REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 01/05/2024 Revised:03/06/2024 Accepted: 01/07/2024

A STUDY ON TIME SYNCHRONIZATION TECHNIQUES IN WIRELESS SENSOR NETWORKS

Mrs. Zalak Bijalkumar Modi

Lecturer, EC Department, Government Polytechnic Gandhinagar, zpmodi@gmail.com

ABSTRACT
Time synchronization is a critical component in wireless sensor networks (WSNs) for ensuring accurate event detection, coordinated sensing, and efficient data aggregation. This study provides a comprehensive review of time synchronization techniques, including master-slave, peer-to-peer, sender-receiver, and receiver-receiver approaches. It also examines clock drift and offset estimation methods, energy-efficient protocols, and secure, attack-resilient schemes. Performance metrics such as synchronization error, energy consumption, and scalability are analyzed to compare different protocols. The findings highlight trade-offs between accuracy, energy efficiency, and robustness, providing insights for designing effective time synchronization solutions in resource-constrained WSN environments.

KEYWORDS
Wireless Sensor Networks (WSNs), Time Synchronization, Clock Drift and Offset, Energy-Efficient Protocols, Secure Synchronization

1. FUNDAMENTALS OF TIME SYNCHRONIZATION IN WSNS

In wireless sensor networks (WSNs), time synchronization is the backbone of efficient network operation. Many critical tasks, such as data aggregation, event detection, energy-efficient scheduling, and coordinated sensing, rely on all nodes sharing a consistent notion of time (Huan et al., 2022; Phan et al., 2019). Unlike conventional networks, WSN nodes are highly resource-constrained: they have limited battery life, low processing power, and restricted communication bandwidth. These constraints make designing energy-efficient, accurate synchronization protocols both challenging and essential (Sarvghadi & Wan, 2016).

At its core, time synchronization is about aligning the clocks of different nodes in the network. Each node in a WSN has its own local clock, Ci(t), which drifts over time due to oscillator imperfections. The goal is to estimate the clock offset θij between two nodes i and j and adjust local clocks accordingly. Mathematically, this can be expressed as:

$\Theta ij = Cj(t) - Ci(t)$ (1)

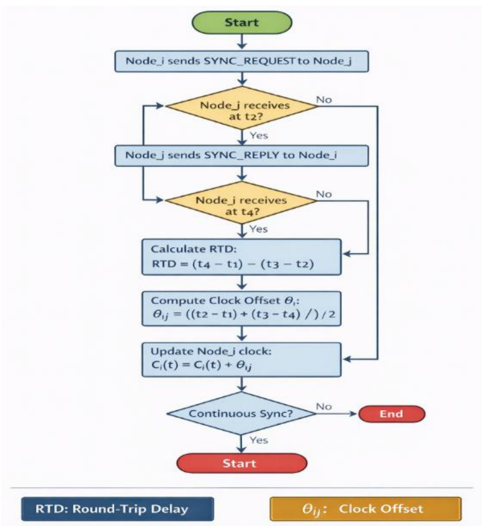


Figure 1: Two-way time sync protocol flowchart
Source: Own creation using Ms. PowerPoint

where Ci(t) is the clock reading at node iii at real time t, and Cj(t) is the clock at node j. Correctly estimating θij ensures that events observed by different nodes can be accurately time-stamped and coordinated.

Several strategies have been proposed to achieve synchronization in WSNs. Traditional two-way message exchange protocols periodically send timestamps between nodes to calculate offsets and adjust local clocks (Kim et al., 2017). To reduce energy consumption in multi-hop networks, beaconless asymmetric protocols allow selective clock updates rather than continuous communication, thereby extending network lifetime (Huan et al., 2020). Huan et al. (2021) enhanced

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 01/05/2024 Revised:03/06/2024 Accepted: 01/07/2024

multi-hop synchronization by introducing packet-relaying gateways with per-hop delay compensation, which minimizes the cumulative error as messages propagate through the network.
Modern approaches go even further. The timestamp-free reverse asymmetric framework avoids explicit timestamp exchanges entirely, reducing communication overhead while maintaining microsecond-level synchronization accuracy (Huan et al., 2022). Security is also a growing concern: blockchain-based secure synchronization schemes have been proposed to prevent malicious nodes from disrupting the network's global time (Fan et al., 2018).
In essence, the fundamentals of WSN time synchronization focus on accurately estimating clock offsets, compensating for drift, minimizing energy usage, and maintaining robustness across multi-hop and potentially adversarial environments. The choice of protocol depends on network size, topology, desired accuracy, and energy constraints, making synchronization a critical design decision in WSN deployments (Phan et al., 2019; Sarvghadi & Wan, 2016).

1.1 AIM
The aim of this study is to analyze and evaluate various time synchronization techniques in wireless sensor networks (WSNs) to identify protocols that provide accurate, energy-efficient, and secure synchronization suitable for multi-hop and resource-constrained environments.

1.2 OBJECTIVES
1. To review and classify time synchronization protocols in WSNs.
2. To analyze clock drift and offset estimation methods.
3. To evaluate energy-efficient synchronization techniques.
4. To examine secure and attack-resilient synchronization methods.
5. To compare protocols based on accuracy, energy use, and scalability.

2. REVIEW OF LITERATURE
Akhlaq, M., & Sheltami, T. R. (2012) introduced a recursive time synchronization protocol. The goal was to achieve global clock alignment efficiently, and results confirmed both low energy consumption and high synchronization accuracy. **Akhlaq, M., & Sheltami, T. R. (2013)** proposed RTSP for accurate and energy-efficient clock synchronization. The study aimed at multi-hop WSNs and showed improved energy efficiency and accuracy compared to existing protocols.
Elson, J., & Römer, K. (2002) highlighted WSNs as a new regime for synchronization. The study reviewed protocols and suggested reference broadcast approaches for practical deployment. **Elson, J., Girod, L., & Estrin, D. (2002)** introduced fine-grained network synchronization using reference broadcasts. The study aimed for high-precision multi-hop WSN synchronization, achieving microsecond-level accuracy.
Fan, K., Ren, Y., Yan, Z., Wang, S., Li, H., & Yang, Y. (2018) developed a secure IoT synchronization scheme using blockchain to prevent malicious disruptions. The study showed that it effectively minimized security risks while remaining efficient and adaptable. **Ganeriwal, S., Čapkun, S., Han, C.-C., & Srivastava, M. B. (2005)** introduced a secure time synchronization service. The study aimed at WSN security, showing protection against time-based attacks while maintaining accuracy.
Ganeriwal, S., Pöpper, C., Čapkun, S., & Srivastava, M. B. (2008) developed a secure synchronization protocol. The objective was to protect against attacks, and results showed high accuracy while maintaining security. **Huan, X., He, H., Wang, T., Wu, Q., & Hu, H. (2022)** proposed a timestamp-free time synchronization scheme for resource-constrained WSNs, aiming to reduce energy use while maintaining microsecond-level accuracy. The study focused on practical multi-hop networks and demonstrated high energy efficiency without sacrificing precision.
Huan, X., Kim, K. S., Lee, S., Lim, E. G., & Marshall, A. (2020) introduced a beaconless asymmetric scheme for energy-efficient multi-hop WSN synchronization. The study targeted resource-limited nodes and found that it reduced energy use by up to 95% while maintaining microsecond-level accuracy. Huan, **X., Kim, K. S., Lee, S., Lim, E. G., & Marshall, A. (2021)** improved multi-hop synchronization using packet-relaying gateways with per-hop delay compensation. The objective was to minimize cumulative errors, and results showed enhanced accuracy and energy efficiency over conventional multi-hop approaches.
Kim, K. S., Lee, S., & Lim, E. G. (2017) proposed energy-efficient synchronization using asynchronous source clock recovery and reverse two-way messaging. The method saved energy without reducing accuracy, suitable for battery-limited WSNs. **Lenzen, C., Sommer, P., & Wattenhofer, R. (2015)** presented PulseSync, a scalable clock synchronization protocol. The objective was efficient large-network synchronization, showing low latency and high accuracy even in extensive multi-hop networks.
Manzo, M., Roosta, T., & Sastry, S. (2005) analyzed time synchronization attacks. The objective was to identify vulnerabilities in WSNs, demonstrating possible attack vectors and mitigation strategies. **Maróti, M., Kusy, B., Simon, G., & Lédeczi, Á. (2004)** developed the Flooding Time Synchronization Protocol (FTSP). The aim was reliable multi-hop synchronization, showing high accuracy and robustness in dynamic networks.
Phan, L.-A., Kim, T., Kim, T., Lee, J.-S., & Ham, J.-H. (2019) analyzed time synchronization protocols to identify efficient approaches in accuracy, energy, and computation. Their results highlighted that adaptive multi-hop protocols

outperform static or single-hop methods. **Prakash, R., & Nygard, K. (2010)** surveyed time synchronization techniques. The study aimed to review and classify protocols, highlighting their applications, strengths, and limitations in WSNs.
Ranganathan, P., & Nygard, K. (2010) presented a survey on WSN synchronization. The study aimed to summarize techniques and challenges, highlighting energy efficiency, scalability, and accuracy as key considerations. **Ren, F., Lin, C., & Liu, F. (2008)** proposed Self-Correcting Time Synchronization (SCTS) using reference broadcasts. The study aimed to minimize communication overhead and drift, achieving low complexity and high accuracy.
Robles, R. S., Borkar, V. S., & Kumar, P. R. (2007) proposed a distributed multi-hop synchronization protocol. The aim was accurate synchronization across multi-hop networks, and results demonstrated improved offset reduction. **Römer, K. (2001)** surveyed time synchronization in ad hoc networks. The objective was to identify key challenges and methods, demonstrating issues with offsets, delays, and multi-hop propagation.
Sarvghadi, M. A., & Wan, T.-C. (2016) surveyed message-passing-based synchronization methods. The study aimed to compare different protocols and concluded that multi-hop message passing offers a scalable and efficient approach. **Schenato, L., & Gamba, G. (2008)** presented a distributed consensus protocol for clock synchronization. The study aimed to reduce offsets in WSNs and showed convergence to accurate global time using consensus mechanisms.
Sichitiu, M. L., & Veerarittiphan, C. (2003) developed simple and accurate synchronization methods. The aim was practical WSN deployment, demonstrating reliable time alignment with minimal complexity. **Simon, G., Maróti, M., Lédeczi, Á., & Balogh, G. (2004)** applied WSNs for a countersniper system. The study used synchronization to coordinate nodes, demonstrating successful real-time tracking and detection.
Sommer, P., & Wattenhofer, R. (2009) proposed gradient clock synchronization. The objective was scalable and precise synchronization in WSNs, demonstrating low error propagation over multi-hop networks. **Song, H., Zhu, S., & Cao, G. (2007)** developed an attack-resilient synchronization protocol. The objective was secure and robust WSN synchronization, showing resilience to malicious time attacks.
Su, P. (2003) introduced Delay Measurement Time Synchronization. The aim was to reduce time offsets in WSNs, though the study remained as an unpublished exploration. **van Greunen, J., & Rabaey, J. M. (2003)** proposed lightweight synchronization for WSNs. The study focused on low-power nodes, achieving simple and low-overhead synchronization. **Yıldırım, K. S., & Gürcan, Ö. (2014)** developed an adaptive value tracking scheme. The aim was dynamic synchronization in multi-hop WSNs, achieving high precision while minimizing energy use. **Yildirim, K. S., & Kantarci, A. (2014)** proposed slow-flooding-based time synchronization. The study targeted energy efficiency and multi-hop networks, demonstrating improved accuracy with lower message overhead.

2.1 RESEARCH GAP

Despite numerous advancements in time synchronization for wireless sensor networks, several gaps remain. Most existing protocols either focus on high accuracy or low energy consumption, rarely achieving an optimal balance for large-scale, multi-hop networks. Security-aware protocols exist, but many introduce additional communication overhead or complexity, limiting their applicability in resource-constrained nodes. Moreover, real-time adaptive schemes that account for dynamic network conditions, varying node densities, and unpredictable delays are still limited. Few studies comprehensively integrate energy efficiency, security, and multi-hop scalability in a single framework, highlighting a need for protocols that are simultaneously accurate, lightweight, robust, and resilient to attacks.

3. CLASSIFICATION OF TIME SYNCHRONIZATION TECHNIQUES

Time synchronization is a critical requirement in wireless sensor networks (WSNs) to ensure accurate event detection, data fusion, and coordinated operation of sensor nodes. The techniques used to synchronize clocks in WSNs can be classified based on the synchronization approach, message exchange methods, and trade-offs between energy efficiency and accuracy.
In **master-slave synchronization**, one node (the master) acts as the reference clock while other nodes (slaves) adjust their clocks to match the master. The clock offset for a slave node can be expressed mathematically as:

$$Ci(t) = Cm(t) + \theta \quad (2)$$

where Ci(t) is the slave node clock at time t, Cm(t) is the master clock, and θi is the offset for node i. PulseSync (Lenzen, Sommer, & Wattenhofer, 2015) is an example of this approach, using synchronization pulses to propagate clock updates efficiently across multi-hop networks.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 01/05/2024 Revised:03/06/2024 Accepted: 01/07/2024

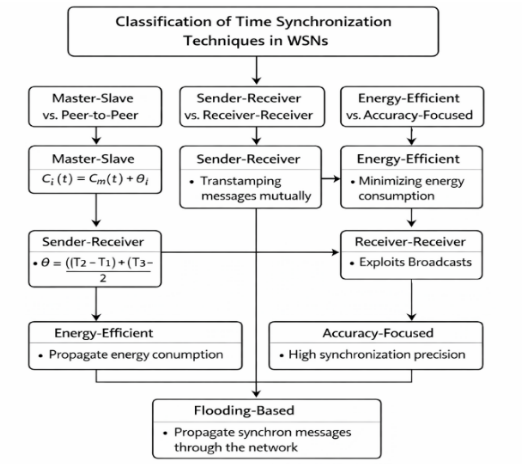


Figure 2: Classification of Time Synchronization Techniques in WSNs
Source: Self-Created in Ms. Word

In **peer-to-peer synchronization**, nodes exchange timing information mutually, updating clocks based on neighboring nodes to achieve consensus. This method improves robustness and avoids a single point of failure.
Sender-receiver protocols timestamp messages at the sender and receiver ends, estimating clock offsets using the formula:

$$\theta = \frac{(T2-T1)+(T3-T4)}{2} \qquad (3)$$

where T1 and T4 are transmission and reception times at the sender and receiver, respectively, and T2 and T3 are the corresponding reception and transmission times at the receiver. Slow-flooding synchronization (Yildirim & Kantarci, 2014) reduces message overhead by controlling flooding rates.

Receiver-receiver methods, like adaptive value tracking (Yıldırım & Gürcan, 2014), synchronize nodes that simultaneously receive the same broadcast message, minimizing delay uncertainties due to the sender.
Protocols such as **RTSP** (Akhlaq & Sheltami, 2013) and the recursive time synchronization protocol (Akhlaq & Sheltami, 2012) focus on energy efficiency by reducing message transmissions while maintaining acceptable synchronization accuracy. Energy-efficient schemes often use adaptive update intervals and asymmetric communication.
Flooding-based protocols propagate synchronization messages through the network, either slowly or using optimized flooding. Pulse-based methods, like PulseSync, generate periodic synchronization pulses from a master node, propagating quickly across multi-hop networks with high precision and minimal communication overhead.
The choice of a time synchronization technique depends on the network topology, resource constraints, and application requirements. Master-slave methods provide a clear reference but may fail if the master node goes offline, while peer-to-peer approaches enhance robustness. Sender-receiver methods are simple but sensitive to delays, whereas receiver-receiver methods exploit broadcasts to reduce uncertainties. Energy-efficient designs balance synchronization accuracy with network lifetime, and flooding or pulse-based schemes optimize message propagation across the network.

4. CLOCK DRIFT AND OFFSET ESTIMATION

Accurate time synchronization in wireless sensor networks (WSNs) depends on precise estimation of both clock offset and clock drift between nodes. The clock offset represents the difference in time between a node's local clock and a reference clock, while the clock drift refers to the rate at which a node's clock diverges from the reference clock over time (Prakash & Nygard, 2010; Ren, Lin, & Liu, 2008).
One widely used approach is the linear regression-based estimation, which models the local clock Ci(t) of node iii as a linear function of the reference clock time t:

$$Ci(t) = a \cdot t + b \qquad (4)$$

Here, a represents the clock drift factor, and b represents the clock offset. By collecting multiple timestamp pairs (t,Ci(t)), the parameters a and b can be estimated using linear regression. This method provides robust drift and offset estimates, particularly in networks with variable delays (Sommer & Wattenhofer, 2009; Schenato & Gamba, 2008).
To dynamically refine the offset estimation in real-time, the Exponentially Weighted Moving Average (EWMA) method can be applied:

$$\Theta new = \alpha \cdot \theta measured + (1-\alpha) \cdot \theta old \qquad (5)$$

In this equation, θnew is the updated offset, θmeasured is the current measured offset from timestamp exchanges, θold is the previous estimate, and α\alphaα is a smoothing factor between 0 and 1. EWMA helps to filter out temporary

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 01/05/2024 Revised:03/06/2024 Accepted: 01/07/2024

fluctuations and network jitter, improving the stability of synchronization (Ganeriwal, Pöpper, Čapkun, & Srivastava, 2008).
By combining linear regression for drift estimation with EWMA for offset correction, WSNs can achieve highly accurate and stable time synchronization, which is critical for applications such as coordinated sensing, event detection, and data fusion.

Table 1: Techniques and Models for Clock Drift and Offset Estimation in Wireless Sensor Networks

Concept	**Explanation**	**Practical Use**
Clock Skew (α)	Rate at which a node clock differs from reference	Helps in correcting cumulative timing errors over time
Clock Offset (θ)	Instantaneous difference between node and reference clock	Initial adjustment for synchronization
Linear Drift Model	Models node clock as linear function of time	Used in predictive synchronization methods
Least Squares Estimation	Estimates drift and offset from multiple timestamps	Accurate estimation in multi-hop networks
Exponential Weighted Moving Average (EWMA)	Smooths offset corrections over time	Reduces sudden jumps and network jitter
Reference Broadcast Method	Uses broadcast to reduce sender-receiver delay uncertainty	Efficient for multi-node synchronization without exact message timestamping

5. ENERGY-EFFICIENT SYNCHRONIZATION PROTOCOLS

Energy-efficient synchronization protocols in wireless sensor networks (WSNs) aim to align the clocks of sensor nodes while minimizing energy consumption, which is crucial due to the limited battery capacity of nodes. Time synchronization in such networks can be achieved using strategies that reduce message transmissions, employ selective broadcasting, and optimize local computations. For example, protocols like the Flooding Time Synchronization Protocol (FTSP) utilize broadcast-based synchronization to efficiently coordinate multiple nodes simultaneously, thereby reducing redundant messages (Maróti, Kusy, Simon, & Lédeczi, 2004).
Security and reliability are also important considerations. Attack-resilient synchronization protocols are designed to ensure that nodes remain accurately synchronized even under potential malicious interference, all while conserving energy by limiting unnecessary communications (Song, Zhu, & Cao, 2007; Ganeriwal, Čapkun, Han, & Srivastava, 2005). Similarly, distributed multi-hop synchronization approaches reduce energy consumption by carefully scheduling transmissions across multiple nodes, preventing excessive network traffic (Robles, Borkar, & Kumar, 2007). Energy-efficient synchronization is further enhanced in real-world systems, such as sensor network-based countersniper applications, where the timing precision must be maintained without draining node batteries (Simon, Maróti, Lédeczi, & Balogh, 2004).
Protocols often balance energy efficiency and computation using the formula:

$$Esync = Ntx \times Etx + Nrx \times Erx + Eproc \quad (6)$$

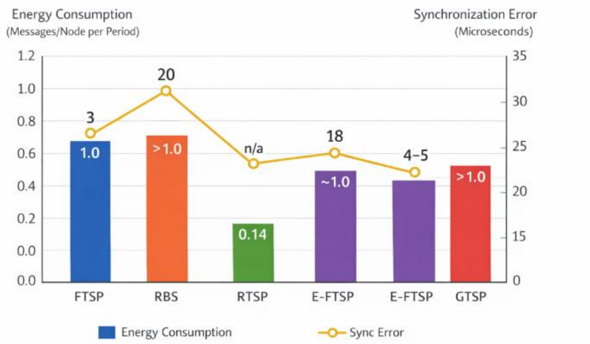
Here, Esync represents the total energy consumed for synchronization, Ntx and Nrx are the numbers of transmitted and received messages, Etx and Erx are the energies per transmission and reception, and Eproc is the energy consumed by local computations. Using this formula, designers can evaluate protocols like FTSP and attack-resilient methods to ensure minimal energy usage while achieving reliable and secure synchronization (Manzo, Roosta, & Sastry, 2005).
By integrating strategies for message reduction, selective broadcasting, and security-aware synchronization, WSN protocols can maintain accurate network-wide time while extending the operational lifetime of sensor nodes.

Table 2: Synchronization Protocols (Performance Metrics)
Source: Survey of Time Synchronization Protocols in Wireless Sensor Networks – IJERT, Performance Analysis of Time Synchronization Protocols in Wireless Sensor Networks

Protocol	**Energy Consumption (messages/node per period)**	**Synchronization Error (µs)**	**Notes**
FTSP	1 message per period (baseline)	~3 µs error per hop *	Broadcast-based synchronization with low message count
RBS	More than FTSP (higher consumption)	~11–29 µs (varies by evaluation)	Receiver-receiver approach; more message exchanges
RTSP (long-run)	~0.14–0.2 messages (very low)	—	Consumes 5–7× less energy than FTSP in long-run simulation
E-FTSP (extended FTSP)	Comparable to FTSP messages	~20 µs max error under jitter	Reduced error vs FTSP in jitter scenarios
GTSP	Higher energy than FTSP	~4–5 µs neighbor error	Distributed consensus; robust but more signaling

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 01/05/2024 Revised:03/06/2024 Accepted: 01/07/2024

Figure 3: Energy consumption and sync error comparison



The table compares various time synchronization protocols in terms of energy consumption and synchronization accuracy. FTSP serves as a baseline with low energy use, sending one message per node per period and achieving around 3 µs error per hop. RBS consumes significantly more energy due to its receiver-to-receiver message exchanges, with higher synchronization errors ranging from 11 to 29 µs. RTSP demonstrates excellent energy efficiency, using only 0.14–0.2 messages per period, which is 5–7 times less than FTSP, though its long-term error data is not specified. Extended FTSP maintains similar energy use to FTSP but reduces maximum error to about 20 µs under jitter conditions. GTSP achieves low neighbor errors of 4–5 µs but requires higher energy, reflecting a trade-off between accuracy and message overhead. Overall, the table highlights the balance between energy efficiency and synchronization precision in WSN protocols.

6. SECURITY AND ATTACK-RESILIENT TIME SYNCHRONIZATION

In wireless sensor networks (WSNs), ensuring accurate time synchronization is critical not only for data consistency and coordination but also for defending against potential attacks. Security vulnerabilities in time synchronization protocols can lead to incorrect data fusion, network misbehavior, or even malicious disruption of critical services. To address these issues, specialized attack-resilient protocols have been developed, emphasizing robustness, accuracy, and minimal communication overhead.

One key technique for secure synchronization involves estimating the **clock skew** between nodes to detect abnormal behavior. Clock skew can be mathematically expressed as:

$$\alpha = \frac{Cj(t2)-Cj(t1)}{Ci(t2)-Ci(t1)} \quad (7)$$

Here, Ci(t) and Cj(t) represent the local clocks of nodes i and j at time t, and α denotes the relative rate difference between the two clocks. By continuously monitoring α, a node can identify irregularities caused by malicious timing modifications, ensuring that synchronization remains accurate and secure.

Protocols such as Delay Measurement Time Synchronization (DMTS) focus on accurately estimating message delays to prevent timing attacks, as suggested by Su (2003). Similarly, lightweight schemes proposed by van Greunen & Rabaey (2003) reduce energy consumption while maintaining secure timing across the network. Sichitiu & Veerarittiphan (2003) introduced simple yet effective methods for detecting inconsistencies in clock updates, which further enhances the network's resilience against attacks.

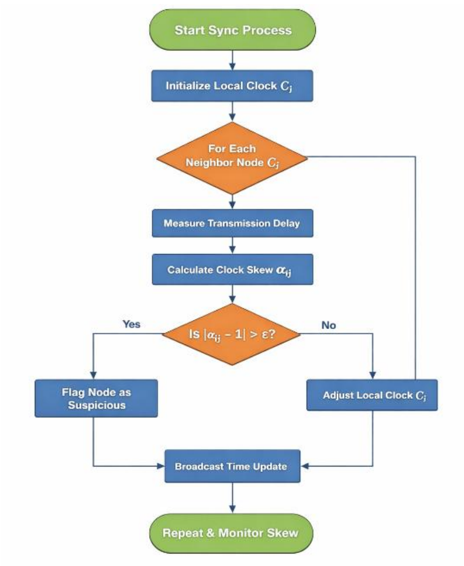


Figure 4: Secure time sync process flowchart
Source: Self-Created in Ms. PowerPoint

Overall, attack-resilient synchronization strategies in WSNs combine mathematical monitoring of clock behavior with protocol-level safeguards to ensure secure and reliable network operation. These approaches are crucial for maintaining integrity in sensor networks deployed in critical applications such as environmental monitoring, industrial automation, and defense systems.

7. PERFORMANCE EVALUATION METRICS AND COMPARATIVE ANALYSIS

Time synchronization protocols in wireless sensor networks (WSNs) are evaluated using several performance metrics that assess their accuracy, efficiency, scalability, and robustness. A critical metric is synchronization error, which measures the deviation between the clocks of different nodes. This is often expressed as the average or maximum offset in microseconds (µs) across the network. Another key metric is message complexity, which quantifies the number of messages exchanged per synchronization cycle, directly affecting energy consumption and network lifetime. Protocols are also analyzed for convergence time, the time required for all nodes to reach a synchronized state, and scalability, which evaluates how well the protocol performs as the number of nodes increases.

For instance, protocols like Reference Broadcast Synchronization (RBS) and Timing-sync Protocol for Sensor Networks (TPSN) focus on reducing synchronization error through broadcast-based or hierarchical approaches, respectively, whereas Gradient Time Synchronization Protocol (GTSP) emphasizes robust distributed consensus among neighboring nodes to maintain accuracy over multi-hop networks. Comparative studies often use simulation and experimental testbeds to measure trade-offs between energy consumption and synchronization accuracy.

Formally, synchronization error ϵi for node i can be defined as:

$$\epsilon i = |Ci(t) - Cref(t)| \qquad (8)$$

where Ci(t) is the local clock of node i at time t and Cref(t)C(t) is the reference clock. Average network error is then:

$$\bar{\epsilon} = \frac{1}{N}\sum_{i=1}^{n} \epsilon i \qquad (9)$$

This provides a quantitative basis for comparing protocols. For example, RBS achieves low average error in dense networks but increases message complexity, whereas TPSN reduces message overhead at the cost of slightly higher synchronization error. Evaluations by Elson et al. (2002) demonstrate that reference broadcast-based protocols achieve microsecond-level accuracy with reasonable energy efficiency, while hierarchical protocols provide faster convergence for larger networks.

In essence, comparative analysis helps select the optimal protocol depending on the application requirements: high accuracy for scientific monitoring or low energy consumption for long-term deployments.

8. CONCLUSION

Accurate time synchronization is essential for coordinated operation and data reliability in wireless sensor networks. Techniques such as PulseSync, RTSP, and adaptive value tracking balance precision, energy efficiency, and robustness, while attack-resilient protocols ensure security against malicious disruptions. Performance metrics like synchronization error and message overhead help in evaluating and selecting suitable protocols. Overall, combining precise offset estimation with energy-efficient and secure methods enables reliable WSN operation in practical applications.

REFERENCES

1. Huan, X., He, H., Wang, T., Wu, Q., & Hu, H. (2022). A timestamp-free time synchronization scheme based on reverse asymmetric framework for practical resource-constrained wireless sensor networks. IEEE Transactions on Communications, 70(9), 6109–6121. https://doi.org/10.1109/TCOMM.2022.3188830
2. Huan, X., Kim, K. S., Lee, S., Lim, E. G., & Marshall, A. (2021). Improving multi-hop time synchronization performance in wireless sensor networks based on packet-relaying gateways with per-hop delay compensation. IEEE Transactions on Communications, 69(9), 6093–6105. https://doi.org/10.1109/TCOMM.2021.3092038
3. Huan, X., Kim, K. S., Lee, S., Lim, E. G., & Marshall, A. (2020). A beaconless asymmetric energy-efficient time synchronization scheme for resource-constrained multi-hop wireless sensor networks. IEEE Transactions on Communications, 68(3), 1716–1730. https://doi.org/10.1109/TCOMM.2019.2960344
4. Phan, L.-A., Kim, T., Kim, T., Lee, J.-S., & Ham, J.-H. (2019). Performance analysis of time synchronization protocols in wireless sensor networks. Sensors, 19(13), Article 3020. https://doi.org/10.3390/s19133020
5. Fan, K., Ren, Y., Yan, Z., Wang, S., Li, H., & Yang, Y. (2018). Secure time synchronization scheme in IoT based on blockchain. In Proceedings of the IEEE International Conference on Internet of Things (iThings), Green Computing and Communications (GreenCom), Cyber, Physical and Social Computing (CPSCom), and Smart Data (SmartData) (pp. 134–141). https://doi.org/10.1109/Cybermatics_2018.2018.00196
6. Kim, K. S., Lee, S., & Lim, E. G. (2017). Energy-efficient time synchronization based on asynchronous source clock frequency recovery and reverse two-way message exchanges in wireless sensor networks. IEEE Transactions on Communications, 65(1), 347–359. https://doi.org/10.1109/TCOMM.2016.2626281
7. Sarvghadi, M. A., & Wan, T.-C. (2016). Message passing based time synchronization in wireless sensor networks: A survey. Journal of Sensors, 2016, Article 1280904. https://doi.org/10.1155/2016/1280904

8. Lenzen, C., Sommer, P., & Wattenhofer, R. (2015). PulseSync: An efficient and scalable clock synchronization protocol. IEEE/ACM Transactions on Networking, 23(3), 717–727. https://doi.org/10.1109/TNET.2014.2309805
9. Yildirim, K. S., & Kantarci, A. (2014). Time synchronization based on slow-flooding in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 25(1), 244–253. https://doi.org/10.1109/TPDS.2013.40
10. Yıldırım, K. S., & Gürcan, Ö. (2014). Efficient time synchronization in a wireless sensor network by adaptive value tracking. IEEE Transactions on Wireless Communications, 13(7), 3650–3664. https://doi.org/10.1109/TWC.2014.2316168
11. Akhlaq, M., & Sheltami, T. R. (2013). RTSP: An accurate and energy-efficient protocol for clock synchronization in wireless sensor networks. IEEE Transactions on Instrumentation and Measurement, 62(3), 578–589. https://doi.org/10.1109/TIM.2012.2232472
12. Akhlaq, M., & Sheltami, T. R. (2012). The recursive time synchronization protocol for wireless sensor networks. In Proceedings of the IEEE Sensors Applications Symposium (SAS 2012) (pp. 1–6). https://doi.org/10.1109/SAS.2012.6166318
13. Prakash, R., & Nygard, K. (2010). Time synchronization in wireless sensor networks: A survey. International Journal of UbiComp, 1(2), 1–12. https://doi.org/10.5121/iju.2010.1206
14. Ranganathan, P., & Nygard, K. (2010). Time synchronization in wireless sensor networks: A survey. *International Journal of Ubiquitous Computing*, 1(2), 1–12. https://doi.org/10.5121/iju.2010.1206
15. Sommer, P., & Wattenhofer, R. (2009). Gradient clock synchronization in wireless sensor networks. In Proceedings of the 8th International Conference on Information Processing in Sensor Networks (IPSN 2009) (pp. 37–48). https://doi.org/10.1145/1602165.1602171
16. Schenato, L., & Gamba, G. (2008). A distributed consensus protocol for clock synchronization in wireless sensor networks. In Proceedings of the 46th IEEE Conference on Decision and Control (CDC 2007) (pp. 2289–2294). https://doi.org/10.1109/CDC.2007.4434671
17. Ganeriwal, S., Pöpper, C., Čapkun, S., & Srivastava, M. B. (2008). Secure time synchronization in sensor networks. ACM Transactions on Information and System Security, 11(4), Article 23. https://doi.org/10.1145/1380564.1380571
18. Ren, F., Lin, C., & Liu, F. (2008). Self-correcting time synchronization using reference broadcast in wireless sensor networks. IEEE Wireless Communications, 15(4), 79–85. https://doi.org/10.1109/MWC.2008.4599225
19. Song, H., Zhu, S., & Cao, G. (2007). Attack-resilient time synchronization for wireless sensor networks. Ad Hoc Networks, 5(1), 112–125. https://doi.org/10.1016/j.adhoc.2006.05.016
20. Robles, R. S., Borkar, V. S., & Kumar, P. R. (2007). A new distributed time synchronization protocol for multihop wireless networks. In Proceedings of the 45th IEEE Conference on Decision and Control (CDC 2006) (pp. 2734–2739). https://doi.org/10.1109/CDC.2006.377675
21. Ganeriwal, S., Čapkun, S., Han, C.-C., & Srivastava, M. B. (2005). Secure time synchronization service for sensor networks. In Proceedings of the 2005 ACM Workshop on Wireless Security (pp. 97–106). https://doi.org/10.1145/1080793.1080809
22. Manzo, M., Roosta, T., & Sastry, S. (2005). Time synchronization attacks in sensor networks. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005) (pp. 107–116). https://doi.org/10.1145/1102219.1102238
23. Maróti, M., Kusy, B., Simon, G., & Lédeczi, Á. (2004). The flooding time synchronization protocol. In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys 2004) (pp. 39–49). https://doi.org/10.1145/1031495.1031501
24. Simon, G., Maróti, M., Lédeczi, Á., & Balogh, G. (2004). Sensor network-based countersniper system. In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys 2004) (pp. 1–12). https://doi.org/10.1145/1031495.1031497
25. Su, P. (2003). Delay measurement time synchronization for wireless sensor networks. Unpublished manuscript.
26. van Greunen, J., & Rabaey, J. M. (2003). Lightweight time synchronization for sensor networks. In Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications (WSNA 2003) (pp. 11–19). https://doi.org/10.1145/941350.941353
27. Sichitiu, M. L., & Veerarittiphan, C. (2003). Simple, accurate time synchronization for wireless sensor networks. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2003) (Vol. 2, pp. 1266–1273). https://doi.org/10.1109/WCNC.2003.1200555
28. Elson, J., Girod, L., & Estrin, D. (2002). Fine-grained network time synchronization using reference broadcasts. ACM SIGOPS Operating Systems Review, 36(SI), 147–163. https://doi.org/10.1145/1060289.1060304
29. Elson, J., & Römer, K. (2002). Wireless sensor networks: A new regime for time synchronization. In Proceedings of the First Workshop on Hot Topics in Networks (HotNets-I) (pp. 149–154).
30. Römer, K. (2001). Time synchronization in ad hoc networks. In Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001) (pp. 173–182). https://doi.org/10.1145/501436.501440

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 25, No. 1 (2024)
http://www.veterinaria.org
Article Received: 01/05/2024 Revised:03/06/2024 Accepted: 01/07/2024