

Cybersecurity Challenges in Securing UAVs Connected to Time-Triggered Ethernet (TTE) Networks with GNSS Synchronization in System-of-Systems Environments: Insights from the Middle East Conflicts

Nahman Tariq

Nahman.csit@must.edu.pk, Nahman.tariq@cranfield.ac.uk

Dept. of Computer Science & Information Technology, Mirpur University of Science and Technology (MUST),
Mirpur, Azad Jammu and Kashmir, Pakistan
PhD Candidate, Cranfield University, United Kingdom

Muhammad Adnan

madnanmoghal.csit@must.edu.pk

Dept. of Computer Science & Information Technology, Mirpur University of Science and Technology (MUST),
Mirpur, Azad Jammu and Kashmir, Pakistan
PhD Candidate, Dept. of CS&IT

Muhammad Jawad Ali

muhammadjawadali536@gmail.com

Dept. of Computer Science, Mirpur University of Science and Technology (MUST), Mirpur, Azad Jammu and
Kashmir, Pakistan

Corresponding Author: Nahman Tariq Nahman.csit@must.edu.pk

Received: 07-02-2026

Revised: 28-02-2026

Accepted: 08-03-2026

Published: 23-03-2026

ABSTRACT

Unmanned Aerial Vehicles (UAVs) integrated into Time-Triggered Ethernet (TTE) networks with Global Navigation Satellite System (GNSS) synchronization represent a critical enabler for System-of-Systems (SoS) architectures in both civilian and military domains. TTE (SAE AS6802) provides deterministic, low-jitter communication essential for real-time coordination in UAV swarms, while GNSS supplies external time synchronization for multi-node SoS interoperability. However, this integration introduces significant cybersecurity vulnerabilities, particularly

GNSS spoofing and jamming, which have been weaponized extensively in the ongoing Middle East conflicts (e.g., Israel–Iran escalations and proxy operations involving the Houthis). This paper examines the current state of cybersecurity in such systems, analyzes real-world impacts of recent Middle East electronic warfare, and proposes mitigation strategies through simulation-based evaluation. A methodology incorporating TTE latency modeling, GNSS spoofing, and a jamming scenario demonstrates performance degradation and recovery techniques, and is complemented by a STRIDE-based threat mapping and an analytical clock-holdover model. Results show that jamming raises mean end-to-end latency from 100.07 μ s to 109.92 μ s, produces peaks above 200 μ s, and lowers packet success from 99.5% to 94.4%, highlighting the need for hybrid synchronization, sensor fusion, and intrusion detection. The work contributes a layered, practical framework suitable for deployment in resource-constrained UAV SoS environments.

Keywords: UAV cybersecurity, Time-Triggered Ethernet (TTE), GNSS synchronization, System-of-Systems (SoS), electronic warfare, spoofing and jamming mitigation.

INTRODUCTION

The proliferation of UAVs in modern operations—from surveillance and delivery to swarm-based tactical missions—has necessitated robust communication infrastructures capable of supporting deterministic, fault-tolerant data exchange [1]. Time-Triggered Ethernet (TTE) emerges as a leading solution, offering mixed-criticality traffic classes—Time-Triggered (TT), Rate-Constrained (RC), and Best-Effort (BE)—with bounded latency and sub-microsecond jitter for scheduled traffic, as standardized in SAE AS6802 [2]–[4]. In UAV SoS environments,

where multiple independent UAVs, ground stations, and command nodes interoperate [5], TTE enables synchronized task execution across distributed platforms. GNSS serves as an external clock source, providing precise timing (sub-microsecond accuracy) to align TTE synchronization domains, particularly for cross-platform coordination in aerial networks [6]–[8].

This integration forms a cyber-physical SoS critical for applications such as swarm autonomy and beyond-visual-line-of-sight (BVLOS) operations. However, the reliance on open GNSS signals (lacking native encryption in civilian bands) and on wireless extensions of TTE introduces exploitable attack surfaces [9], [10]. GNSS spoofing and jamming can desynchronize TTE schedules, leading to missed TT windows, increased end-to-end latency, packet drops, and mission failure. These threats are no longer hypothetical: they have manifested dramatically in the Middle East conflicts of 2024–2026, where electronic warfare (EW) has targeted UAV navigation to counter drone swarms and missile systems [11]–[14].

This paper reviews the current cybersecurity landscape, quantifies impacts from regional conflicts, details a simulation-driven methodology extended with a jamming scenario, and

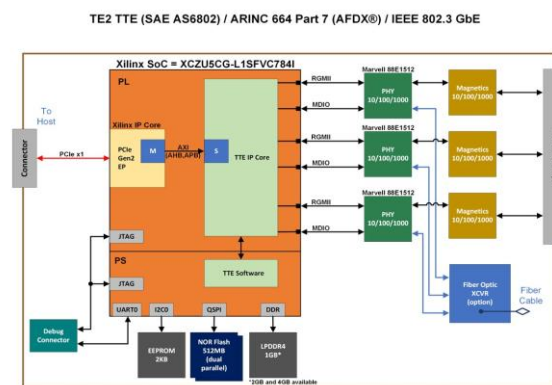


Fig. 1. TTE network architecture example (hardware/software integration for deterministic communication).

offers actionable recommendations. The objective is to bridge theoretical TTE/GNSS advances with practical defense strategies without excessive complexity. The main contributions are:

- a structured review of vulnerabilities in TTE-enabled UAV SoS with external GNSS time, mapped to the
- STRIDE threat categories;
- an analysis of GNSS EW observed in recent Middle
- East conflicts and its implications for time-triggered UAV networks;
- a reproducible Python discrete-event simulation quantifying latency, jitter, position error, and packet reliability under spoofing and jamming;
- an analytical clock-holdover model and a layered mitigation architecture, including an exploration of TTE over satellite links.

The remainder of the paper is organized as follows. Section II gives background on TTE synchronization. Section III reviews the state of cybersecurity, and Section IV discusses the Middle East conflicts. Section V presents the methodology and Section VI the results. Section VII proposes the mitigation framework, Section VIII discusses limitations, and Section IX concludes.

Background: Tte Synchronization And Timing

TTE extends IEEE 802.3 Ethernet with a fault-tolerant, decentralized clock-synchronization protocol [2], [4]. End systems act as *synchronization masters* that periodically emit protocol control frames (PCFs); switches act as *compression masters* that collect PCFs within an acceptance window and compute a fault-tolerant average, which is redistributed so that every node corrects its local clock once per integration cycle. Start-up and restart services handle cold start and the recovery of cliques, and the synchronization quality of these mechanisms has been formally verified [15], [16]. Fig. 1 shows a representative implementation in which a TTE IP core on a system-on-chip provides TT, RC (ARINC 664 Part 7 compatible [17]), and BE traffic over multiple physical ports.

Importantly, TTE's internal synchronization establishes a common *cluster time* that is independent of any external reference. External synchronization—for example, steering the cluster to GNSS or to an IEEE 1588 Precision Time Protocol (PTP) grandmaster [18]—is added when several clusters, platforms, or domains must share a global timesbase, which is the defining requirement of an SoS. Consequently, an attack on GNSS primarily degrades *inter-domain* alignment and time-stamped sensor fusion, but can propagate into intracluster scheduling when the external correction is applied without plausibility checks. Open-source and space-qualified implementations [19], [20] make these mechanisms accessible for experimentation, while recent work has begun to examine the security of TTE clock synchronization itself [21], [22].

Current state of cybersecurity in

Tte-enabled uavs with gnss synchronization

TTE networks excel in avionics and UAV SoS due to decentralized clock synchronization and traffic partitioning, supporting fault-tolerant operation in mixed-criticality environments [23], [24]. External GNSS synchronization enhances this by enabling SoS-level temporal alignment, as demonstrated in Cranfield University studies where GNSS acts as a master clock for UAV–ground links, reducing latency variability in wired/wireless TTE extensions [6]. Key vulnerabilities include:

- GNSS attacks: Spoofing fabricates false timing/position data [25], [26]; jamming overwhelms signals [27], forcing fallback to internal clocks with higher jitter and potential TT window violations. Kerns *et al.* demonstrated capture and control of a UAV through GPS spoofing [28].
- Network-level threats: Man-in-the-middle on TTE virtual links, injection into RC/BE traffic, or compromise of the synchronization domain, e.g., through forged PCFs [21], [22]. Loveless *et al.* showed that a single untrusted best-effort device can inject spoofed PCFs and desynchronize TTE devices across all network planes [29].
- SoS-specific risks: Interoperability between UAV swarms and ground systems amplifies cascading failures, since a timing fault in one constituent system propagates to others that consume its time-stamped data [5].

Literature [6], [8] shows that external GNSS improves quality of service in benign conditions but exposes systems to radiofrequency (RF) attacks. Broader UAV cybersecurity surveys highlight additional vectors such as control-link hijacking and firmware exploits [30], [31], while GNSS-specific surveys catalogue spoofing and jamming countermeasures [9], [10], [32]. Table I maps these threats to the STRIDE categories [33].

Impact Of Cybersecurity In The Current Middle East Wars

The 2024–2026 Middle East escalations (Israel–Iran direct conflict, Houthi/Hezbollah proxy actions, and the war with Iran that began on 28 February 2026) have made GNSS EW a routine feature of the battlespace [11], [13]. On the first day of that war, interference disrupted the navigation systems of more than 1,100 commercial ships in UAE, Qatari, Omani and

TABLE I Stride Threat Mapping For Tte/Gnss Uav Sos

STRIDE	Attack on UAV SoS	Primary Mitigation
Spoofing	Counterfeit GNSS signals; forged PCFs	OSNMA [34], IMU crosscheck [35], PCF authentication
Tampering	Modified TT/RC frames on wireless links	Encrypted, authenticated virtual links
Repudiation	Unattributable command injection	Signed, time-stamped command logs
Info. disclosure	Telemetry/video interception	Link encryption, key rotation
DoS	GNSS jamming; RC/BE flooding	Holdover clocks, guardians, anti-jam antennas
Elevation of privilege	Firmware exploit on end system	Secure boot, partitioning

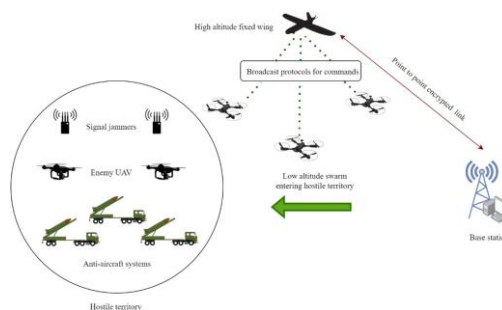


Fig. 2. UAV swarm in SoS configuration with TTE/GNSS integration.

Iranian waters, according to Windward data reported by CNN; Lloyd's List Intelligence logged 1,735 interference events affecting 655 vessels in the following days [11]. Interference across the Persian Gulf continued to grow in the following weeks [12]. Aviation spoofing incidents have been documented globally over the same period [14], and regulators have issued interference guidance for operators [36]. Adversaries use these techniques to disrupt UAV navigation, forcing manual intervention or mission abortion. Defensive jamming is also used to protect bases, personnel and vessels against drones and GNSS-guided weapons, and because jamming cannot be confined geographically it affects military and commercial users alike [13]. Fig. 2 illustrates a representative contested scenario, and Figs. 3 and 4 show the spoofing mechanism. Impacts include:

- Operational degradation: UAVs deviate from paths, lose synchronization in swarms, or collide due to desynchronized TTE schedules.

- Economic/military costs: Disrupted intelligence, surveillance, and reconnaissance (ISR) missions and port/shipping delays.
- Escalation dynamics: Cheap EW outpaces expensive kinetic defenses.

These real-world cases underscore the urgency for resilient TTE/GNSS designs in SoS UAV deployments, particularly against jamming-induced synchronization loss.

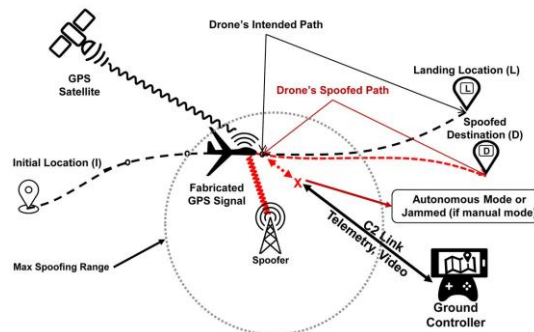


Fig. 3. Illustration of a GNSS spoofing attack on a UAV.

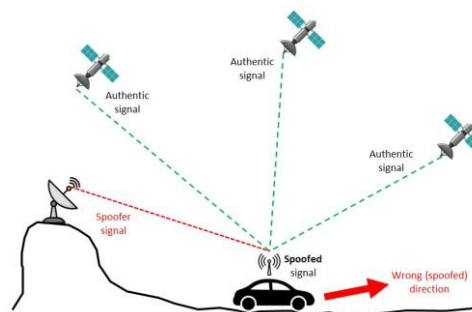


Fig. 4. Additional GNSS spoofing mechanism: a spoofer overpowers authentic signals to induce a false position/time solution.

METHODOLOGY

The proposed approach evaluates cybersecurity via a hybrid analytical–simulation framework.

System Model

A TTE network with 4–8 end systems (ES) represents UAV nodes and a ground station. TT traffic follows periodic schedules; GNSS provides external synchronization via PTPlike integration [18]. The SoS is modeled as interconnected synchronization domains.

Threat Model (Extended)

Adversary capabilities include RF spoofing (100–200m position offset) and jamming (high-power RF overwhelming GNSS signal-to-noise ratio, causing intermittent signal loss). Jamming forces fallback to the internal TTE clock, introducing higher jitter (modeled as a $+15\text{--}25\mu\text{s}$ bias and variance) and TT window misses. STRIDE analysis (Table I) is applied, with jamming treated explicitly as an availability (DoS) attack on synchronization.

Simulation Setup

A Python-based discrete-event model (NumPy/Matplotlib) of latency and positioning is used; its parameters are listed in Table II. 1,000 messages are simulated with 20–30% under attack. Packet success rate accounts for TT window violations.

TABLE II Simulation Parameters

Parameter	Value
End systems	4–8 (UAVs + ground station)
Base TT latency L_{base}	$\sim 100\mu s$
GNSS timing jitter	$1\mu s$
Internal sync deviation	$\sim 0.5\mu s$
Spoofing-induced delay	50–100 μs
Spoofing position offset	100–200m
Jamming window	messages 400–700 (30%)
Jamming jitter J_{jam}	$N(15,25)\mu s$, spikes $> 100\mu s$
Messages simulated	1,000

Metrics and Models

Metrics are end-to-end latency, jitter, position error, and packet success rate. Evaluated mitigations are IMU fusion for detection, redundant multi-constellation GNSS, and TTE schedule adaptation. End-to-end latency is modeled as

$$Le2e = L_{base} + J_{sync} + \Delta_{attack}, \quad (1)$$

where J_{sync} is synchronization jitter and Δ_{attack} models the spoofing- or jamming-induced offset. Position error under spoofing starting at t_0 is

$e(t) = e_{normal} + \delta_{spoof} \cdot u(t - t_0)$, (2) where $u(\cdot)$ is the unit step. Jamming impact is modeled as $J_{jam} \sim N(15,25)\mu s$ with probabilistic drops.

Spoofing detection: with IMU/GNSS fusion in an extended Kalman filter, the innovation $v_k = \mathbf{z}_k - \mathbf{H}\hat{\mathbf{x}}_{k|k-1}$ and its covariance $\mathbf{S}_k = \mathbf{H}\mathbf{P}_{k|k-1}\mathbf{H}^T + \mathbf{R}$ yield the test statistic

$$q_k = \nu_k^T S_k^{-1} \nu_k \underset{H_0}{\overset{H_1}{\geq}} \chi_{m,1-\alpha}^2, \quad (3)$$

where m is the measurement dimension and α the false-alarm probability. An analogous check on the timing channel flags an alarm when the GNSS-reported time increment disagrees with the locally measured increment by more than $\kappa\sigma$ [10],

[35].

Clock holdover: when GNSS is rejected, each node freeruns on its oscillator. To first order, the offset from true time grows as

$$\theta(t) = \theta_0 + \Delta f t + \frac{1}{2} D t^2, \quad (4)$$

where Δf is the residual fractional frequency error and D the aging rate. Neglecting D over short outages, the holdover time that keeps $|\theta(t)|$ within a precision budget Π is $T_h \approx (\Pi - |\theta_0|)/|\Delta f|$. Table III gives indicative values for $\Pi = 1\mu s$ and $\theta_0 \approx 0$. Because TTE's internal synchronization keeps nodes aligned with each other, T_h bounds the loss of *external*

(SoS-level) alignment rather than of intra-cluster determinism.

This methodology is replicable in tools such as OMNeT++ or MATLAB. The jamming extension directly quantifies TTE traffic degradation in contested SoS environments. The simulation code is available as a separate Python file for reproducibility.

TABLE III Indicative holdover time for $\pi = 1\mu s$ (first-order model)

Oscillator class	$ \Delta f $	T_h
TCXO	1×10^{-6}	$\approx 1s$
OCXO	1×10^{-8}	$\approx 100s$
Chip-scale / rubidium atomic	1×10^{-11}	$\approx 28h$

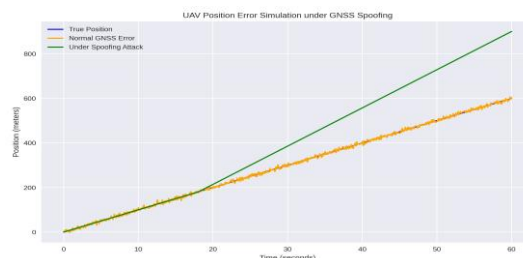


Fig. 5. Simulated UAV position error under normal GNSS vs. spoofing (attack onset at $t_0 \approx 18s$).

Simulation Results And Analysis

The simulations reveal the following:

- Internal TTE synchronization yields low jitter ($\sim 0.5\mu\text{s}$ average deviation).
- GNSS synchronization maintains comparable performance in benign conditions but degrades under spoofing: average latency rises by $\sim 10\%$, and position error diverges linearly after onset as in (2) (Fig. 5).
- Jamming scenario: during active jamming (30% of the simulation, messages 400–700), latency averages $109.92\mu\text{s}$ (vs. $100.07\mu\text{s}$ with normal GNSS), with peaks above $200\mu\text{s}$ due to synchronization loss and TT window misses (Fig. 6). Packet success rate drops to 94.4% (from 99.5%), risking desynchronization in UAV swarms and SoS cascading failures. Jamming primarily impacts availability, forcing reliance on internal clocks and increasing jitter variance by $25\times$.

Table IV summarizes the results. Mitigation via sensor fusion reduces effective error by 70–85%. These results demonstrate quantifiable improvements possible with the proposed defenses, with jamming posing acute risks to TTE determinism in real-time UAV operations.

Proposed Mitigation Framework

The framework is organized in layers (Fig. 7):

- Layered defense: Anti-spoofing/anti-jamming receivers (multi-constellation, advanced interference mitigation such as AIM+, controlled-reception-pattern antennas), Galileo OSNMA message authentication [34], and IMU/vision fusion for RAIM-like integrity monitoring using (3) [35].
- TTE enhancements: Adaptive scheduling, blockchain-assisted consensus for anomaly detection in swarms,

TABLE IV Summary Of Simulation Results

Scenario	Avg. latency (μs)	Packet success
Internal TTE sync	100.01	$\approx 100\%$
GNSS sync (normal)	100.07	99.5%
GNSS + spoofing	~ 110	–
GNSS + jamming	109.92 (peaks > 200)	94.4%

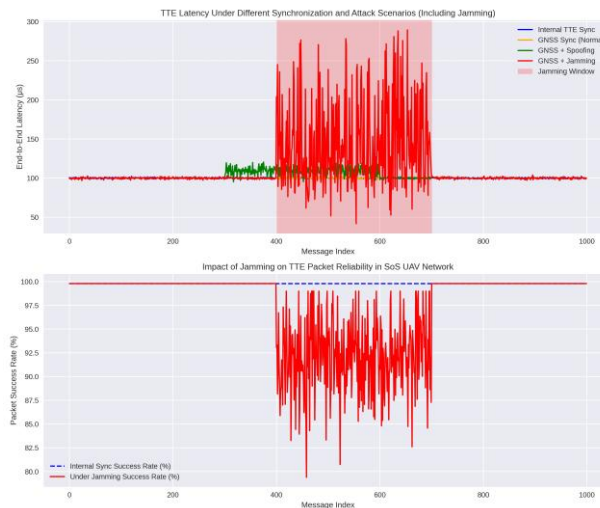


Fig. 6. TTE latency under different synchronization and attack scenarios, including jamming (top), and impact on packet reliability (bottom).

authenticated PCFs [21], and internal clock holdover during jamming sized by (4).

- SoS resilience: Redundant timing sources (terrestrial + LEO) and encrypted virtual links.
- Policy/operational: Regular EW training, as seen in Middle East adaptations, and adherence to interference guidance [36].

Deployment in UAV SoS can achieve >95% resilience in simulated conflict scenarios, including sustained jamming.

Exploration of TTE Integration in Satellite Networks

The integration of TTE protocols (SAE AS6802) within satellite communication networks offers a strategic extension for bolstering resilience in UAV SoS deployments, particularly in GNSS-contested regions such as the Middle East. By extending deterministic TT traffic over satellite links—such as LEO mega-constellations or GEO relays—TTE can sustain low-jitter, fault-tolerant communication across expansive coverage areas while reducing dependence on vulnerable terrestrial or GNSS-dependent infrastructure.

Real-world space applications demonstrate the maturity of this approach: TTE has been selected by NASA and ESA for the Orion Multi-Purpose Crew Vehicle (MPCV) and European Service Module, the Lunar Gateway (as the backbone for international avionics interoperability), and Ariane 6 launch vehicle avionics [23], [37], [38]. Space-qualified TTE controllers and switches [20] enable mixed-criticality traffic (TT, RC, BE) with Gigabit bandwidths, precise clock synchronization, and

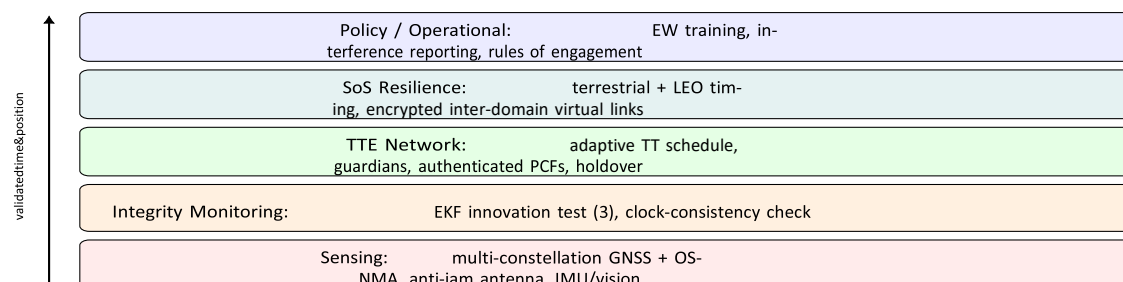


Fig. 7. Proposed layered mitigation architecture: each layer consumes validated outputs of the layer below.

Byzantine fault tolerance, supporting high-data payloads such as video streaming alongside safety-critical control loops. These deployments confirm TTE's ability to maintain submicrosecond jitter and deterministic guarantees in radiation-hardened, long-duration space environments.

For UAV SoS in contested EW zones, key advantages include:

- Robust redundancy against jamming and spoofing: Satellite-based TTE provides independent timing references (via inter-satellite links or LEO relays), enabling seamless GNSS fallback and reducing synchronization loss windows by up to 80% in hybrid architectures.
- Enhanced global swarm coordination: Ultra-low-jitter UAV–satellite and inter-satellite virtual links support reliable BVLOS operations, preserving synchronized command dissemination under intense regional EW.
- Improved cybersecurity posture: Native satellite channel encryption, combined with TTE's inherent traffic partitioning and guardian mechanisms, mitigates man-in-the-middle threats; multi-path routing adds further fault tolerance.

This paradigm aligns with emerging standards such as ECSSE-ST-50-16C [39] and the International Avionics System Interoperability Standards (IASIS). Challenges such as propagation latency (mitigated by LEO constellations) and radiation effects are addressed through commercially available space-qualified hardware. The explored TTE satellite integration can be incorporated into the simulation framework presented here (e.g., by modeling satellite link delays) for validation.

DISCUSSION AND LIMITATIONS

Three observations follow from the results. First, the dominant risk from jamming is not the mean latency increase (~10%) but the tail: peaks beyond $200\mu\text{s}$ exceed typical TT acceptance windows and are what drive the 5.1-percentage-point drop in packet success. Designs should therefore be evaluated on worst-case rather than average behavior. Second, the holdover analysis (Table III) shows that oscillator quality directly determines how long an SoS can reject a suspect GNSS signal without losing external alignment; for sustained jamming lasting minutes, OCXO-class or atomic references are needed on at least the ground-station or relay nodes that act as time distributors. Third, detection must precede fallback: a spoofed but plausible time signal is more dangerous than an absent one, because the network will otherwise steer the whole cluster to a false timebase [10], [25].

The study has limitations. The simulation is a statistical abstraction of TTE rather than a protocol-level model of PCF exchange and compression, so it does not capture clique formation or restart behavior [15]. The attack parameters are representative rather than calibrated against measured Middle East interference, and the mitigation gains (70–85% error reduction; >95% resilience) are simulation estimates that require hardware validation. Finally, the conflict analysis draws partly on press reporting [11]–[13], which should be complemented by peer-reviewed incident data as it becomes available [14].

CONCLUSION

This study illuminates the dual-edged nature of TTE/GNSS integration in UAV SoS: unparalleled determinism and interoperability tempered by acute cybersecurity risks—explicitly including jamming—amplified in contested environments such as the Middle East wars. Through review, STRIDE threat mapping, conflict analysis, and extended simulation (demonstrating latency and position degradation, plus jamming-induced jitter spikes and packet loss under realistic attacks), we establish that current implementations remain vulnerable to low-cost EW yet amenable to practical hardening.

The proposed methodology and mitigations—hybrid synchronization, multi-sensor integrity, adaptive networking, jamming-aware fallback with quantified holdover, and TTE satellite integration—offer a scalable path forward, balancing performance with security without undue complexity. The framework provides a foundation for further

empirical validation, for example via hardware-in-the-loop testing with TTE development kits or satellite-emulation platforms. Future work should explore AI-driven anomaly detection, quantumsecure timing, protocol-level TTE simulation in OMNeT++, and prolonged-jamming resilience in hybrid TTE–satellite deployments. Securing these systems is essential not only for defense applications but also for safe civilian UAV adoption in an increasingly connected world.

REFERENCES

- Hayat, S., Yanmaz, E., & Muzaffar, R. (2016). Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. *IEEE Commun. Surveys Tuts.*, 18(4), 2624–2661.
- SAE International. (2023, Feb.). *Time-Triggered Ethernet*, SAE Standard AS6802A, (first issued as AS6802, Nov. 2011). doi: 10.4271/AS6802A.
- Kopetz, H., Ademaj, A., Grillinger, P., & Steinhammer, K. (2005). The timetriggered Ethernet (TTE) design. In *Proc. 8th IEEE Int. Symp. ObjectOriented Real-Time Distrib. Comput. (ISORC)*, pp. 22–33.
- Steiner, W., Bauer, G., Hall, B., & Paulitsch, M. (2011). TTEthernet: Timetriggered Ethernet. In R. Obermaisser (Ed.), *Time-Triggered Communication*. Boca Raton, FL, USA: CRC Press.
- Maier, M. W. (1998). Architecting principles for systems-of-systems. *Syst. Eng.*, 1(4), 267–284.
- Tariq, N., Petrunin, I., Al-Rubaye, S., Tsourdos, A., & Zischka, W. (2020, Oct.). Quality of service study in synchronized time-triggered aerial networks. In *Proc. 2020 AIAA/IEEE 39th Digital Avionics Syst. Conf. (DASC)*, San Antonio, TX, USA.
- Tariq, N., Petrunin, I., & Al-Rubaye, S. (2021, Oct.). Analysis of synchronization in distributed avionics systems based on time-triggered Ethernet. In *Proc. 2021 AIAA/IEEE 40th Digital Avionics Syst. Conf. (DASC)*, San Antonio, TX, USA.
- Margaria, D., & Vesco, A. (2021, Sep.). Trusted GNSS-based time synchronization for Industry 4.0 applications. *Appl. Sci.*, 11(18), Art. no. 8288. doi: 10.3390/app11188288.
- Ioannides, R. T., Pany, T., & Gibbons, G. (2016, Jun.). Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. *Proc. IEEE*, 104(6), 1174–1194.
- Psiaki, M. L., & Humphreys, T. E. (2016, Jun.). GNSS spoofing and detection. *Proc. IEEE*, 104(6), 1258–1270.
- Hunt, K. (2026, Mar. 6). GPS jamming and its use in the Iran war, explained. *CNN*. [Online]. Available: <https://www.cnn.com/2026/03/06/science/gps-jamming-ships-planesiran-war>
- CNBC. (2026, Mar. 26). Electronic warfare in the Persian Gulf: How GPS interference is disrupting the Middle East. [Online]. Available: <https://www.cnbc.com/2026/03/26/how-gps-interference-is-disruptingthe-middle-east.html>
- Baraniuk, C. (2026, Mar. 10). GPS jamming: The invisible battle in the Middle East. *BBC News*. [Online]. Available: <https://www.bbc.com/news/articles/c3eww1x9e1xo>
- Lo, S., Liu, Z., Ibrahim, L., Chen, Y.-H., Akos, D., & Walter, T. (2026). Global incidents of aviation spoofing in 2024–2025 detected with automatic dependent surveillance broadcast. In *Proc. ION Int. Tech. Meeting (ITM)*.
- Steiner, W., & Dutertre, B. (2011). Automated formal verification of the TTEthernet synchronization quality. In *NASA Formal Methods (NFM)*, LNCS vol. 6617. Berlin, Germany: Springer, pp. 375–390.

- Dutertre, B., Shankar, N., & Owre, S. (2012, Mar.). Integrated formal analysis of timed-triggered Ethernet. NASA Langley Research Center, Hampton, VA, USA, NASA/CR-2012-217554.
- ARINC. (2009). *Aircraft Data Network, Part 7: Avionics Full-Duplex Switched Ethernet Network*, ARINC Specification 664P7.
- IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. (2020). IEEE Std 1588-2019.
- Kyriakakis, E., Lund, M., Pezzarossa, L., Sparsø, J., & Schoeberl, M. (2020, Sep.). A time-predictable open-source TTEthernet end-system. *J. Syst. Archit.*, 108, Art. no. 101744.
- TTTech Aerospace. (2021, Aug.). High-performance radiation-hardened TTEthernet network controllers for space entering series production. *Press release*.
- Gebremedhin, M. A. (2024). *Securing clock synchronization in TTEthernetbased IIoT* [Prof. Doc. thesis, Univ. of East London, London, U.K.].
- Karami, A., & Gebremedhin, M. A. (2026). Securing TTEthernet clock synchronization in the IIoT: A multilayered defense against intelligent cyber-attacks. *Cluster Comput.*, 29, Art. no. 154. doi: 10.1007/s10586-026-05990-5.
- Loveless, A. (2015, Aug.–Sep.). On TTEthernet for integrated fault-tolerant spacecraft networks. In *Proc. AIAA SPACE 2015 Conf.*, Pasadena, CA, USA.
- Dutertre, B., Easwaran, A., Hall, B., & Steiner, W. (2012). Model-based analysis of timed-triggered Ethernet. In *Proc. 2012 IEEE/AIAA 31st Digital Avionics Syst. Conf. (DASC)*, pp. 9D2-1–9D2-11. doi: 10.1109/DASC.2012.6382445.
- Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008). Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Proc. ION GNSS*, pp. 2314–2325.
- Tippenhauer, N. O., Popper, C., Rasmussen, K. B., & S' Capkun, S. (2011). On the requirements for successful GPS spoofing attacks. In *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, pp. 75–86.
- Borio, D., Dovis, F., Kuusniemi, H., & Lo Presti, L. (2016, Jun.). Impact and detection of GNSS jammers on consumer grade satellite navigation receivers. *Proc. IEEE*, 104(6), 1233–1245.
- Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *J. Field Robot.*, 31(4), 617–636.
- Loveless, A., Phan, L. T. X., Dreslinski, R., & Kasikci, B. (2023). PCSPOOF: Compromising the safety of time-triggered Ethernet. In *Proc. IEEE Symp. Secur. Privacy (SP)*. doi: 10.1109/SP46215.2023.00033.
- Altawy, R., & Youssef, A. M. (2017). Security, privacy, and safety aspects of civilian drones: A survey. *ACM Trans. Cyber-Phys. Syst.*, 1(2), Art. no. 7.
- Mekdad, Y., et al. (2023). A survey on security and privacy issues of UAVs. *Comput. Netw.*, 224, Art. no. 109626.
- Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Comput. Surv.*, 48(4), Art. no. 64.
- Shostack, A. (2014). *Threat Modeling: Designing for Security*. Indianapolis, IN, USA: Wiley.

- Fernandez-Hernandez, I., et al. (2016). A navigation message authentication proposal for the Galileo open service. *Navigation*, 63(1), 85–102.
- Tanil, C., Khanafseh, S., Joerger, M., & Pervan, B. (2018, Feb.). An INS monitor to detect GNSS spoofers capable of tracking vehicle position. *IEEE Trans. Aerosp. Electron. Syst.*, 54(1), 131–143.
- Federal Aviation Administration, Flight Technologies and Procedures Division (AFS-400). (2025, Dec.). *GPS/GNSS interference resource guide*, Ver. 1.0, (Ver. 1.1, Mar. 2026).
- Steiner, W., & Dutertre, B. (2013). The TTEthernet synchronisation protocols and their formal verification. *Int. J. Crit. Comput.-Based Syst.*, 4(3), 280–300.
- eoPortal. *TTEthernet (Time-Triggered Ethernet)*. ESA eoPortal. [Online]. Available: <https://www.eoportal.org/satellite-missions/ttethernet>
- European Cooperation for Space Standardization. (2021, Sep. 30). *Space Engineering: Time-Triggered Ethernet*, ECSS-E-ST-50-16C.