Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.587 – 597

RESEARCH ARTICLE

Time Synchronization in Wireless Sensor Network

JYOTI YADAV
DEPARTMENT OF COMPUTER
SCIENCE AND ENGINEERING
GURGAON INSTITUTE OF
TECHNOLOGY AND MANAGEMENT
GURGAON
Jyotiyadav034@gmail.com

RAJESH YADAV
DEPARTMENT OF COMPUTER
SCIENCE AND ENGINEERING
GURGAON INSTITUTE OF
TECHNOLOGY AND MANAGEMENT
GURGAON
Rajeshyadav02@gmail.com

Abstract: ***Time synchronization is a basic requirement for various applications in wireless sensor network, e.g., event detection, speeds estimating, environment monitoring, data aggregation, target tracking, scheduling and sensor nodes cooperation. Time synchronization is also helpful to save energy in WSN because it provides the possibility to set nodes into the sleeping mode. In wireless sensor networks all of above applications need that all sensor nodes have a common time reference. However, most existing time synchronization protocols are likely to deteriorate or even be destroyed when the WSNs attack by malicious intruders. The recently developed maximum and minimum consensus based time synchronization protocol (MMTS) is a promising alternative as it does not depend on any reference node or network topology. But MMTS is vulnerable to message manipulation attacks. In this thesis, we focus on how to defend the MMTS protocol in wireless sensor networks under message manipulation attacks. We investigate the impact of message manipulation attacks over MMTS. Then, a novel Secured Maximum and Minimum Consensus based Time Synchronization (SMMTS) protocol is proposed to detect and invalidate message manipulation attacks.***

Keywords: wireless sensor network, time synchronization, maximum consensus, minimum consensus, message manipulation attack

1.INTRODUCTION

WIRELESS SENSOR NETWORKS:

A Wireless Sensor Networks (WSN) is a collection of small programmable devices with limited power supply and having computational and transmission capability. The wireless sensor networks were developed to fulfill the motive of military applications such as battlefield surveillance in this day these networks are used in many applications such as industrial process monitoring and control and machine health monitoring and so on.

Wireless Sensor Networks (WSNs) has become an emerging area of interest among the academia and industry in the last one decade [1]. It consists of a large number of densely deployed nodes which are tiny, low power, in-expensive, multi-functional and have limited computational and communication capabilities. These nodes interact with their environment, sense the parameters of the interest such as temperature, light, sound, humidity, and pressure; and report it to the sink node/base station. Deployment of WSN may vary from a controlled indoor environment to a remote and inaccessible area. Therefore, a sensor node is configured with necessary extra components for on-board limited processing ability, communication, and storage capabilities. A typical WSN is shown in Figure - 1.1.

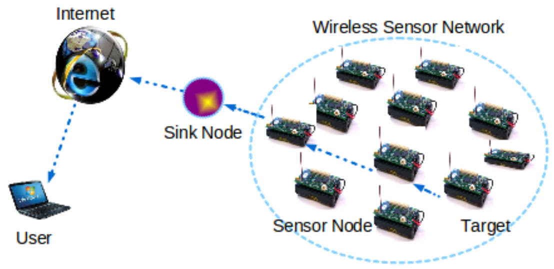

Figure 1.1: Wireless Sensor Network.

With the span of time, usage of WSN in diverse field have increased with the agile growth in micro-electromechanical systems (MEMS), very large scale integration (VLSI), low-power radios, and wireless communication protocols. Applications of WSN includes environment monitoring (e.g., habitat, geophysical monitoring), traffic management [5], military applications (e.g., surveillance and battle field monitoring) [6], health monitoring (e.g., medical sensing) [7, 8], industrial process control, context-aware computing (e.g., smart homes, remote metering), infrastructure protection (e.g., bridges, tunnels) [9] and so on. For interoperability, sensor nodes produced by different manufacturer need to follow a particular standard. Protocol stack of WSN consists of five layers:

(*i*) physical layer, (*ii*) data-link layer, (*iii*) network layer, (*iv*) transport layer, (*v*) application layer [10].

Physical and data-link layer operations are specified by the task group 4 of IEEE 802.15, accordingly named as IEEE 802.15.4. The remaining layers of WSN follow the Zig Bee standard, developed by the Zig Bee Alliance, which consists of various companies working for low-power, reliable and open global wireless networking standards focused on control, monitoring, and sensor applications.

An overview of protocol stack in WSNs and the main functions performed at each layer is shown in Figure - 1.2

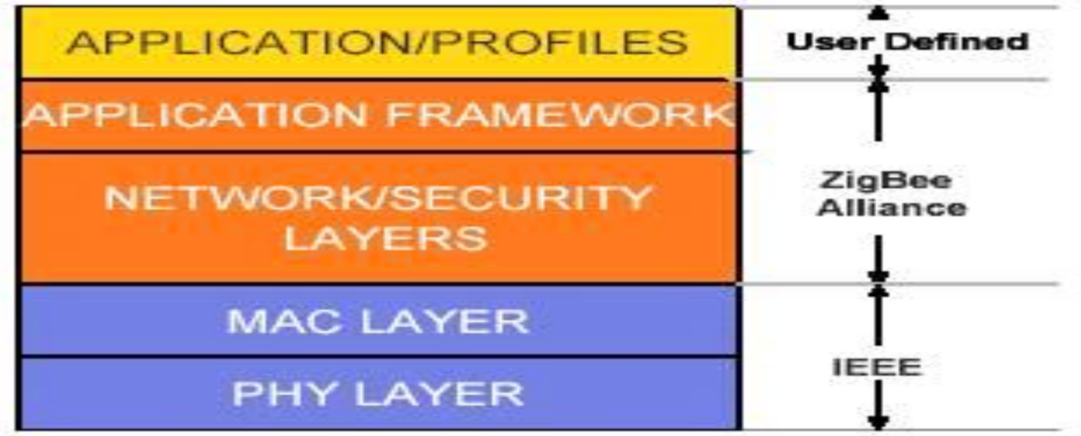

Figure 1.2: Protocol Stack Of Wireless Sensor Network.

1.1 APPLICATIONS OF SENSOR NETWORKS

At first sensor nodes were predominantly used to discover interruption in military applications. Now a day, we can't develop even a venture without WSNs. Sensor networks have been Utilized as a part of quickened movement in every field. Wireless sensor network applications are as follows:

- **Area Monitoring**: It is the most essential application of wireless sensor networks. In area monitoring wireless sensor networks is conveyed over a region where we need to watch some phenomena.
- **Health Care Monitoring**: The medical applications are of two types: implanted and wearable. Implantable medical devices are those that are embedded inside the human body. The Wearable devices are utilized on the body surface of a human or precisely at close region of the user. There are various diverse procurements exorbitantly e.g. body position estimation and location of the individual, general observing of sick patients in healing centers and at homes. Body-area network can gather data about a individual's health, fitness, and energy expenditure.
- **Air Pollution Monitoring:** Air pollution monitoring is a very important application of wireless sensor networks where by the help of sensor nodes we monitor air pollution. In air pollution monitoring WSNs have been deployed in several cities to screen the amassing of unsafe gasses for natives. These can exploit the ad hoc wireless links as opposed to wired installations, which likewise make them more versatile for testing readings in different areas.
- **Forest Fire Detection**: Since sensor nodes may be deliberately, arbitrarily, and densely deployed in a forest, sensor nodes can relay the accurate birth place of the blaze to the end clients before the flame is spread uncontrollable [1]. A huge number of sensor nodes could be conveyed and incorporated utilizing radio frequencies/optical systems. Additionally, they may be outfitted with powerful power rummaging methods [2], for example, sun powered cells, in light of the fact that the sensors may be left unattended for months and even years. The sensor nodes will work together with one another to perform conveyed sensing and overcome snags, for example, trees and shakes, that square wired sensor's observable pathway.
- **Water Quality Monitoring:** Water quality monitoring incorporates softening down water properties up dams, streams, underground water reserves and lakes & oceans. The usage of various wireless appropriated sensors enables the creation of a more correct aide of the water status, and grants the enduring course of action of checking stations in ranges of troublesome access, without the need of manual data recuperation.

- **Natural Disaster Prevention**: WSNs can sufficiently act to keep the outcomes of characteristic catastrophes, in the same way as floods [4]. Wireless nodes have effectively been conveyed in streams where movements of the water levels must be watched logically.
- **Machine Health Monitoring**: WSNs have been created for machinery condition-based backing as they offer vital cost speculation supports and enable new value. In wired structures, the establishment of enough sensors is consistently limited by the cost of wiring. Previously out of achieve regions, rotating mechanical assembly, dangerous or restricted areas, and versatile stakes can now be landed at with wireless sensors.

2.TIME SYNCHRONIZATION IN WSN

Time synchronization is a basic requirement for various applications in wireless sensor network, e.g., event detection, speed estimating, environment monitoring [5], data aggregation [6] [7] [8], target tracking, scheduling and sensor nodes cooperation. Time synchronization is helpful in saving energy in WSN because it provides the possibility to set nodes into the sleeping mode. In wireless sensor networks all of above applications need that all sensor nodes have a common time reference.

2.1 CHARACTERISTICS

Many different methods of distributed time synchronization are in common use today. Systems such as the U.S. Global Positioning System (GPS) [8] and the WWV/WWVB radio stations operated by the National Institute of Standards and Technology [2] provide references to the U.S. time and frequency standards. Network time protocols, most notably Mills' NTP [10], distribute time received from these primary sources to network-connected computers.

In studying their application to sensor networks, we have found it useful to characterize the different types of time synchronization along various axes. We consider certain metrics to be especially important:

- ***Precision*** either the dispersion among a group of peers, or maximum error with respect to an external standard.
- ***Lifetime*****:** which can range from persistent synchronization that lasts as long as the network operates, to nearly instantaneous (useful, for example, if nodes want to compare the detection time of a single event).
- ***Scope and Availability*****:** The geographic span of nodes that are synchronized, and completeness of coverage within that region.
- ***Efficiency*** the time and energy expenditures needed to achieve synchronization.
- ***Cost and Form Factor*** which can become particularly important in wireless sensor networks that involve thousands of tiny, disposable sensor nodes.

The services provided by existing time synchronization methods fall into many disparate points in this parameter space. All of them make tradeoffs no single method is optimal along all axes.

For example, consumer GPS receivers can synchronize nodes to a persistent-lifetime time standard that is Earth-wide in scope to a precision of 200ns [9]. However, GPS units often cannot be used (e.g., inside structures, underwater, during Mars exploration), can require several minutes of settling time. In some cases, GPS units might also be large, high-power and expensive compared to small sensors.

3. REASONS FOR TIME SYNCHRONIZATION

There can be distinguished different reasons to use time synchronization; the most crucial are presented below.

Cryptography

Authentication schemes frequently rely on upon synchronized time to guarantee freshness, avoiding replay attacks and other manifestation of circumvention [9].

Sleep Scheduling

One of the most significant sources of energy savings is turning off the radios of sensor devices in the situation when they are not active. It means, that without proper synchronization, such technique cannot exist and work correctly and efficiently [10].

Medium-Access

TDMA-based medium-access schemes require that nodes are synchronized. There is a need to assign distinct slots for collision-free communication.

Coordinated Signal Processing

Time stamps are needed to determine which information from different sources can be fused/aggregated within the network.

Multi-node Cooperative Communication

Multi-node cooperative communication techniques involve transmitting in-phase signals to a given receiver. Such techniques [11] have the potential to provide significant energy saving and robustness, but again, there is required synchronization, as key element of the communication process.

Mobile Object Tracking

In mobile object tracking application sensor network is sent in the range where we need to screen passing objects. At the point when an object is sensed by some node, then locating nodes record the recognizing location and the time when an item is identified. After that time data and location is sent to the aggregation node which appraises the moving trajectory of the item. In the event that time is not synchronized, then assessed trajectory of the followed item could contrast altogether from the genuine one [12] [13].

Logging and Debugging

Throughout configuration and debugging, it is regularly fundamental associate logs of numerous distinctive nodes exercises to comprehend the global system's behavior [9].

4. COMMON CHALLENGES FOR SYNCHRONIZATION METHODS

Time synchronization procedures in all networks depend upon the message, which is transfer between the nodes of that particular network. Nondeterministic nature of the system flow, for example, propagation time or physical channel access time makes the synchronization error and testing in numerous systems. When a node in the system generates a timestamp to send a substitute node for synchronization, packet carrying the timestamp will stand up to a variable measure of deferment until it accomplishes and is decoded at its arranged beneficiary. This postponement keeps the beneficiary from precisely thinking about the neighborhood tickers of the two nodes and exactly synchronizing to the sender node. In network time synchronization methods, sources of error can be decomposed into four basic components [14]:

- **Send Time:** Time used to create a message at the sender end.
- **Access Time**: Each packet confronts some deferral at the MAC layer before genuine transmission. The sources of this postponement rely on upon the MAC scheme utilized, however some regular purposes behind deferral are holding up for the channel to be idle or waiting up for the TDMA slot for transmission.
- **Propagation Time:** This is the time used in the transfer of the message between the network system interfaces of the sender and the receiver.
- **Receive Time:** This is the time required for the network system interface of the beneficiary to get the message and exchange it to the host.

LITERATURE REVIEW

Many time synchronization protocols have been proposed in the past few years, e.g. RBS [28] [29] [30], TPSN [31], FTSP [32] [33] [34] [35] [36], etc. However, most of these protocols are root-based or tree-based time synchronization protocols, which are sensitive to the dynamic network topology. Thus, in order to enhance the robustness and scalability of the protocols, consensus concept, e.g., average consensus, has been introduced to solve the time synchronization problem in WSNs recently, which is called consensus-based time synchronization [20] [37] [38] [39] [40] [41] [42] [43]. Compared with the traditional root-based or tree-based time synchronization protocols, consensus-based time synchronization protocols are fully distributed without requiring any certain reference node. Meanwhile, the consensus-based time synchronization protocols are able to simultaneously compensate both the clock offset, i.e., instantaneous clock difference, and the clock skew, i.e., clock speed, which can prolong there synchronization period and thus reducing communication and energy costs. The existing consensus based time synchronization protocols can be divided into two categories, i.e., average consensus-based [37] [21] and maximum consensus-based [20].

In RBS [28] [29] [30], at first sender node broadcast reference message and then receiver node record their local time when they received a reference broadcast. After that, they exchange the recorded time with each other.

J. Elson et al., in [28] proposed RBS protocol in which sender nodes send reference signals to their neighbors utilizing physical-layer broadcasts. A reference broadcasts does not contain an express timestamp; rather, beneficiaries utilize its entry time as a perspective for looking at their clocks. They utilize estimations from two wireless used to show that expelling the sender's non determinism from the critical path in this way result in a dramatic improvement in synchronization over using NTP, their protocol permits time to be proliferated crosswise over broadcast domains without losing the reference-broadcast property. Their protocol keeps up microsecond-level synchronization to an external timescale, for example, UTC. As NTP protocol is not suited for energy use, precision, cost, scope, and lifetime. Elson et al., in [29] proposed some configuration standard use numerous, tunable modes of synchronization; don't keep up a global timescale for the whole network; use post-facto synchronization; adjust to the application, and exploit domain knowledge.

F. Ren et al., proposed a new time synchronization protocol called Self-Correcting Time Synchronization (SCTS). This protocol converts the time synchronization problem into an online dynamic self-adjusting optimizing process. This conversion is done to make offset and drift compensation simultaneously. The SCTS protocol proposed by [30] completely misuses the inherent broadcast property of wireless channel, so the communication overhead is noticeably low. They also proposed equivalent digital PLL without a real voltage controlled oscillator to evade the additional hardware needed by a traditional PLL circuit.

The main advantage of RBS is that it removes non determinism of transmitter side, by using the idea of a time critical path. Time critical path contributes to nondeterministic synchronization errors. The disadvantage of RBS is that it requires a lot of extra message exchange to communicate the neighborhood timestamps between the nodes.

5.CONCLUSION AND FUTURE WORK

This thesis investigates time synchronization under cyber physical attacks in WSNs. By theoretical analysis and simulation results it is clear that existing Maximum and Minimum consensus based Time Synchronization (MMTS) protocol is invalid under message manipulation attacks defined in this thesis. A Secured Maximum and Minimum consensus based Time Synchronization (SMMTS) protocol is proposed to defend against message manipulation attacks. Specifically, in SMMTS, by carefully designing the hardware clock and logical clock checking processes, it will be able to detect and invalidate the potential message manipulation attacks. Meanwhile, the maximum and minimum consensus based logical clock updating process guarantees faster convergence and compensates clock skew and offset simultaneously and logical clock does not deviate more from real clock. In future we can investigate more attack on Time Synchronization Algorithm and proposed proper solution for that attack.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, \Wireless sensor networks: a survey," Computer networks, vol. 38, no. 4, pp. 393{422, 2002.

[2] A. Chandrakasan, R. Amirtharajah, S. Cho, J. Goodman, G. Konduri, J. Kulik, W. Rabiner, and A. Wang, \Design considerations for distributed microsensor systems," in Custom Integrated Circuits, 1999. Proceedings of the IEEE 1999, pp. 279{286, IEEE, 1999.

[3] P. Bonnet, J. Gehrke, and P. Seshadri, \Querying the physical world," Personal Communications, IEEE, vol. 7, no. 5, pp. 10{15, 2000.

[4] M. Castillo-E_er, D. H. Quintela, W. Moreno, R. Jordan, and W. Westho Wireless sensor networks for ash flood alerting," in Devices, Circuits and Systems, 2004. Proceedings of the Fifth IEEE International Caracas Conference on, vol. 1, pp. 142{146, IEEE, 2004.

BIOGRAPHY

Jyoti Yadav passed B .Tech in Information Technology from GCEW, GURGAON, pursuing M.Tech in Computer Science and Engineering from GITM, GURGAON. The area of research is Time Synchronization In Wireless Sensor Network