RESEARCH ARTICLE OPEN ACCESS

Challenges of Time Synchronization in Wireless Sensor Networks and overcoming the issues

ASIR SATHIA REGIN.D [1], Dr. VIKRAM JAIN [2]
[1] Research Scholar, Himalayan University, Arunachal Pradesh,
[2] Associate Professor, Department of Computer Science, S.S.Jain Subodh PG College - Jaipur

ABSTRACT
A Wireless Sensor Network (WSN) is a network of sensor nodes that can be used to examine physical surroundings, communicate, and gather data. To distribute their data, sensor node communication is performed with a base station, for processing and storage remotely. Because they are dispersed, there are some obstacles and limits in terms of energy, design, security, and other areas. WSNs face challenges in terms of deployment, coverage, trust models, time synchronization, middleware, fault tolerance, and other factors. We explored Time Synchronization (TS) and its importance, as well as concerns, in this paper so that we may quickly identify problems and suggest useful solutions.

I. INTRODUCTION

Wireless sensor networks are a new field that combines sensing, processing, and communication into a single small device. Without a doubt, wireless transmission techniques are used for all communication between nodes. Sensing is a technique for gathering data about a physical object or process, such as when events occur. A sensor is an object that performs such a sensing task.

A sensor network is a collection of sensing (measurement), computation, and communication components. A wireless sensor network (WSN) is made up of distributed nodes that provide signal processing, embedded computer, and connection. WSNs normally send data to collecting (monitoring) stations, which then aggregate some or all of it [5]. Because of their distributed structure and deployment in remote places, these networks are exposed to a variety of security vulnerabilities that can jeopardize their correct operation.

Sensor nodes are generally concerned about two key security concerns: privacy preservation and node authentication. The term "privacy" refers to data secrecy established through a security method [4]. While sensor networks have a lot in common with other distributed systems, they also have their own set of challenges and limits.

Time synchronization helps sensor nodes communicate more effectively. The wireless network's time synchronization problem is to get synchronized with the local clocks of sensor network. Many sensor network applications necessitate the synchronization of sensor node local clocks, which necessitates varying degrees of precision. Local clocks of nodes may drift apart in time due to the imperfection of all hardware clocks. When a network node creates a timestamp to send to another node for synchronization, the packet containing the timestamp will experience a variable degree of delay before it reaches the destination node. This delay hinders the receiver from precisely comparing the two nodes' local clocks and synchronizing with the sender node. Addressing the synchronization problem in sensor networks is important for a variety of reasons. The following are some of the reasons: Sensor nodes must coordinate their operations in order to complete a task, and the network's life depends on electricity. So, in order to extend the life of the network, we must employ power-saving strategies

II. LITERATURE REVIEW

WSNs are large-scale distributed systems, however due to their unique properties, particularly the severe resource limits, typical distributed techniques cannot be considered solving problems [3]. Because wireless communications use a broadcast transmission medium, attackers can readily compromise WSNs. Self-identification, self-diagnosis, dependability, time awareness for cooperation with other nodes, and network interfaces are all included in sensor nodes.

The synchronization mechanism is a phenomenon that is subject to a number of constraints and must meet a number of criteria. These constraints, such as decreasing energy use, lowering associated expenses, and maximizing the quality and accuracy of services offered, can sometimes be incompatible. In distributed computing environments, time synchronization is a critical function for many applications and operating systems [7].

However, when using sensor networks, the time synchronization requirements are drastically different. These networks, which are made up of a huge number of

sensor nodes, are generally impenetrable [10]. This characteristic makes maintaining central synchronization extremely challenging. Due to the restricted battery capacity of nodes, energy efficiency is another key issue in the synchronization problem.

III. WIRELESS SENSOR NETWORK(WSN)

A wireless sensor network is a distributed network that connects autonomous sensors for a variety of network operations. WSN is made up of several sensor nodes, which are compact, light, and portable detecting stations. WSNs are bidirectional, and the topology varies depending on the application. WSN features include node mobility and heterogeneity, large-scale deployment, ease of use, and the ability to cope with node failures, among others.

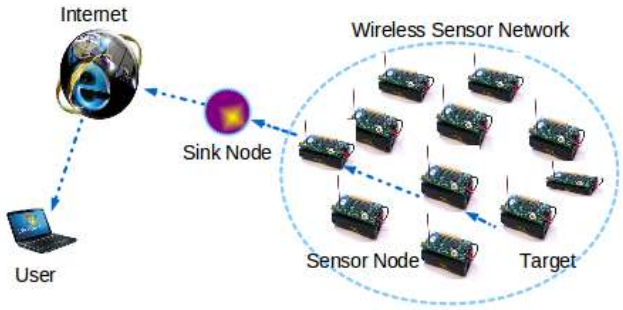

Fig1. A Wireless Sensor Network

A sensor node's job is to detect events, execute local data processing, and communicate raw and/or processed data in a sensor region. Sink node is nothing more than a base station that serves as a distributed controller in a wireless environment. The base station is necessary for the following reasons: sensor nodes are mostly prone to become failure, data collection is improved, and backup is always provided even if the master node fails.

IV. CHALLENGES IN WSN

Wireless sensor networks have a lot of potential since they will allow us to monitor and interact with the physical world from a distance. Sensors have the capacity to capture a large volume of previously unidentified data. Sensors can be accessible remotely and installed in areas where data and power lines are prohibitive. To fully realize the potential of sensor networks, we must first solve the networks' unique limits and the resulting technical challenges. Although data fusion necessitates synchronization of nodes, synchronization algorithms for sensor networks must take into account the following characteristics. A number of hurdles and obstacles must be addressed in order for WSNs to become genuinely widespread.

4.1 Energy Efficiency

Energy efficiency is the first and most critical design problem for a WSN. The three functional domains of power consumption are sensing, communication, and data processing, each of which requires optimization. The sensor node's lifetime is usually highly dependent on battery life. Sensor nodes have limited energy budgets, which is the most common constraint associated with sensor network architecture.

Sensors are usually powered by batteries, which must be changed or recharged when they run out.. A sensor node should be able to operate with non-rechargeable batteries until the mission timer expires or the battery can be replaced. The duration of the mission is determined by the application.

4.2 Limited bandwidth

In wireless sensor networks, analyzing data consumes far less energy than transmitting it. Wireless communication is currently limited to data rates of 10–100 kilobits per second. Message transfers between sensors are directly influenced by bandwidth limitations, and synchronization is impossible without them. Sensor networks frequently use a multi-hop wireless communication medium with limited bandwidth and performance. These wireless communication links use radio, infrared, or optical frequencies to communicate.

4.3 Node Costs

A sensor network is made up of several sensor nodes. As a result, the cost of a single node is essential to the sensor network's total financial metric. Clearly, every sensor node's expenditure must be kept to minimum in order for the global metrics to be acceptable. Depending on the use of a sensor network, such as weather monitoring, a large number of sensors may be dispersed randomly around an environment. If the overall cost of sensor networks was suitable, it would be more acceptable and successful for users who require careful-attention.

4.4 Node Deployment

In Wireless Sensor Networks, one of the critical issues to address is the node deployment. The complexity of problems can be reduced by using a good node deployment scheme. Deploying and administering a large number of nodes in a constrained environment necessitates the use of unique methodologies. In a sensor zone, hundreds to thousands of sensors may be installed. At the moment, there are two deployment models: (i) The static deployment

and (ii) The dynamic deployment. The static deployment selects the ideal position based on the optimization technique, and the location of the sensor nodes remains constant during the WSN's lifetime. The nodes are thrown at random in the dynamic deployment for optimization.

4.5 Design Constraints

Wireless sensor design's main goal is to make devices that are smaller, cheaper, and more efficient. The design of sensor nodes and wireless sensor networks might be hampered by a number of other issues. With limited limits, WSN has issues in both software and hardware design models.

4.6 Security Issues

One of the difficulties in WSNs is meeting high security requirements while working with limited resources. A large number of wireless sensor networks collect sensitive data. Sensor nodes that are operated remotely and unmanaged are more vulnerable to hostile invasions and attacks. Node authentication as well as the data secrecy are two security criteria in WSNs. The deployment sensors must pass a node authentication examination by their respective manager nodes or cluster heads to detect both trustworthy and unreliable nodes from a security standpoint, and unauthorized nodes can be isolated from WSNs during the node authentication method. As a result, new solutions for key creation and distribution, node authentication, and secrecy are required for sensor networks.

V. TIME SYNCHRONIZATION

Time synchronization is a technique for ensuring reliable communication between network nodes. The ability to discern movement, location, and speed is possessed by TS. Time synchronization is required in any distributed system. Transmission scheduling, power control, data fusion, and a variety of other applications all require it. Sensors in the sensor network observe the movement and speed of moving objects, necessitating the use of TS. Furthermore, the time difference between sensor time stamps should correspond to the time difference between real timings in order to accurately identify the velocity of a moving item.

5.1 Clock Drift and Skew

When a clock does not run at the exact same pace as another clock, this is referred to as clock drift. That is, the clock "drifts apart" from the other clock over time. Timing attacks can take advantage of clock drift on the negative side. The stability of the interrupt requests limits its accuracy. The clock gains or loses time as the interrupt request rate changes. The discrepancy between two clocks of two nodes at one moment in time is known as clock offset or skew.

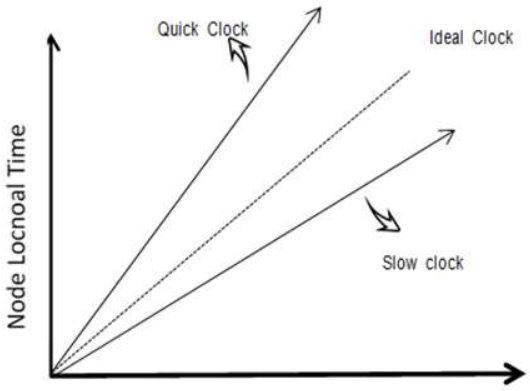

Fig2. The Synchronization Clock Differences

5.2 Metrics of Synchronization

Sensor node synchronization is usually based on some type of message exchange. Synchronization metrics are a measurement of a sensor network's overall performance. The following metrics are used to determine each node's performance.

Energy Efficiency — Because network nodes have limited energy resources, synchronization techniques should account for the sensor nodes' restricted energy resources.
Scalability — Hundreds of thousands of sensors could be used in some applications. The number of nods can be raised or lowered at any time. With an increasing number of nodes and/or high network density, a synchronization mechanism
should scale well.
Precision — Depending on the application and the goal of synchronization, the necessity for precision, or accuracy, might vary greatly. The precision of the results may vary by microseconds.
Robustness — In potentially hazardous circumstances, a sensor network is frequently left unattended for long periods of time. If one of the network's nodes fails or goes offline, it has no effect on the network's other nodes or the synchronization system.
Lifetime — A synchronization algorithm's offered synchronized time among sensor nodes can be instantaneous or last as long as the network's operating duration.
Cost and Size — Because of new technologies, wireless sensor nodes are compact and inexpensive devices. As a result, the synchronization technique should not be very expensive or excessive in size.

5.3 Communication for Time Synchronization

Sensor nodes have also been employed for communication, as previously indicated. Messages are used by the nodes to have communication between one another. Nodes that primarily broadcast their own sensor data and nodes that primarily relay messages from other nodes, for example Sensor data is transferred out from source nodes to the sink via relay nodes, culminating in a multi-hop architecture. On the other hand, single-hop communication varies significantly from multi-hop communication. Single-hop communication, on the other hand, differs slightly from that of the multi-hop communication.

• Single-hop communication

In a single-hop network, a sensor node can communicate and share messages with any other sensor. On the other hand, most wireless sensor network technologies encompass many domains or communities. (Nodes in a neighbourhood can communicate using single hop message transmission.) Because the network is typically too large, each sensor node is unable to interact directly with the others.

• Multi-hop communication

The growing size of wireless sensor networks necessitates the use of multi-hop communication. In such instances, sensors inside one domain interact with sensors in some other domain through an intermediate sensor that may relate to both domains. A sequence of hops can be used to communicate in a series of pair-wise neighbouring sensors.

5.4 Time Synchronization through Connection - Oriented Services

Before transmitting a packet, the source establishes a connection with the destination in a connection-oriented service. Once the connection has been established, a string of packets are sent one after the other on the same path.. The connection is terminated when all packets of a message have been delivered. In a nutshell, there are three stages to this service: connection formation, data transfer, and connection release / termination. This service is sometimes referred to as dependable, as it provides acknowledgement after each successful delivery.

For time synchronization, two approaches have been used: (i) Network Time Protocol (NTP) and (ii) Global Positioning System (GPS). In NTP, the client sends a request to the server for time synchronization. Both of the server and client need an accurate clock to share time. GPS is generally expensive, and for synchronization, it talks with satellites.

5.5 Time Synchronization through Connectionless Services

Packets of a message are sent on separate paths in a connectionless service. Because the packets are not numbered and are treated separately, they may be delayed, misplaced, or arrive out of order. It can be characterized as a shaky, best-effort delivery service. There is no mechanism for error checking or tracking when the term "best effort" is used.

Table1. Comparison Between Connection-Oriented and Connectionless Services

Characteristics	Connection Oriented	Connectionless
Connection Setup	Required	Not Required
Data Interface	Stream based	Message based
Retransmission	Retransmitted	Not Performed
Speed	Low	Very High
Packets	Packets sent in sequential order	Packets are not numbered
Authentication	Required	Not Required
Reliability	Often reliable not always	Unreliable, best effort delivery service
Acknowledgement	Data is acknowledged	No Such Provision
Flow of data	Flow control using sliding window	None
Overhead	High and demands on bandwidth	Less

Batteries power wireless devices, and sensor nodes are all inexpensive. Due to a lack of coverage, wireless networks are limited in size. The sequencing of messages determines time in a wireless network, and each node's clock is independent. The local time of each node is used to synchronize the nodes. Information regarding a node's drift and offset is saved.

VI. ISSUES OF TIME SYNCHRONIZATION

Time synchronization is a well-known requirement for flawless communication, although it has significant drawbacks in terms of various synchronization systems.

Synchronization maintains the sensor network's nodes' credibility and increases its security.

6.1 Master – Slave Synchronization

One node has total control over one or more other nodes in a master-slave communication system. In certain networks, a master is selected from among a group of nodes, with the rest of the nodes operating as slaves. The slave nodes use the master node's local clock reading as the reference time and attempt to synchronize with it. One or more synchronization slaves receive time code information (synchronization signals) from the synchronization master.

6.2 Peer – Peer Synchronization

Peer - Peer synchronization is a direct synchronization approach in which a node can connect directly with other nodes in the sensor network. It's also known as point-to-point synchronization. This method eliminates the possibility of the master node failing. As a result, this type of synchronization is more adaptable, but also more unpredictable.

6.3 Internal Synchronization

Internal synchronization refers to the fact that all nodes in a network are in sync with one another, although the time is not always precise in terms of UTC (Universal Time Controller). Internal clocks might differ not only in terms of the time they contain, but also in terms of the rate at which they tick. Because it lacks global time, it tries to reduce the maximum divergence between the readings of the sensors' local clocks.

6.4 Probabilistic Synchronization

In distributed systems with unlimited random communication delays, a probabilistic method for reading remote clocks is proposed. The method can be used to improve synchronization precision. Because it does not ensure that a node can always read a remote clock with an a priori stated precision, the approach is probabilistic. When a process succeeds in reading a remote clock, it understands the actual reading precision attained, which is a crucial feature of the method.

6.5 External Synchronization

All nodes in the network are synced with an external source of time, which is known as external synchronization. There is a standard time that can be used as a reference time. Sensors' local clocks attempt to synchronize with this reference time. The time will not differ from one network node to the next.

6.6 Deterministic Synchronization

Deterministic synchronization algorithm for networks with time-varying topologies. Depending on the uses, a network's topology may alter. When we move nodes around, their response times shift. This synchronization compares the two response times, that is, before and after the change in topology.

6.7 Sender – Receiver Synchronization

Every so often, the sender node sends a message to the receiver with it's own local time like a timestamp, and also the receiver synchronizes well with sender using the sender's timestamp. The total round-trip time between the moment a receiver requests a timestamp and the time it actually receives a response is used to compute the message delay between the sender and receiver.

6.8 Receiver – Receiver Synchronization

This method takes advantage of the fact that in a single-hop transmission, if two recipients get the identical message, they will receive it at roughly the same time. Receivers compare the times at which they got the same message and calculate their offset depending on the time difference. This strategy has the advantage of reducing message delay variance, which is susceptible to propagation delays caused by different receivers and variances in receiving time.

VII. CONCLUSION

Due to the efficiency of computer and sensing technologies, compact, low-power, and low-cost sensors and controllers may be developed. A wireless sensor includes a sensing component as well as processing, transmission, and storage capabilities. We recognize that communication is one of the most difficult aspects of designing a sensor network. The transmission energy rapidly increases as the distance in between sensor node as well as a base station grows. As a result, splitting a long journey into multiple shorter ones saves energy, posing the difficulty of enabling multi-hop communications. Multi hop communication necessitates network nodes cooperating with one another, identifying optimal paths, and acting as relays. This problem is exacerbated in energy-conservation networks. WSN's Time Synchronization is indeed a huge region that helps sensor nodes achieve maximum precision. Finally, this study will serve as a valuable framework for academics to work on diverse WSN challenges and uncover strategies and techniques for overcoming Time Synchronization issues.

REFERENCES

[1]Amir Ijaz, Fulvio Babich,“ A Brief Review of Network and Sensor Virtualization for Wireless Sensor Networks,” International Journal of Sensors Wireless Communications and Control, 2015.
[2] Carmen Delgado, et.al,‘‘ On Optimal Resource Allocation in Virtual Sensor Networks,’’ Journal of Ad-hoc Networks,April.2016.
[3] Vahid Maleki Raee and Amin Ebrahimzadeh,‘‘Energy Efficient Virtual Network Embedding in Virtualized Wireless Sensor Networks,’’ IEEE Consumer Communications & Networking Conference. January 2022.
[4] P. Zhang, X. Pang, Y. Bi, H. Yao, H. Pan, and N. Kumar, “DSCD: Delay sensitive cross-domain virtual network embedding algorithm,” IEEE Transactions on Network Science and Engineering, 2020.
[5] V. M. Raee, D. Naboulsi, and R. Glitho, “Energy efficient task assignment in virtualized wireless sensor networks,” in Proc. IEEE Symposium on Computers and Communications (ISCC), 2018, pp. 00 976–00 979.
[6] A. Mukherjee, P. Goswami, Z. Yan, L. Yang, and J. J. Rodrigues, “ADAI and adaptive PSO-based resource allocation for wireless sensor networks,” IEEE Access, vol. 7, pp. 131 163–131 171, 2019.
[7] Z. Li and A. Zhong, “Resource allocation in wireless powered virtualized sensor networks,” IEEE Access, vol. 8, pp. 40 327–40 336, 2020.
[8] C. Delgado, J. R. Gállego, M. Canales, J. Ortín, S. Bousnina, and M. Cesana, “On optimal resource allocation in virtual sensor networks,” Elsevier Ad Hoc Networks, vol.
50, pp. 23–40, 2016.
[9] M. N. Alam and R. H. Glitho, “An infrastructure as a service for the Internet of Things,” in Proc. IEEE.
[10] Z. Yan, J. Ge, Y. Wu, L. Li, and T. Li, “Automatic virtual network embedding: A deep reinforcement learning approach with graph convolutional networks,” IEEE Journal on Selected Areas in Communications,vol. 38, no. 6, pp. 1040–1057, 2020.
[11] Z. Xu, L. Zhuang, S. Tian, M. He, S. Yang, Y. Song, and L. Ma,“Energy-driven virtual network embedding algorithm based on enhanced bacterial foraging optimization,” IEEE Access, vol. 8, pp. 76 069–76 081, 2020.
[12] H. Q. Al-Shammari, A. Lawey, T. El-Gorashi, and J. M. Elmirghani “Energy efficient service embedding in IoT over PON,” in Proc. IEEE International Conference on Transparent Optical Networks (ICTON),2019, pp. 1–5.
[13] H. Q. Al-Shammari, A. Q. Lawey, T. E. El-Gorashi, and J. M. Elmirghani, “Service embedding in iot networks,” IEEE Access, vol. 8, pp. 2948–2962, 2019.