JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhancement in Energy Conserving and Securing the Data in Wireless Sensor Networks: A Comprehensive Review

Manjula G. Hegde[(1)], Dr. E. Kavitha[(2)]

[1]Research scholar, Dept. of ECE, Sir. M. Visveswaraya Institute of Technology, Bangalore, India
[2]Prof. and Head, Department of Telecommunication Engineering., Sir. M. Visveswaraya Institute of Technology, Bangalore, India.

Abstract

Wireless sensor networks (WSN) are a technology that has been demanding, emerging and popular in recent decades. Since WSN has many areas of application, it also presented the researchers with several challenges. Even though there are many energy conservation techniques available, energy conservation in the WSNs has become a very big task for designers. Security has also become a huge concern because of the inclusion of the wireless channel in the WSN. The biggest task in recent trends is to secure the data, maintaining confidentiality without hampering coverage. Therefore, a mechanism is needed to overcome all these problems in order to improve the network lifetime with energy conservation, data security, reliability, and improvement of the network lifetime. With enhancement of energy efficiency, data protection, t, and without hindering the coverage, network life time will be increased. This paper discusses the different approaches used for the above problems and also offers a brief overview of some of the protocols used to achieve protection and conservation of energy. The other researchers will further use these results to make the WSN more safe and increase energy efficiency by selecting the best mechanism.

Key words- Energy conservation. Security, challenge.

I. INTRODUCTION

The Wireless Sensor Network (WSN) is a cluster of spatially distributed and dedicated sensors designed to track physical or environmental conditions such as temperature, pressure, etc. and to systematize the data collected to a main location through the network. One of the primary objectives of wireless sensor networks is to gather knowledge from the real environment. Combined with computing power and wireless connectivity, sensing technology makes it lucrative to be used in abundance in the future[1]. The wireless sensor network (often referred to as the wireless actuator network)[2] consists of sensor nodes that range in size from shoebox size to grain dust size. WSN is independent of infrastructure, where it can be built virtually to work without the need for wired connection in any harsh environment. Military applications such as battlefield surveillance have driven the development of WSN, and today such networks are used in many industrial and consumer applications [2]. WSN is used in many indoor and outdoor applications [3]. It is very important to provide security during the transmission of data on the network [4]. In WSN, security is considered to be the most difficult task because it is very difficult to keep track of the sensor nodes or network all the time. But it needs to be secured to the maximum extent to prevent the data from being attacked by an intruder.

In wireless sensor network (WSN) research, energy efficiency has also become a major theme. The interest in energy efficiency may be due to the limitations imposed by these devices on the power used by the batteries. Because batteries are the primary energy source for these devices, they have a limited life span after which they must be recharged or discarded, so energy conservation in WSN is also a very big challenge.

WSNs form the backbone of pervasive computer applications such as military surveillance, disaster surveillance, environmental surveillance, systemic surveillance, health and safety, monitoring of wildlife and ecosystems, and precision agriculture. Deployment of sensor nodes is typically in inaccessible areas, and their lifetime is usually a major problem with limited battery power. Several methods to increase the lifespan of sensor nodes as well as sensor networks have been suggested in the literature [5-10].

Long lasting sensor nodes that could never die have been suggested in recent times [6-8]. For the lifetime of a sensor network, several meanings have been suggested; A widely accepted definition, however, is when the network deteriorates to a point where it can no longer perform its intended function [9].This could occur when any of the following instances occur: when the first sensor node dies, when a number or percentage of nodes dies, or when the network is partitioned so that there is no contact between sub-networks or when the coverage is lost.

Energy management approaches are typically employed to further prolong the lifespan of sensor nodes and networks. In this, attempts are made to reduce the unit's consumed electricity. Under the three major headings: task cycling, data oriented, and mobility-driven strategies, the authors in [3] narrowly categorized energy saving schemes. As the node's radio waits in vain for frames and overhears when nodes remain active listening to uninterested frames, Duty cycling helps to eliminate idle listening. Data-driven strategies make decisions to minimize energy consumption during communication using certain data parameters themselves, while mobility schemes regard the mobility of the sink or relay nodes as a factor influencing the energy consumed in the network.

The architecture of a typical wireless sensor node is shown in Figure 1. Each of the sensor node components is presented as shown in the MicaZ mote. As can be seen, four main components, a sensing unit, a processing unit, a communications unit, and a power unit would make up a typical node. The communications device, which requires data transmission, accounts for a considerably greater proportion of the various components. A significantly high portion of energy expends for both transmission and reception [11]. In order to extend the life time of the node or network, various methods have been implemented. One of the new techniques is to move the energy from the energy-rich node to the one with the shortcoming. In the literature, many methods have been proposed to provide efficient energy transmission to increase the lifetime of the network [8, 13-19]. In this paper we present different energy harvesting and security related concerns and protocols.

Energy harvesting methods to energy scavenging from outside conditions, such as wind, vibration, solar, Thermal, and acoustical. Techniques used in energy harvesting transform energy from the atmosphere into electrical energy that can be used in nodes/devices for wireless sensing. Energy harvesting can be used in wireless sensor networks, To resolve the energy depletion challenge that triggers shorter node lifespan in the network and in other nodes cases of issues with the black hole [20]. To realize the promised benefits of energy harvesting, researchers need a concerted effort to resolve certain outstanding issues. The harvesting of energy does not guarantee that eternal nodes are because of the uncontrollable energy, and continuous activity due to references, making them volatile and difficult to model. Nodes in the network could be attached with energy harvesting devices, such as special scavenging machines for energy from the environmental condition for electric energy conversion.

In the case of solar energy, the panel size is directly related to the panel size and is proportional to the quantity of energy converted by the photovoltaic technique [22]. It presents a challenge when the unit for energy harvesting becomes larger than that of the node sensor. Accordingly, special energy harvesting devices can be given to scavenge energy in the network and then move them to nodes

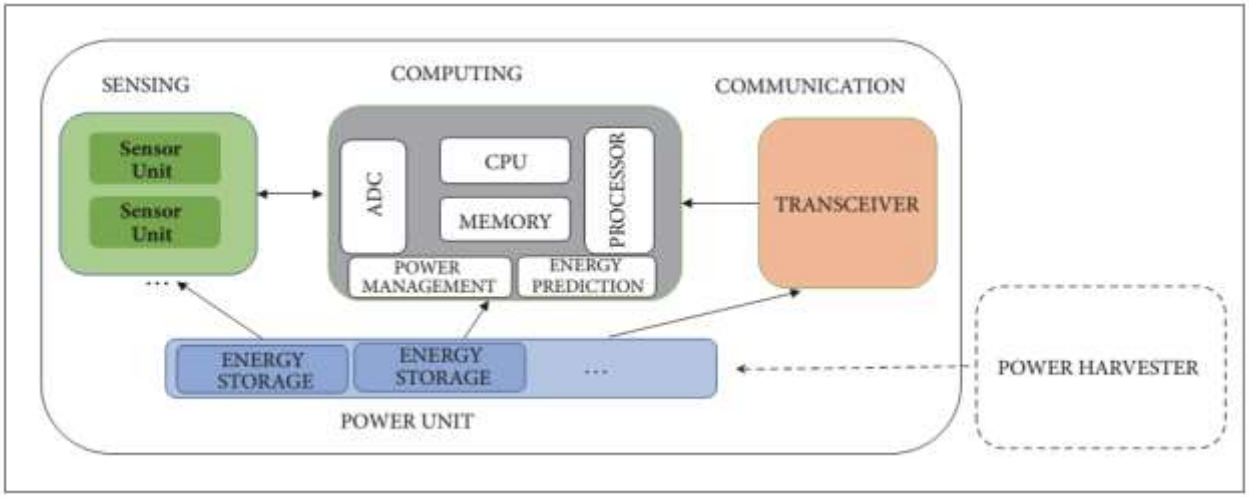

Fig 1: A typical architecture of a wireless sensor node.

II. Sources of Energy Harvesting:

As it specifies the amount of energy available to the network and the rate of conversion from the source to electrical energy, the source from which energy is harvested in a sensor network is a valuable resource. Energy harvested can be listed as ambient sources available in the environment and as human sources. Solar, vibration, thermal, and radio frequency are ambient sources of energy discussed.

2.1 Solar Energy Harvesting:

Given its abundance in the world, solar energy is an incredible and renewable source of energy. The effect is seen as a probable choice for energy harvesting sensor nodes [12, 23, 24]. With its abundance, there are also times of the day when there will be no solar available; thus Energy storage is required to manage the energy balance depending on the energy stored at the sensor node's consumption rate. In [21], when solar operation is used, an energy neutral operation the only source of energy was energy, and the sensor node was It doesn't have a battery. When a solar cell is collected, solar energy with enough energy, it receives sunlight. Depending on the quantity of energy produced from a normal solar system, about the sum of illumination and the area of the surface with power conversion efficiencies of 15% to 25%, solar cells.

2.2 Vibration Energy Harvesting:

Vibrational energy can be obtained from activities such as subways, industrial machinery, and automobiles that generate sufficient vibrations. Quantity of energy extracted is approximated in 100-W range. These use mechanical-to-electrical energy generators (MEEG). MEEG uses piezoelectric and magnetostrictive materials, and electrostatic or electromagnetic mechanisms to harvest energy [25,26]. The extracted energy is directly proportional to the size of the used MEEG. In networks of sensors where the smaller node size is a necessity, there may not be vibration is the best alternative.

2.3 Thermal Energy harvesting:

Thermal energy is dependent on the presence of a difference in temperature within an environment. Thermal energy harvesting has found application in many areas including use in devices attached to the body and implantable devices such as pacemakers for the heart. It is possible to envisage their use in other applications for tracking, where necessary.

There is a temperature distinction. A thermal energy harvester capable of achieving an output of 100 µW was reported in [27].

2.4 Radio frequency Energy Harvesting

It is very desirable to extract energy from this source, given the large number of radio transmitters available in any urban area. There will be very limited power requirements for those devices capable of using extracted RF resources. In addition, they must be in near proximity to the source of the energy or have a very large energy collection antenna. Advances in the use of RF sources will require improvement.

Power specifications for wireless node sensors of the Any RF systems that exist but are not Bluetooth, Wi-Fi technology and Ultra-Wideband are designed for WSN use (UWB IEEE 802.15.3). In contrast to Wi-Fi and Bluetooth, UWB has a higher speed ratio with lower power consumption, but is restricted to communications within a short range.

III. SECURITY THREATS AND ISSUES IN WSN

3.1WSNs are vulnerable to security attacks. Furthermore, WSNs have an additional vulnerability because nodes are often deployed in a hostile or dangerous environment where they are not physically protected [29]. Basically the attacks are classified into two types, according to the interruption of communication act. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack [28]. This attack obtains the data exchanged in the network without interrupting the communication. The attacks against privacy are passive in nature [29]. The passive attack does the following function:

- Attacker is similar to a normal node and gathers information from WSN
- Monitoring and eavesdropping from communication channel by unauthorized attackers

The unauthorized attacker monitors, listens to and modifies the data stream in the communication channel are known as active attack [28]. This kind of attacker performs the following operations:

- Injecting fault data into the WSN
- Impersonating
- Packet modification
- Unauthorized access, monitor, eavesdrop and modify resources and data stream
- Overloading the WSN

IV. SECURITY MECHANISM IN WSN

Security mechanism is actually used to detect, prevent and recover from the security attacks [29]. Some of the key mechanism (discussed in below sections) is essential before developing the intrusion detection system. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high-level (secure group management, intrusion detection, secure data aggregation) and low-level mechanism (key establishment, secrecy, privacy, secure routing and resilience to node capture) [29].

A. Key establishment and trust setup

Cryptographic key establishment is chief concern in setting up the sensor network. This technique need to scale to networks with hundreds or thousands of nodes. Security can be achieved in sensor network by encrypting the message.

B. Secrecy and authentication

Most of attacks like eavesdropping, injection of false node and modification of packets can be prevented by using cryptography technique. Cryptography provides high level of security but requires that keys be set up among all the end points and be incompatible with passive participation and local broadcast [29].

C. Privacy

WSNs must potency privacy. Initially sensor network are deployed for legitimate purpose might subsequently be used in unanticipated ways, providing awareness of the presence of sensor nodes and data acquisition is particularly important [29].

D. Secure routing

Routing and data forwarding is a crucial service for enabling communication in sensor networks, unfortunately, current routing protocols suffer from many security vulnerabilities [29].

E. Resilience to node capture

Most of the time the sensor nodes are placed in the application that are easily accessible to adversary, such exposure raises a possibility that an attacker might capture sensor nodes, extract cryptographic secrets, modify their programming or replace them with malicious node under the control of an attacker [29].

F. Secure group management

Each and every node in WSN is limited in its computing and communication capabilities, however interesting in-network data aggregation and analysis can be performed by group of nodes [6]. Consequently secure protocols are required for group management, securely admitting new group member and supporting secure group communication [6]. The outcome of the group key computation is normally transmitted to a base station; the output must be authenticated to ensure it comes from the valid group [29].

G .Secure data aggregation

Depending on the architecture of the WSNs, aggregation may take place in many places in the network; all the aggregation locations must be secure. The data from the group of sensor nodes are aggregated and sent to the sink node.

V. SECURITY REQUIREMENTS

Cryptography could be a basic technique to attain the safety in a very network. This establishes a secure relationship between two end points. In this, sender encrypts the first data and receiver decrypts the received data to get an artless data. Different types of keys are employed in the method of cryptography. the varied protocols [30] that are proposed by different authors for solving the safety issue in WSN are:

a) SPINs:

SPIN (Sensor Protocols for Information via Negotiation) protocol works in three steps. First, a node advertises the ADV packet containing the metadata. If the received node is interested in the information then it sends the request for data using REQ packet. Finally, the advertiser node after receiving request sends the info packet to the requestor node. It performs best in small size networks due to its efficiency and high latency properties . Typical SPIN consists of two secure building blocks named as μTESLA (Timed Efficient Stream Loss-tolerant Authentication) and SNEP (Sensor Network Encryption Protocol). SNEP provides confidentiality, authentication and integrity. It uses the concept of encryption. To authenticate the info, MAC (Message authentication Code) is employed. It adds 8 bytes to the message [30]. to cut back the communication overhead, SNEP uses a shared counter between sender node and receiver node. After each block counter gets incremented. Counter helps in identifying the freshness of information. In TESLA, digital signatures are accustomed authenticate the information packet. Sink node computes a MAC on the packet after receiving the packet with the key to send an authenticated packet back to source. After receiving a packet, node confirms that the sink doesn't disclose the computed MAC key to other nodes. With this, receiving node assures that data packet is original and no alterations are tired the packet.

b) LEAP

LEAP (Localized Encryption and Authentication Protocol) may be a protocol with key management scheme that's very efficient with its security mechanisms used for giant scale distributed sensor networks. It generally supports for inside network processing like data aggregation. In-network processing results in reduction of the energy consumption in network. To provide the confidentiality and authentication to the information packet, LEAP uses multiple keys mechanism. for every node four keys are used called individual, pair wise, cluster and group key. [13] All are symmetric keys and use as follows: x Individual Key: it's the unique key used for the communication between source node and also the sink node. x Pair wise Key: it's shared with another sensor nodes. x Cluster Key: it's used for locally broadcast messages and shares it between the node and everyone its surrounding neighbouring nodes. x Group Key: globally shared key utilized by all the network nodes These keys also can be employed by other non-secured protocols to increase the network security. LEAP is satisfies several security and performance requirements of WSN. LEAP is employed to defend against HELLO Floods Attack, Sybil Attack and Wormhole Attack [30].

c) TINYSEC

TINYSEC is link layer security architecture for WSNs. It is a lightweight protocol. It supports integrity, confidentiality and authentication. to realize confidentiality, encryption is finished by using CBC (Cipher-block chaining) mode with cipher text stealing, and authentication is completed using CBC-MAC [30]. No counters are employed in TINYSEC. Hence, it doesn't check the data freshness. Authorized senders and receivers share a secret key to compute a MAC. TINYSEC has two different security options. One is for authenticated and encrypted messages (TinySec-AE) and another is for authenticated messages (TinySec-Auth). In TinySec-AE, the information payload is encrypted and the received data packet is authenticated with a MAC. In TinySec-Auth mode, the whole packet is authenticated with a MAC, but on the opposite hand the information payload isn't encrypted.

VI.CONCLUSION

The WSNs continue to grow and become widely used in many applications even today. So security plays vital role . However WSN suffers from many constraints like limited energy, processing capability, storage capability, as well as unreliable communication and unattended operation, etc. Providing an appropriate security method to sensor node is fundamental aim in WSN. Most of the attacks are caused by the insertion of false information Security has become the major issue in providing confidentiality to data in the network. In this paper, We have discussed about various the threats and vulnerabilities to WSNs. And we have also discussed about the different energy conserving techniques so that the network lifetime is increased without even losing the data and also without hampering the coverage of the network. A better security and energy conserving protocol must be used for better functionality of sensor network.

REFERENCES

[1] Vikash Kumar, Anshu Jain and P N Barwal, "wireless sensor networks: security issues, challenges and solutions", IJICT, Vol. 4, 2014.

[2] https://en.wikipedia.org/wiki/Wirelessensornetwork issues

[3] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella,"Energy conservation in wireless sensor networks: a survey," *AdHoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.
[4] 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.
[5] L. J. Chien, M. Drieberg, P. Sebastian, and L. H. Hiung, "A simple solar energy harvester for wireless sensor networks," in *Proceedings of the 6th International Conference on Intelligent and Advanced Systems (ICIAS '16)*, pp. 1–6, August 2016.
[6] S. Soro and W. B. Heinzelman, "Prolonging the lifetime of wireless sensor networks via nequal clustering," in *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS '05)*, pp. 236–243, Washington, DC, USA, April 2005.
[7] L. Xie, Y. Shi, Y. T. Hou, and A. Lou, "Wireless power transfer and applications to sensor networks," *IEEE Wireless Communications Magazine*, vol. 20, no. 4, pp. 140–145, 2013.

[8] T. Rault, A. Bouabdallah, and Y. Challal, "Energy efciency in wireless sensor networks: a top-down survey," *Computer Networks*, vol. 67, pp. 104–122, 2014.

[9] Y. Chen and Q. Zhao, "On the lifetime of wireless sensor networks," *IEEE Communications Letters*, vol. 9, no. 11, pp. 976–978, 2005.
[10] I. Dietrich and F. Dressler, "On the lifetime of wireless sensor networks," *ACM Transactions n Sensor Networks*, vol. 5, no. 1,article 5, 2009.

[11] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.

[12] F. K. Shaikh and S. Zeadally, "Energy harvesting in wireless sensor networks: a omprehensive review," *Renewable & Sustainable Energy Reviews*, vol. 55, pp. 1041–1054, 2016.
[13] M. Y. Naderi, K. R. Chowdhury, S. Basagni, W. Heinzelman, S.De, and S. Jana, Experimental study of concurrent data and wireless energy transfer for sensor networks," in *Proceedings of the IEEEGlobalCommunications Conference (GLOBECOM '14)*,pp. 2543–2549, December 2014.
[14] R. J. M. Vullers, R. V. Schaijk, H. J. Visser, J. Penders, and C. Hoof, "Energy harvesting for autonomous wireless sensor networks," *IEEE Journal of Solid-State Circuits*, vol. 2, no. 2, pp.

[15] R. Du, C. Fischione, and M. Xiao, "Joint node deployment and wireless energy transfer scheduling for immortal sensor networks," in *Proceedings of the 15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '17)*, pp. 1–8, Paris, France, May 2017.
[16] L. Xie, Y. Shi, Y. T. Hou, and H. D. Sherali, "Making sensor networks immortal: an energy-renewal approach with wireless power transfer," *IEEE/ACM Transactions on Networking*, vol. 20, no. 6, pp. 1748–1761, 2012.
[17] L. Xie, Y. Shi, Y. T. Hou, W. Lou, H. D. Sherali, and S. F. Midkif, "On renewable sensor networks with wireless energy transfer: the multi-node case," in *Proceedings of the 9th Annual IEEE CommunicationsSocietyConferenceonSensor,MeshandAdHoc Communications and Networks (SECON '12)*, pp. 10–18, June 2012.
[18] C. Zhu, K. Liu, C. Yu, R. Ma, and H. Cheng, "Simulation and experimental analysis on Wireless energy transfer based on magnetic resonances," in *Proceedings of the Vehicle Power and Propulsion Conference (VPPC '08)*, pp. 1–4, 2008.
[19] M. K. Watfa, H. AlHassanieh, and S. Selman, "Multi-hop wireless energy transfer in WSNs," *IEEE Communications Letters*, vol. 15, no. 12, pp. 1275–1277, 2011.

[20] E. Ever, R. Luchmun, L. Mostarda, A. Navarra, and P. Shah, "UHEED: an unequal clustering algorithm for wireless sensor networks," in *Proceedings of the 1st International Conference on Sensor Networks (SENSORNETS '12)*, pp. 185–193, February 2012.
[21] A. Kansal, J. Hsu, S. Zahedi, and M. B. Srivastava, "Power management in energy harvesting sensor networks," *ACM Transactions on Embedded Computing Systems*, vol. 6, no. 4, article 32, 2007.

[22] F. Akhtar and M. H. Rehmani, "Energy replenishment using renewable and traditional energy resources for sustainable wireless sensor networks: a review," *Renewable & Sustainable Energy Reviews*, vol. 45, pp. 769–784, 2015.
[23] P. T. V. Bhuvaneswari, R. Balakumar, V. Vaidehi, and P. Balamuralidhar, "Solar energy harvesting for wireless sensor networks," in *Proceedings of the 1st International Conference on Computational Intelligence, Communication Systems and Networks (CICSYN '09)*, pp. 57–61, July 2009.
[24] T. J. Kazmierski and S. Beeby, *Energy Harvesting Systems*, Springer, 2014.
[25] C. O. Math´ ´ una, T. O'Donnell, R. V. Martinez-Catala, J. Rohan, and B. O'Flynn, "Energy scavenging for long-term deployable wireless sensor networks," *Talanta*, vol. 75, no. 3, pp. 613–623, 2008.
[26] S. Roundy, P. K. Wright, and J. M. Rabaey, "Energy scavenging for wireless sensor etworks," *Norwell*, 2003.
[27] I. Stark, "Invitedtalk: Termal energy harvesting with thermo life," in *Proceedings of the International Workshop Wearable and Implantable Body Sensor Networks (BSN '06)*, pp. 19–22, 2006.

[28] Vikash Kumar, Anshu Jain and P N Barwal, "wireless sensor networks: security issues, challenges and solutions", IJICT, Vol. 4, 2014.

[29] Yogesh Kumar, Rajiv Munjal, Krishan Kumar, "Wireless Sensor Networks and Security Challenges", IJCA, 2011.

[30] Yogesh Kumar, Rajiv Munjal, Krishan Kumar, "Wireless Sensor Networks and Security Challenges", IJCA, 2011.