INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A STUDY ON WIRELESS SENSOR NETWORK AND SECURITY USING DATA AGGREGATION

C.Nagarani[1], V.Kamakshi[2]
[1]*Assistant Professor, Dept of CS, PSG college of Arts and Science, Coimbatore, Tamilnadu, India*
E-Mail: idnandhu_govi@yahoo.co.in
[2] *Research scholar, Dept of CS, PSG college of Arts and Science, Coimbatore, Tamilnadu, India*
E-Mail:pmkamakshi@gmail.com

Abstract
A wireless sensor network (**WSN**) represents in its simplest form and it consists of sensor nodes with sensing and communication capabilities, the information gathered from the monitored field through wireless links nodes; the data is forwarded, through multiple hops relaying, to a sink that can use it locally, or is connected to other networks through a gateway. WSN nodes must have meet requirements of autonomy, low power consumption, low cost and robustness. Data aggregation is an efficient approach for wireless sensor networks to save energy and extend network lifetime. Cluster-based data aggregation algorithms are most fashionable algorithm because it has more merits such as high flexibility and reliability. The main aim of data aggregation algorithms is to get together and aggregate data in an energy efficient manner so that network lifetime is improved. In this paper, presents a survey of data aggregation algorithms in wireless sensor networks.

Keywords*:* wireless sensor network, Data aggregation, Cluster,

1. Introduction

Sensor networks are used to monitor and control the smart environments, whether like buildings, utilities, industrial, home, shipboard, transportation systems automation, or elsewhere e.g. aircraft, and have self-organizing capabilities. Many current WSN solutions are developed with simplifying assumptions about wireless communication and the environment, even though the realities of wireless communication and environmental sensing are well known. Many of these solutions work very well in simulation. It is either unknown how the solutions work in the real world or they can be shown to work poorly in practice. We note that, n general, there is an excellent understanding of both the theoretical and practical issues related to wireless communication. For example, it is well known how the signal strength drops over distance.

Effects of signal reflection, scattering and fading are understood. However, when building an actual WSN, many specific system, application, and cost issues also affect the communication properties of the system. Radio communication in the form of AM or FM broadcast from towers performs quite differently than short range, low power wireless found in self-organizing WSNs. Of course, while the same basic principles apply, the system performance characteristics vary considerably. In other words, the size, power, cost constraints and their tradeoffs are fundamental constraints. In the current state of the art, the tradeoff among these constraints has produced a number of devices currently being used in WSNs. In such applications, running wires or cabling is usually impractical.

A sensor network is required that is fast and easy to install and maintain. Engineers have created WSN applications for areas including health care, utilities, and remote monitoring. In health care, wireless devices

make less invasive patient monitoring and health care possible. For utilities such as the electricity grid, streetlights, and water municipals, wireless sensors offer a lower-cost method for collecting system health data to reduce energy usage and better manage resources.

Remote monitoring covers a wide range of applications where wireless systems can complement wired systems by reducing wiring costs and allowing new types of measurement applications. Remote monitoring applications include:

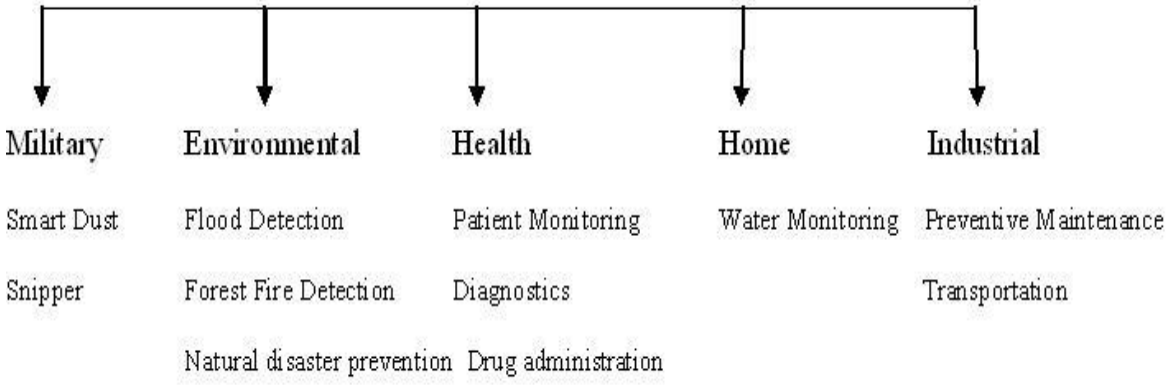


Fig 1. Wireless Sensor Network Applications

Sensor networks are characterized by limited energy, processing power, and bandwidth capabilities. These limitations become particularly critical in the case of event-based sensor networks where multiple collocated nodes are likely to notify the sink about the same event, at almost the same time. The propagation of redundant highly correlated data is costly in terms of system performance, and results in energy depletion, network overloading, and congestion. Data aggregation is regarded as an effective technique to reduce energy consumption and prevent congestion.

2. Wireless Sensor Network Issues

WSN deals with real world environments. In many cases, sensor data must be delivered within time constraints so that appropriate observations can be made or actions taken. Very few results exist to date regarding meeting real-time requirements in WSN.This issue becomes especially important in case of event-based applications, where sensors monitor a given phenomenon and send notifications and measurements back to one or more sink nodes. A significant amount of redundant data is likely delivered to the sink(s), particularly in case of dense networks, thus, wasting precious bandwidth and energy resources. Also, due to the so-called *funnelling effect* [2], the closer a node is to the destination (i.e., the sink), the more demands are made on its energy resources and the higher is the traffic it has to manage and relay. For this reason aggregation in sensor networks is regarded as an effective technique to reduce energy consumption ([3], [4]) as well as preventing congestion [5].

When performing aggregation, usually the cost of processing is disregarded. Instead, this could contribute to make the aggregation process even more costly than no-aggregation. Also one can expect that, the higher the number of packets aggregated, the higher the advantage of using aggregation with respect to not using it. However, aggregation cannot be increased indefinitely unless precious information is lost from the system. And attention should be paid to metrics used to fuse data together, thus avoiding weighing multiple times the same readings leading to unreliable estimates at the sink(s). To make aggregation more efficient, in case of event based applications, spatial correlation of data monitored by nodes in close proximity can be used [6].

2.1 Attacks on Sensor Networks

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often

placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks. [9]

A. Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

- **Attacks against Privacy**

  The main privacy problem is not that sensor networks enable the collection of information. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks [8] against sensor privacy are:

- **Monitor and Eavesdropping:**

  When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

- **Traffic Analysis**:

  Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns.

- **Camouflage Adversaries**:

  One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

B. Active Attacks

The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature. Routing Attacks in Sensor Networks, Denial of Service Attacks, Node Subversion, Node Malfunction, Node Outage, Physical Attacks, Message Corruption, False Node, Node Replication Attacks, Passive Information Gathering etc.

2.2 Security Requirements

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks.

2.2.1 Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following [7]:

- A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

2.2.2 Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

2.2.3 Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

2.2.4 Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:
Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.

- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

2.2.5 Self Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well.

2.2.6 Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair-wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc.

2.2.7 Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc.

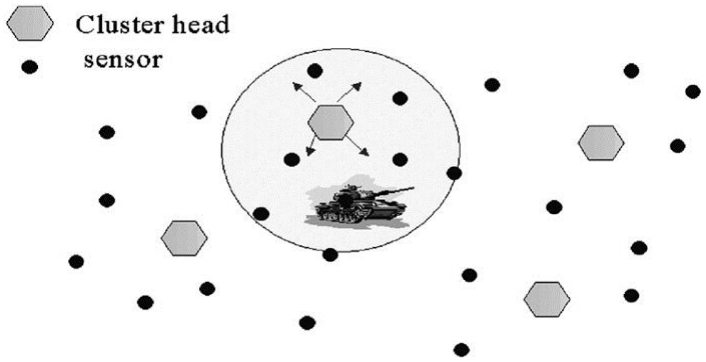
2.2.8 Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks. From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

2.3 Clustering for Data Aggregation

Serious security threat is originated by node capture attacks in hierarchical information aggregation wherever a hacker achieves full management over a sensing element node through direct physical access in wireless sensing element networks. It makes a high risk of knowledge confidentiality. Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station. The main goal of data-aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Data aggregation helps in improving the performance of the wireless sensor network protocols especially the routing protocols which in turn improve the overall performance of the network.WSNs have many constraints including energy, redundant data, and many-to-one flows.

Data aggregation is one of the most important issues for achieving energy-efficiency in wireless sensor networks. Sensor nodes in the surrounding region of an event may generate redundant sensed data. A data aggregation technique in WSNs focuses on decreasing the energy consumption by reducing the amount of data that needed to be sent to the sink node.



3. Conclusion

In this paper, we present a brief survey on wireless sensor network, its characteristics, and applications. Then we discussed about the security in sensor networks, security issues and Issues, Attacks and Data aggregation. Security is an important requirement and complicates adequate to set up in different domains of WSN.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Comm. Magazine*, vol. 40,no. 8, Aug. 2002.

[2] G. Ahn, S. G. Hong, E. Miluzzo, A. T. Campbell, and F. Cuomo, “Funneling-MAC: a localized, sink-oriented MAC for boosting fidelity in sensor networks,” *ACM Sensys 2006, Boulder, CO*, Nov. 2006.

[3] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidenmann, and F. Siva, “Directed diffusion for wireless sensor networking,” *ACM/IEEE Trans. on Netw.*, vol. 11, no. 1, Feb. 2002.

[4] A. Boulis, S. Ganeriwal, and M. Srivastava, “Aggregation in sensor networks: an energy-accuracy tradeoff,” *IEEE SNPA 2003, Ankorage, AL*, May 2003.

[5] L. Galluccio, A. T. Campbell, and S. Palazzo, “Concert: aggregation-based congestion control for sensor networks,” *ACM Sensys, San Diego, CA*, Nov. 2005.

[6] Galluccio, Laura, Sergio Palazzo, and Andrew T. Campbell. "Efficient data aggregation in wireless sensor networks: an entropy-driven analysis." *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*. IEEE, 2008.

[7] Jain, Manoj Kumar. "Wireless sensor networks: Security issues and challenges." *International Journal of Computer and Information Technology* 2.1 (2011): 62-67.

[8] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. “Security for sensor networks”. In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002.

[9] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002.
[10] Rajagopalan, Ramesh, and Pramod K. Varshney. "Data aggregation techniques in sensor networks: A survey."

[11] Bhattacharya, Rina. "A Comparative Study Of Physical Attacks On Wireless Sensor Networks." *International Journal Of Research in Engineering And Technology* 2.1 (2013).
[12] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi, Sareh Beheshti, **"**A Survey on Wireless Sensor Networks Security", SETIT 2007, *4th International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications*, March 25-29, 2007 – TUNISIA
[13] Bhattacharya, Rina. "A Comparative Study Of Physical Attacks On Wireless Sensor Networks." *International Journal Of Research in Engineering And Technology* 2.1 (2013).