were then compared to the true parameter values at the test point. This procedure was repeated with all stations being chosen as the test point one by one. Figure 4 shows one example of the surface that was fit through the mass density of air data points obtained from a snapshot over Dallas-Fort Worth. The red marker denotes the true value of mass density of air at the test point location, and its distance from the surface characterizes the estimation error. Using four snapshots of data from 15 stations over each city, about 60 error points were obtained to generate the error statistics. The root mean square (RMS) errors observed in each of the three parameters of interest have been summarized in Tables I and II for the first and second experiment scenarios, respectively. The RMS error in the interpolated altitude has also been presented.

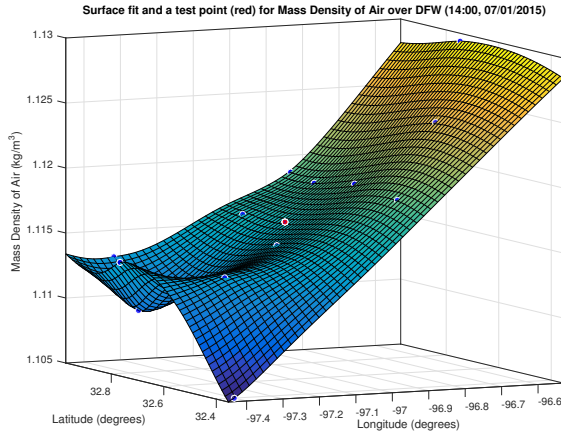


Fig. 4. Spline-based thin plate interpolation on the training points (blue markers) for mass density of air over DFW at 14:00 on 07/01/2015. The red marker shows the true value of mass density of air at the test point.

TABLE I
RMS ERROR IN INTERPOLATED METEOROLOGICAL PARAMETERS
(01/01/2015, 11:00-14:00)

RMS Error	DFW	MIN	CHI
ρ (kg/m ³)	0.0058	0.0098	0.0042
e (mb)	0.5197	0.2576	0.2702
T (K)	0.7910	0.8313	1.0696
h (m)	35.8172	35.5747	20.4472

In order to conclude if this interpolation technique is adequate for accurate estimation of tropospheric delay, it is required that the errors in Tables I and II be mapped to a corresponding distance-equivalent error, which can be used to

TABLE II
RMS ERROR IN ESTIMATED METEOROLOGICAL PARAMETERS
(07/01/2015, 11:00-14:00)

RMS Error	DFW	MIN	CHI
ρ (kg/m ³)	0.0037	0.0097	0.0052
e (mb)	1.5304	1.1111	1.6882
T (K)	0.8415	0.7724	1.4470
h (m)	40.6546	35.5747	20.4472

quantify the uncertainty in tropospheric delay. The distance-equivalent error for a particular parameter can be obtained by setting all other parameters to their nominal values and calculating the difference in tropospheric delay between the nominal and the nominal-plus-error scenarios using Equation (18). For example, to calculate the distance-equivalent error due to the uncertainty in partial pressure of water vapor, ρ is set to a nominal value of 1.2 kg/m³ and T is set to a nominal value of 290 K. Then, the difference in tropospheric delay over 1 km due to the nominal and nominal-plus-uncertainty values of e is calculated using Equation (18). It must be noted that all parameters, as well as the estimate error, are assumed to be constant over the 1 km long path. This would give a pessimistic distance-equivalent error if the error in the estimated parameter is positive at some points along the path and negative at others. But, as will be seen later, a consistently positive error in the parameter estimate is not an unrealistic scenario. Figures 5, 6, and 7 show the distance-equivalent error corresponding to ρ , e , and T , respectively, for a range of estimate errors and nominal meteorological conditions.

The constants k_1 , k_2 , and k_3 used in Equation (17) also have uncertainty in their values due to the experimental difficulty of measuring these constants, and the conflicting values found in the literature [13]. However, the distance-equivalent error introduced due to the uncertainty in these constants is negligible, and may be ignored.

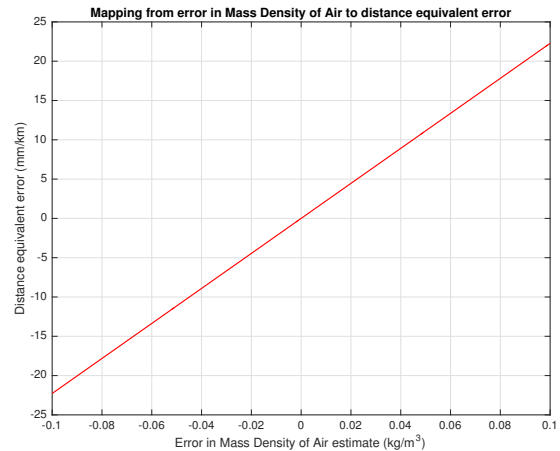


Fig. 5. Distance-equivalent error due to a constant error in the estimate of mass density of air. Note that distance-equivalent error due to ρ does not depend on e or T .

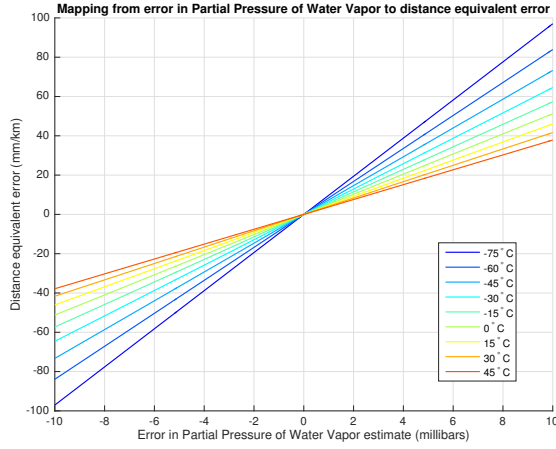


Fig. 6. Distance-equivalent error due to a constant error in the estimate of partial pressure of water vapor. Note that distance-equivalent error due to e depends on the local value of T .

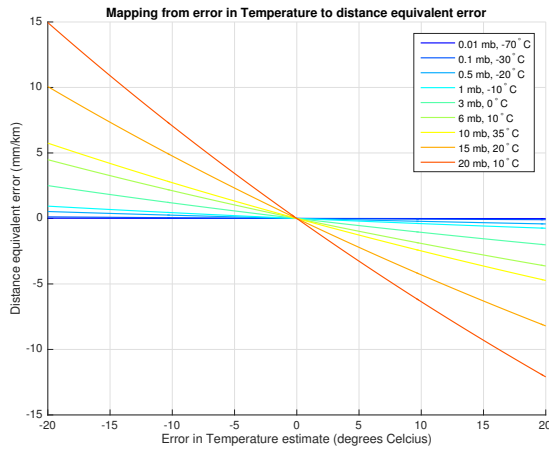


Fig. 7. Distance-equivalent error due to a constant error in the estimate of temperature. Note that distance-equivalent error due to T depends on the local value of e and T itself.

In view of Figures 5, 6, and 7, it can be seen that a simple interpolation on a snapshot of meteorological data might not be adequate for a system that requires nanosecond-level accuracy. For example, the RMS error in estimate of e over Chicago in July 2015 is seen to be 1.6882 mb from Table II. This would lead to a distance-equivalent error of around 1 cm over a 1 km long communication link. For reference, light travels about 30 cm in 1 nanosecond. Taking the errors in ρ and T into account, it would not be possible to achieve nanosecond-level accurate time transfer over a 25 km long link. It must be noted that these errors arise just from the interpolation of the meteorological parameters along the surface. As will be seen in the next section, extrapolation of the parameter values above the surface will add more error to the tropospheric delay estimate.

It is also interesting to note the seasonal variation of RMS

error in the interpolated parameter values. The uncertainty in the partial pressure of water vapor is high in summers, and comparatively lower in the dry winter season.

2) *Extrapolation along Altitude:* The timing signal does not, in general, travel along the Earth's surface. This entails extrapolation of the values of meteorological parameters upwards from the surface. A simple technique for performing this extrapolation is to use the existing climatological models that characterize the variation of the meteorological parameters of interest with altitude.

One such climatological model is used in the Saastamoinen model for tropospheric delay [16]. The Saastamoinen model is often used for estimating the zenith tropospheric delay as seen by a GNSS receiver based on the local weather conditions. This model is known to perform adeptly at high elevation angles [15], so the climatological model used in the Saastamoinen model may be used for extrapolating the weather parameters in altitude.

This climatological model assumes that temperature has a constant lapse rate, and its variation with altitude is characterized as

$$T = T_1 + \beta(r - r_1) \quad (19)$$

where T is the temperature at distance $(r - r_1)$ from the surface of the Earth, r_1 is the radius of Earth, T_1 is the temperature at the surface, and β is the lapse rate, which is typically taken to be 6.5 Kelvin per 1,000 meters [13]. This model of the vertical profile of temperature is only valid within the troposphere, beyond which the temperature remains constant within the tropopause. The height of tropopause can be determined using the monthly average of historical tropopause heights observed above a particular location over the Earth. This data is provided by the NCEP/NCAR [22]. Above the tropopause, the temperature starts to rise again. However, this region of the neutral atmosphere has not been considered in this paper as its contribution to the neutral atmospheric delay is negligible. Figure 8 shows the variation of temperature with altitude as given by the typical lapse rate. For comparison, the true vertical profile of temperature has been plotted alongside.

The pressure at altitude $(r - r_1)$ from the surface is given as

$$p = p_1(T/T_1)^{-g/(R_d\beta)} \quad (20)$$

where p_1 is the pressure at the surface, g is the local acceleration due to Earth's gravity, and R_d is the gas constant for dry air.

The amount and distribution of water vapor in the atmosphere varies greatly according to condensation. An approximate expression for variation of partial pressure of water vapor with altitude as used in the Saastamoinen model is

$$e = e_1(T/T_1)^{-4g/(R_d\beta)} \quad (21)$$

where e is the partial pressure of water vapor at altitude $(r - r_1)$, and e_1 is the partial pressure of water vapor at the surface.

The partial pressure of water vapor is not a direct measurement made by the weather stations, but it can be derived

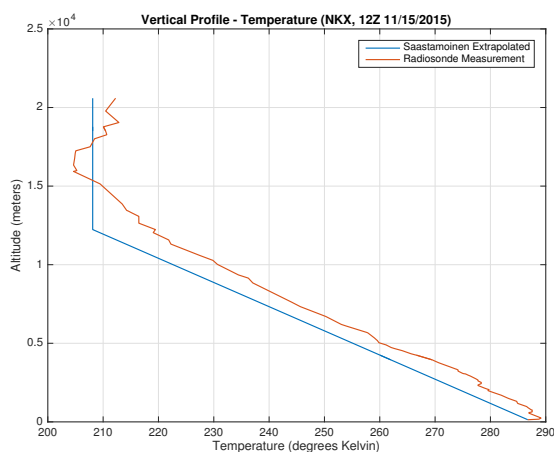


Fig. 8. Comparison of vertical profile of temperature as predicted by the climatological model and the true snapshot of profile obtained via radiosonde sounding over San Diego, CA, on 12Z 11/15/2015.

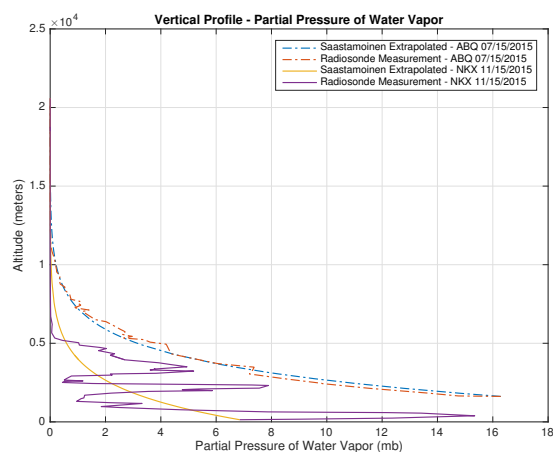


Fig. 9. Comparison of vertical profile of partial pressure of water vapor as predicted by the climatological model and the true snapshot of profile obtained via radiosonde sounding over San Diego and Albuquerque.

using the temperature and relative humidity. Also, the third parameter of interest, namely the mass density of air, can be derived at any altitude using temperature, total pressure, and partial pressure of water vapor at that altitude.

Using the above climatological model, the meteorological parameters of interest may be obtained at any altitude if the temperature, total pressure, and relative humidity are known at the surface. As has been shown already, the values of these parameters at the surface can be obtained by interpolating between the weather station locations. However, to quantify the performance of this model, it must be compared against the true value of meteorological parameters in the upper air.

The NOAA has been taking upper air observations using radiosondes since the late 1930s. A radiosonde is a miniature weather station coupled with a radio transmitter. The radiosonde is suspended from a weather balloon and goes up in the atmosphere to as high as 35,000 meters. A vertical profile of the weather parameters can be generated using the data received from the radiosonde. Although the radiosonde may take up to two hours to complete its ascent, the vertical profile generated may be viewed as a snapshot of weather conditions in upper air. The data from radiosondes is used for understanding weather phenomenon and performing weather forecasts. The soundings, however, are only done twice a day from each location. So a snapshot of the vertical profile is only available after every 12 hours.

In this paper, radiosonde data is used to study the uncertainty in the extrapolated values of meteorological parameters. To this end, two scenarios were considered: a scenario close to ocean (San Diego (NKX), CA), and another scenario in an arid region (Albuquerque (ABQ), NM). Figure 9 shows the vertical profile of partial pressure of water vapor as predicted by the climatological model as well as the true snapshot generated using the radiosonde observations. It can be seen that the climatological model as used by Saastamoinen tracks the true vertical profile very closely for the case of the dry and arid

Albuquerque scenario. However, for the more volatile scenario in San Diego, the true vertical profile of partial pressure of water vapor deviates significantly from the climatological model prediction. A consistently positive error of close to 5 mb is seen between 1,500 meters and 2,000 meters altitude. This kind of error may lead to distance-equivalent error of as high as 4 cm/km as seen from Figure 6.

Similarly, in Figure 8, a consistently positive error of 5-10 K can be seen in the comparison of vertical profile of temperature. Although the true lapse rate of temperature matches closely to the typical lapse rate considered, the extrapolated vertical profile could not follow the initial increase in temperature with altitude that might have been caused by the phenomenon of temperature inversion.

The discussion above indicates that the climatological model considered by Saastamoinen works accurately over certain regions and weather conditions, but might deviate significantly in other regions. To quantify the uncertainty in prediction by the climatological model, RMS error of the estimated values was calculated at a number of altitude points for both San Diego and Albuquerque. Using the sounding data from the same time of the day (12:00 UTC) for all days in the year 2015, monthly variations in the RMS error were also generated. These results have been plotted in Figures 10, 11, 12, and 13.

Figures 10 and 11 show the RMS error in partial pressure of water vapor estimate at different altitudes for Albuquerque and San Diego, respectively. It can be seen that the uncertainty in estimate of partial pressure of water vapor is higher in case of San Diego, possibly due to its proximity to the Pacific ocean. In arid regions like Albuquerque, the uncertainty in partial pressure of water vapor is comparatively lower. However, as the altitude increases, the partial pressure of water vapor becomes more predictable in both cases. From Figure 6 it becomes clear that the distance-equivalent error due to uncertainty in partial pressure of water vapor would

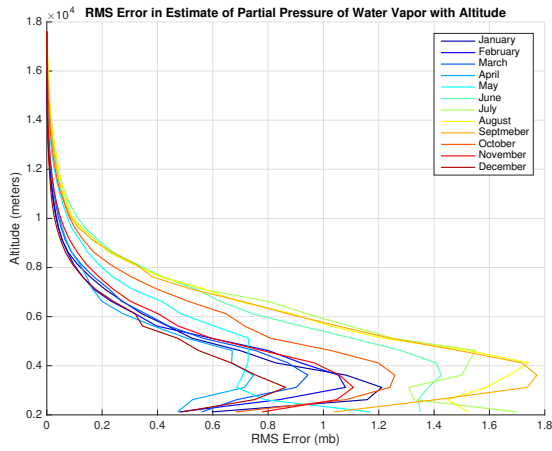


Fig. 10. RMS error in partial pressure of water vapor versus altitude for different months of the year 2015 in Albuquerque, NM.

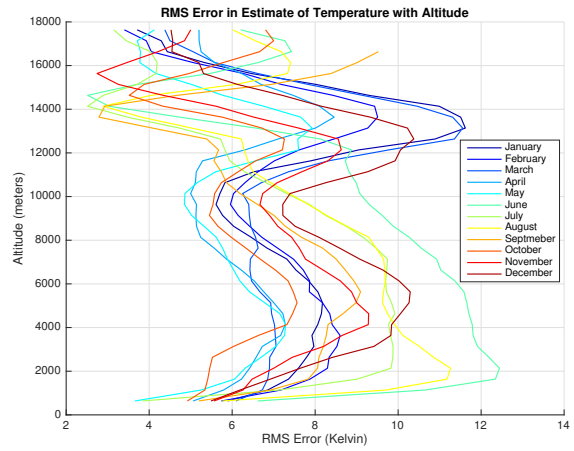


Fig. 12. RMS error in temperature versus altitude for different months of the year 2015 in San Diego, CA.

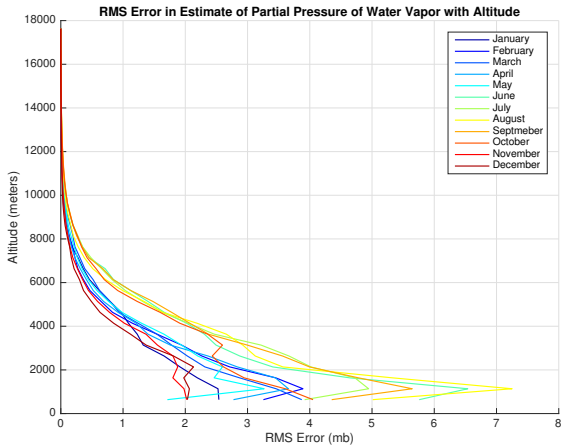


Fig. 11. RMS error in partial pressure of water vapor versus altitude for different months of the year 2015 in San Diego, CA.

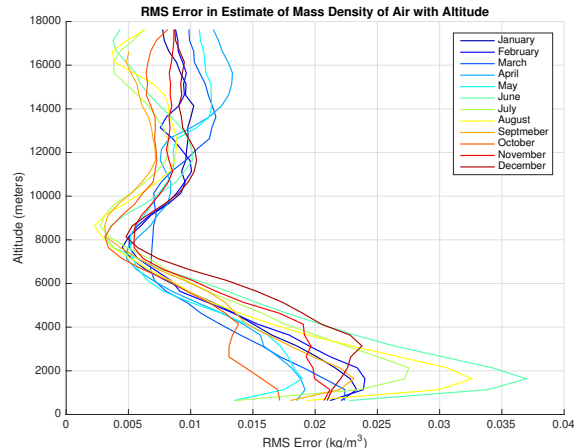


Fig. 13. RMS error in mass density of air versus altitude for different months of the year 2015 in San Diego, CA.

be negligible at altitudes above 10,000 meters. However, the large uncertainty at lower altitudes in San Diego precludes nanosecond-level accurate time transfer over long distance. Also, it is interesting to note that at both test locations, the partial pressure of water vapor deviates from the climatological model more in the summer season.

Figure 12 shows the RMS error in the estimate of temperature at different altitudes for San Diego. Similar results were obtained for Albuquerque. In light of Figure 7 it is clear that such levels of uncertainty in temperature would not be acceptable for nanosecond-level accurate time transfer at lower altitudes. However, as seen in Figure 9, the partial pressure of water vapor diminishes rapidly at high altitudes. In such a scenario, the high uncertainty in temperature would contribute a negligible distance-equivalent error.

The RMS error in estimate of mass density of air at different altitudes in San Diego is shown in Figure 13. Similar level of uncertainty was observed in Albuquerque. Once again, the

high uncertainty at low altitudes, especially in the summer season, would limit the possibility of nanosecond-accurate time transfer over long distances. Unlike temperature and partial pressure of water vapor, the uncertainty in estimate of mass density of air remains a concern at higher altitudes too.

From the discussion thus far, it can be seen that simple climatological model based estimation of weather parameters might not be adequate for highly accurate time transfer. Thus, a new method of estimating these parameters based on historical weather data is being explored. The concept driving this new method has been presented in the next sub-section.

D. Improved Approach to Estimation of Weather Parameters

The methods for estimating weather parameters described thus far only rely on a snapshot of weather data from stations. However, these weather stations provide logged historical data [21] that may be exploited to figure out trends and correlations between the values of weather parameters at different times

and locations. For example, if local historical trends are used to estimate the vertical profile of temperature instead of using the typical constant lapse rate for all regions and seasons, it might be possible to predict times of the year when temperature inversion is common, and adjust the estimates accordingly. A local data-driven approach to estimation of local weather parameters can overcome limitations of climatological models that are approximated for global application. This approach is similar in concept to the numerical weather prediction techniques. However, the goal of this technique is much simpler than that of weather forecasting, and might be computationally tractable for a receiver with limited resources.

As a first step in this approach, the spatial correlation between the parameter values at different altitudes is being studied. Generating covariance matrices using historical data and using contemporary observations from aircrafts and radiosondes, a Minimum Mean Square Error (MMSE) estimator is used to reduce the uncertainty of the estimated parameters. The initial results from this approach look promising and considerably improve the prediction skills in some cases. However, an in depth analysis of the results, and study of other trends such as temporal correlation and correlation between different weather parameters is still underway.

VI. CONCLUSIONS

All one-way wireless time transfer protocols, including GPS, were shown to be fundamentally vulnerable to man-in-the-middle replay attacks. It was concluded that only two-way time transfer can be made secure to an arbitrarily sophisticated attacker. Four necessary conditions for security of a two-way timing protocol were presented. Each of these conditions were shown to be important by devising an attack against a system that violated any one of the conditions. An example compliant system based on spread spectrum multiple access was presented in detail. The design of this system was comparatively simple and easy to implement.

It was argued that for highly accurate and secure time transfer over long distances, it is important to estimate the tropospheric delay experienced by the timing signal. The existing techniques for tropospheric delay estimation were shown to be inadequate for the purpose of nanosecond-level accurate time transfer for terrestrial systems. It was concluded that ray-tracing through the troposphere would be required for estimating this delay. To this end, it was shown that the weather parameters mass density of air, partial pressure of water vapor, and temperature need to be evaluated at each point along the path of the ray. Interpolation and extrapolation of meteorological parameter values using climatological models was implemented, and it was seen that these methods can achieve the required accuracy for links that are about 10 km or shorter.

VII. ACKNOWLEDGEMENTS

This work was supported by the Department of Energy in collaboration with Oak Ridge National Lab under the *Timing Authentication Secured by Quantum Correlations (TASQC)*

project, by the Texas Department of Transportation under the *Connected Vehicle Problems, Challenges and Major Technologies* project, by the National Science Foundation under Grant No. 1454474, and by the Data-supported Transportation Operations and Planning Center (D-STOP), a Tier 1 USDOT University Transportation Center.

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 phasor measurements for relaying and control," *IEEE Transactions on Power Delivery*, vol. 9, no. 1, pp. 442–452, 1994.
- [2] J. G. McNeff, "The global positioning system," *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 3, pp. 645–652, 2002.
- [3] D. W. Allan and M. A. Weiss, *Accurate time and frequency transfer during common-view of a GPS satellite*. Electronic Industries Association, 1980.
- [4] L. D. Shapiro, "Time synchronization from Loran-C," *IEEE Spectrum*, vol. 8, no. 5, pp. 46–55, 1968.
- [5] 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.
- [6] 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.
- [7] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, revised second ed. Lincoln, Massachusetts: Ganga-Jumana Press, 2012.
- [8] D. Kirchner, "Two-way time transfer via communication satellites," *Proceedings of the IEEE*, vol. 79, no. 7, pp. 983–990, 1991.
- [9] 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.
- [10] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, 2016, to be published.
- [11] K. D. Wesson, M. P. Rothlisberger, and T. E. Humphreys, "Practical cryptographic civil GPS signal authentication," *Navigation, Journal of the Institute of Navigation*, vol. 59, no. 3, pp. 177–193, 2012.
- [12] E. Hecht, *Optics*. Reading, Mass: Addison-Wesley, 2002.
- [13] J. L. Davis, T. A. Herring, I. I. Shapiro, A. E. E. Rogers, and G. Elgered, "Geodesy by radio interferometry: Effects of atmospheric modeling errors on estimates of baseline length," *Radio Sci.*, vol. 20, no. 6, pp. 1593–1607, 1985.
- [14] RTCA (Firm). SC-159, *GNSS-based Precision Approach Local Area Augmentation System (LAAS) Signal-in-space Interface Control Document (ICD)*. RTCA, 2005.
- [15] J. J. Wang, J. Wang, D. Sinclair, H. K. Lee *et al.*, "Tropospheric delay estimation for pseudolite positioning," *Positioning*, vol. 1, no. 09, 2005.
- [16] J. Saastamoinen, "Atmospheric correction for the troposphere and stratosphere in radio ranging of satellites," in *Geophysical Monograph 15*, S. W. Henriksen, Ed. Washington, D.C.: American Geophysical Union, 1972, pp. 247–251.
- [17] A. E. Niell, "Global mapping functions for the atmosphere delay at radio wavelengths," *Journal of Geophysical Research*, vol. 101, pp. 3227–3246, 1996.
- [18] J. Zhang and G. Lachapelle, "Precise estimation of residual tropospheric delays using a regional GPS network for real-time kinematic applications," *Journal of Geodesy*, vol. 75, no. 5-6, pp. 255–266, 2001.
- [19] J. Böhm, A. Niell, P. Tregoning, and H. Schuh, "Global mapping function (GMF): A new empirical mapping function based on numerical weather model data," *Geophysical Research Letters*, vol. 33, no. 7, 2006.
- [20] P. Mateus, G. Nico, R. Tomé, J. Catalao, and P. M. Miranda, "Experimental study on the atmospheric delay based on GPS, SAR interferometry, and numerical weather model data," *Geoscience and Remote Sensing, IEEE Transactions on*, vol. 51, no. 1, pp. 6–11, 2013.
- [21] A. Smith, N. Lott, and R. Vose, "The integrated surface database: Recent developments and partnerships," *Bulletin of the American Meteorological Society*, vol. 92, no. 6, p. 704, 2011.
- [22] Kalnay *et al.*, "The NCEP/NCAR 40-year reanalysis project," *Bull. Amer. Meteor. Soc.*, vol. 77, pp. 437–471, 1996.