Challenges of Wireless Sensor Networks and Issues associated with Time Synchronization

S. Karthik
Research Scholar, Research & Development Centre, Bharathiar University, Coimbatore-46
Email: kalini1987@gmail.com

Dr. A. Ashok Kumar
Assistant Professor, Department of Computer Science, Alagappa Govt. Arts College, Karaikudi-03
Email: ashokjuno@rediffmail.com

ABSTRACT

Wireless Sensor Network (WSN) is a network with numerous sensor nodes for examining physical situations, communication and data collection. Sensor nodes communicate with a base station to distribute their data for the purpose of remote process and storage. They are scattered, so it has some challenges and constraints in energy, design, security and more. WSNs have some tribulations on different methods such as deployment, coverage, trust model, time synchronization, middleware, fault tolerance and the rest. In this paper, we have discussed about Time Synchronization (TS) and its importance, issues, so that we can easily find the problems and propose some valuable methods to solve those issues.

Keywords - **Sensor Network, Clock Drift & Skew, Single-hop, Multi-hop, Synchronization.**

1. NTRODUCTION

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Undoubtedly, all communication between nodes is through the wireless transmission techniques. Sensing is a technique used to gather information about a physical object or process, including the occurrence of events. An object performing such a sensing task is called a sensor.

A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication. A WSN consists of distributed nodes that support signal processing, embedded computing and connectivity. WSNs typically transmit information to collecting (monitoring) stations that aggregate some or all of the information [5]. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning.

Generally, sensor nodes are concerned about two major security issues, which are privacy preserving and node authentication. Privacy means the data confidentiality is achieved under security mechanism [4]. While sensor networks share many similarities with other distributed systems, they are subject to a variety of unique challenges and constraints.

Time Synchronization is useful for better communication among the sensor nodes. The time synchronization problem is to synchronize the local clocks of sensor nodes in the wireless network [8]. Many applications of sensor networks need local clocks of sensor nodes to be synchronized, requiring various degrees of precision. Since all hardware clocks are imperfect, local clocks of nodes may drift away from each other in time. When a node in the network generates a timestamp to send to another node for synchronization, the packet carrying the timestamp will face a variable amount of delay until it reaches. This delay prevents the receiver from exactly comparing the local clocks of the two nodes and accurately synchronizing to the sender node.

There are several reasons for addressing the synchronization problem in sensor networks. Some reasons are as following: Sensor nods are required to coordinate their operations to perform a particular task, Life time of network is depending on power. So to increase the life of network we need to use power saving schemes.

2. LITERATURE REVIEW

WSNs are large-scale distributed systems, but traditional distributed algorithms cannot be considered for problems due to their unique characteristics, especially the severe resource constraints [3].

WSNs are easily compromised by attackers due to wireless communications use a broadcast transmission medium. Sensor nodes include some functions such as self-identification, self-diagnosis, reliability, time awareness for coordination with other nodes and network interfaces.

The synchronization mechanism is a phenomenon subject to many constraints, which must meet several requirements. These limitations sometimes can be incompatible, such as minimizing energy consumption, reducing the associated costs, and maximizing the quality and accuracy of services provided. Time synchronization is a key service for many applications and operating systems in distributed computing environments [7].

However, the time synchronization requirements differ significantly in the context of use of sensor networks. In general, these networks are impenetrable, composed of a large number of sensor nodes [10]. This property makes a lot of difficulties to keep the central synchronization. Energy efficiency is another major problem in synchronization problem due to limited battery capacity of nodes.

3. WIRELESS SENSOR NETWORK

A Wireless sensor network is a distributed network where autonomous sensors are connected together for various network operations. WSN consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. WSNs are bi-directional and its topology differs from each application. WSN has some characteristics such as: mobility and heterogeneity of nodes, large scale of deployment, ease of use, ability to cope with node failures and more.

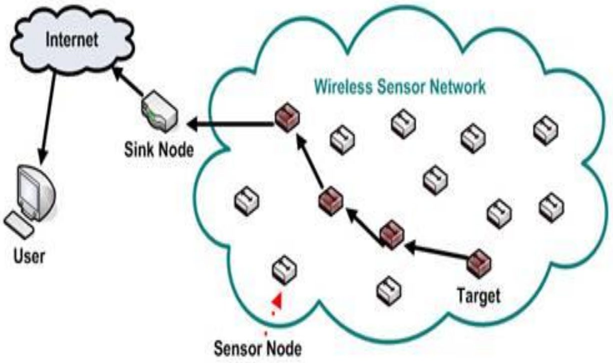

Fig1. An example of Wireless Sensor Network

The function of a sensor node in a sensor area is to detect events, perform local data processing, and transmit raw and/or processed data. Sink node is nothing but a base station which plays a vital role in wireless environment and it acts like a distributed controller. Base station is important for the following reasons: sensor nodes are prone to failure, better collection of data and provides the backup if the master node is failure.

4. CHALLENGES IN WSN

Wireless sensor networks have tremendous potential because they will expand our ability to monitor and interact remotely with the physical world. Sensors have the ability to collect vast amounts of unknown data.

Sensors can be accessed remotely and placed where it is impractical to deploy data and power lines. To exploit the full potential of sensor networks, we must first address the peculiar limitations of these networks and the resulting technical issues. Although data fusion requires that nodes be synchronized, the synchronization protocols for sensor networks must address the following features of these networks. WSNs to become truly ubiquitous, a number of challenges and obstacles must be overcome.

4.1 Energy

The first and often most important design challenge for a WSN is energy efficiency. Power consumption can be allocated to three functional domains: sensing, communication, and data processing, each of which requires optimization. The sensor node lifetime typically exhibits a strong dependency on battery life. The constraint most often associated with sensor network design is that sensor nodes operate with limited energy budgets.

Typically, sensors are powered through batteries, which must be either replaced or recharged when depleted. For non rechargeable batteries, a sensor node should be able to operate until either its mission time has passed or the battery can be replaced. The length of the mission time depends on the type of application.

4.2 Limited bandwidth

In wireless sensor nets, much less power is consumed in processing data than transmitting it. Presently, wireless communication is limited to a data rate in the order of 10–100 Kbits/second.

Bandwidth limitation directly affects message exchanges among sensors, and synchronization is impossible without message exchanges. Sensor networks often operate in a bandwidth and performance constrained multi-hop wireless communications medium. These wireless communications links operate in the radio, infrared, or optical range.

4.3 Node Costs

A sensor network consists of a large set of sensor nodes. It follows that the cost of an individual node is critical to the overall financial metric of the sensor network. Clearly, the cost of each sensor node has to be kept low for the global metrics to be acceptable. Depending on the application of sensor network, large number sensors might be scattered randomly over an environment, such as weather monitoring. If the overall cost was appropriate for sensor networks and it will be more acceptable and successful to users which need careful consideration.

4.4 Deployment

Node deployment is a fundamental issue to be solved in Wireless Sensor Networks. A proper node deployment scheme can reduce the complexity of problems. Deploying and managing a high number of nodes in a relatively bounded environment requires special techniques. Hundreds to thousands of sensors may be deployed in a sensor region. There are two deployment models at present: (i) static deployment (ii) dynamic deployment. The static deployment chooses the best location according to the optimization strategy, and the location of the sensor nodes has no change in the lifetime of the WSN. The dynamic deployment throws the nodes randomly for optimization.

4.5 Design Constraints

The primary goal of wireless sensor design is to create smaller, cheaper, and more efficient devices. A variety of additional challenges can affect the design of sensor nodes and wireless sensor networks. WSN have challenges on both software and hardware design models with restricted constraints.

4.6 Security

One of the challenges in WSNs is to provide high security requirements with constrained resources. Many wireless sensor networks collect sensitive information. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. The security requirements in WSNs are comprised of node authentication and data confidentiality. To identify both trustworthy and unreliable nodes from a security stand points, the deployment sensors must pass a node authentication examination by their corresponding manager nodes or cluster heads and unauthorized nodes can be isolated from WSNs during the node authentication procedure. As a consequence, sensor networks require new solutions for key establishment and distribution, node authentication, and secrecy.

5. TIME SYNCHRONIZATION

Time Synchronization is a method for successful communication between nodes on the network. TS have the ability to determine the movement, location and speed. Any distributed system requires time synchronization. It is essential for transmission scheduling, power management, data fusion and many other applications. The need of TS is, in the sensor network, sensors observe the objects movement and speed of the moving objects. Further, to accurately determine the velocity of the moving object, the time difference between sensor time stamps should correspond to the time difference of the real times.

5.1 Clock Drift and Skew

Clock drift refers to a clock does not run at the exact right speed compared to another clock. That is, after some time the clock "drifts apart" from the other clock. On the negative side, clock drift can be exploited by timing attacks. Its accuracy is limited by the stability of the interrupt requests. Any change in the interrupt request rate causes the clock to gain or lose time. Clock offset or skew is the difference between two clocks of two nodes at one point in time.

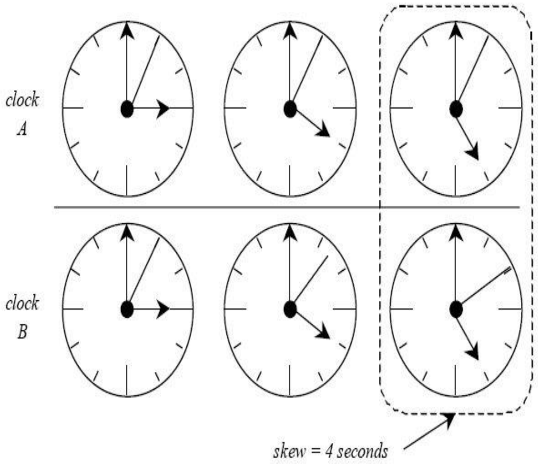

Fig2. Clock differences comparison for different days.

5.2 Synchronization Metrics

Synchronization is typically based on some sort of message exchange among sensor nodes. Synchronization metrics is a measurement of overall performance of nodes in the sensor network. To determine the performance of each node, the following metrics are involved.

Energy Efficiency — Network nodes have limited energy resources, synchronization schemes should take into account the limited energy resources contained in sensor nodes.

Scalability — In some applications, tens of thousands of sensors might be deployed. At any time numbers of nods can be increased or decreased. A synchronization scheme should scale well with increasing number of nodes and/or high density in the network.

Precision — The need for precision, or accuracy, may vary significantly depending on the specific application and the purpose of synchronization. The results of accuracy may be varying in microseconds.

Robustness — A sensor network is typically left unattended for long times of operation in possibly hostile environments. If any node in the network is break down or go out of then it does not affect the working of other nods in the network and synchronization scheme.

Lifetime — The synchronized time among sensor nodes provided by a synchronization algorithm may be instantaneous, or may last as long as the operation time of the network.

Cost and Size — Wireless sensor nodes are very small and inexpensive devices due to advanced technologies. So its results that synchronization algorithm should not have too much cost and too much large in the size.

5.3 Communication for Time Synchronization

As we mentioned earlier, sensor nodes have also been used for communication. Nodes communicate with each other through sending messages. For instance, nodes that mainly transmit their own sensor readings and nodes that mainly relay messages from other nodes.

Sensor readings are routed from the source nodes to the sink via the relay nodes, thus creating a multi-hop topology. However, single-hop communication is slightly different from multi-hop.

- Single-hop communication

A sensor node can directly communicate and exchange messages with any other sensor in the single-hop network. However, many wireless sensor network applications span several domains or neighborhoods. (Nodes within a neighborhood can communicate via single-hop message transmission.) The network is often too large, making it impossible for each sensor node to directly exchange messages with every other node.

- Multi-hop communication

The need for multi-hop communication arises due to the increase in the size of wireless sensor networks. In such settings, sensors in one domain communicate with sensors in another domain via an intermediate sensor that can relate to both domains. Communication can also occur as a sequence of hops through a chain of pair-wise adjacent sensors.

5.4 Time Synchronization through Connection - Oriented Services

In a connection- oriented service, the source makes a connection with the destination before sending the packet. When the connection is established, a sequence of packets can be sent one after another on the same path. When all packets of a message have been delivered, the connection is terminated. In short, this type of service includes three stages, connection establishment, data transfer, and connection release / termination. This service is often described as a reliable one, providing acknowledgment after every successful delivery.

There are two methods have been followed for time synchronization: (i) Network Time Protocol (NTP) and (ii) Global Positioning System (GPS). In NTP, client request to server for synchronization with the timing information. Both client and server requires accurate clock for sharing the time. GPS is generally expensive and it communicates with satellite for synchronization.

5.5 Time Synchronization through Connectionless Services

In a connectionless service, packets of a message send on different paths. The packets are treated independently and are not numbered, they may be delayed or lost or may arrive out of sequence. It can be described as an unreliable, a best effort delivery service. The term best effort means there is no provision for error checking or tracking.

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

Wireless devices are powered by batteries and sensor nodes are all inexpensive. Wireless networks are limited to size due to coverage problem. In wireless network, time relies on the ordering of messages and clock of each node is independent. Nodes are synchronized with local time of each node. Atomic clocks are impossible for wireless networks. A node saves information about its drift and offset.

6. ISSUES OF TIME SYNCHRONIZATION

Time Synchronization is an accepted key for seamless communication but it has some issues on various synchronization methods. Synchronization ensures the trustworthiness and imparts higher security to the nodes in the sensor network.

6.1 Master – Slave Synchronization

Master - slave is a form of communication where one node has unidirectional control over one or more other nodes. In some networks a master is elected from a group of nodes, with the other nodes acting in the role of slaves. The slave nodes regard the local clock reading of the master node as the reference time and try to synchronize with the master. The synchronization master sends time code information (synchronization signals) to one or more synchronization slaves.

6.2 Peer – Peer Synchronization

Peer – Peer is a direct synchronization method where a node can directly communicate with others in the sensor network. It can be simply called as point to point synchronization. This approach removes the risk of the master node failure. Therefore this kind of synchronization is more flexible but also more uncontrollable.

6.3 Internal Synchronization

Internal synchronization means that all nodes in the network are synchronized with one another, but the time is not necessarily accurate with respect to UTC (Universal Time Controller). Internal clocks may vary not only in the time they contain but also in the clock rate. Since it does not have global time, attempts to minimize the maximum difference between the readings of local clocks of the sensors.

6.4 External Synchronization

External synchronization means that all nodes in the network are synchronized with an external source of time. A standard time is available and is used as a reference time. The local clocks of sensors seek to synchronize to this reference time. The time will not vary from node to node in the network.

6.5 Probabilistic Synchronization

A probabilistic method is proposed for reading remote clocks in distributed systems subject to unbounded random

communication delays. The method can be used to improve the precision of synchronization. The approach is probabilistic because it does not guarantee that a node can always read a remote clock with an a priori specified precision. An important characteristic of the method is that, when a process succeeds in reading a remote clock, it knows the actual reading precision achieved.

6.6 Deterministic Synchronization

Deterministic to be used for synchronization in networks whose topologies may be time varying. The topology of a network may change depending on the applications. The response time of nodes change if we change its locations. This synchronization does the function of comparing the two response times i.e. before and after the change in topology.

6.7 Sender – Receiver Synchronization

The sender node periodically sends a message with its local time as a timestamp to the receiver and then the receiver synchronizes with the sender using the timestamp received from the sender.

The message delay between the sender and receiver is calculated by measuring the total round-trip time, from the time a receiver requests a timestamp until the time it actually receives a response.

6.8 Receiver – Receiver Synchronization

This method uses the property that if any two receivers receive the same message in a single-hop transmission, they receive it at approximately the same time. Receivers exchange the time at which they received the same message and compute their offset based on the difference in reception times. The merit of this approach is reduced message delay variance which is vulnerable to the propagation delay related to different receivers and the differences in receiving time.

7. CONCLUSION

The efficiency of computing and sensing technologies enables the development of tiny, low-power, and inexpensive sensors and controllers. A wireless sensor has not only a sensing component, but also capable of processing, communication, and storage. We are aware that communication poses a number of challenges in a sensor network design. An escalating distance between a sensor node and a base station rapidly increases the transmission energy. Therefore, it is more energy efficient to split a large distance into several shorter distances, leading to the challenge of supporting multi-hop communications. Multi-hop communication requires nodes in a network to cooperate with each other, to identify efficient routes and serve as relays. This challenge is further aggravated in networks to preserve energy. Time Synchronization is a tremendous area in WSN which is useful to maximize the precision of sensor nodes. Eventually, this paper will be a useful scale for researchers to work on various challenges of WSN and discover methods & techniques to overcome the issues of Time Synchronization.

REFERENCES

[1]R.Jordan, C.A.Abdallah,“Wireless Communications and Networking: An Overview,” Report, Elect. and Comp.Eng.Dept., Univ. New Mexico, 2002.

[2].K.Romer and F.Mattern,‘‘The Design Space of Wireless Sensor Networks,’’ IEEE Wireless Communications, Dec. 2004.

[3]M.A.M.Vieiraetal, ‘‘Survey on Wireless Sensor Network Devices,’’ Proceedings of IEEE Conference on Emerging Technologies and Factory Automation (ETFA’03), Sept. 16–19, 2003, pp. 537–544.

[4]I.F.Akyildiz, W.Su, Y.Sankarasubramanian, and E.Cayirci. A Survey on Sensor Networks. IEEE Communications Magazine, 40(8):102–114, Aug.2002.

[5].Waltenegus Dargie and Christian Poellabauer “Fundamentals of Wireless Sensor Networks” – Wiley Edition, 2010.

[6].M.L.Sichitiu and C.Veerarittiphan, Simple, 2003 “Accurate Time Synchronization for Wireless Sensor Networks”, IEEE Wireless Communications and Networking Conference, WCNC.

[7].K.Rhee, J.Lee, J.Kim , E.Serpedin ,and Y.Wu, 2009 “ Clock Synchronization in Wireless Sensor Networks: An Overview”, Open Access sensors ISSN 1424-8220.

[8].P.Sommer and R.Wattenhofer. Symmetric Clock Synchronization in Sensor Networks. In ACM Workshop on Real-World Wireless Sensor Networks (REALWSN), 2008.

[9].K.Arvind. Probabilistic Clock Synchronization in Distributed Systems. IEEE Transactions on Parallel and Distributed Systems, 5(5):474–487, May 1994.

[10].Fikret Sivrikaya and Bulent Yener, Time Synchronization in Sensor Networks: A Survey, IEEE Network, 18(4): Pages: 45-50, August 2004.

[28] J. Van Greunen and J. Rabaey. Lightweight Time Synchronization for Sensor Networks. Proc. 2nd ACM Int. Workshop on Wireless Sensor Networks and Applications (WSNA ’03), pp. 11–19, San Diego, California, Sept. 2003.

[29] G. Pottie and W. Kaiser. Wireless integrated network sensors. Communications of the ACM, 43(5):51–58.