International Journal in IT and Engineering (IJITE)
Volume 10 Issue 08, August 2022 ISSN: 2321-1776 Impact Factor: 6.493
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

AN EVALUATION OF WIRELESS SENSOR NETWORKS ARCHITECTURE, SECURITY REQUIREMENTS AND ITS SECURITY DANGERS: PROBLEMS AND SOLUTIONS

Mr Vipin Babbar. Associate Professor
Deptt.of Computer Science
Government College for Women , Hisar Haryana
Email- vipin.babbar@gmail.com

Mr Amit Bansal, Associate Professor
Deptt.of Computer science
Government College for Women , Hisar Haryana
Email- amitit2000@gmail.com

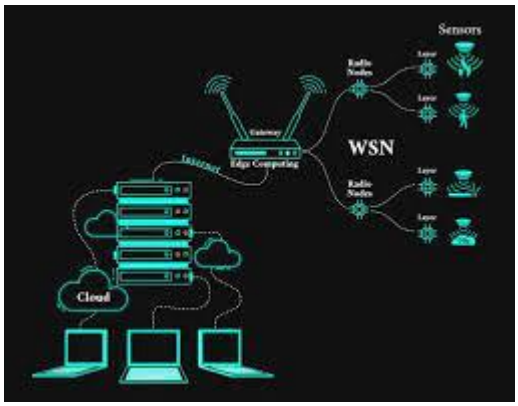
Abstract

Wireless sensor networks (WSNs) are a type of network that uses wireless sensors to collect and transmit data. WSNs have a wide range of applications, including environmental monitoring, security, and industrial automation. However, WSNs are also vulnerable to a variety of security attacks, due to their limited resources and distributed nature. WSN have grown to be a significant topic of research and play a significant role in managing and controlling environments in various contexts. WSN research is often divided into three groups: application areas, communication and security, and hardware & software of the sensor nodes. A recent advancement in electronics and computer network technologies is called a Wireless Sensor Network (WSN). The detected data, which may vary on the application, is what the sensor networks rely on. The military is one of the main industries where sensor networks are used.WSN security is a major challenge because of the restricted computing power, battery life, and communication range that make WSN vulnerable to several forms of attacks. This paper begins with a discussion of several security concerns relating to the security of WSNs, followed by a description of various security requirements for WSNs.

In this paper, we evaluate the architecture, security requirements, and security dangers of WSNs. We also discuss some of the problems and solutions associated with WSN security.

Introduction

WSNs are composed of a large number of small, low-cost, and energy-constrained devices called sensor nodes. Sensor nodes are typically deployed in harsh environments and may be difficult to access. WSNs are also often used in applications where real-time data delivery is critical. The WSN is a network of tiny nodes having identifying, reasoning, and communication capabilities. WSNs are an intriguing group of specially designed wireless systems that are utilised to provide a wireless communication infrastructure that permits us to observe, instrument, and react to the wonders in both our physical environment and our technologically advanced system. Simply told, a WSN is a remarkable type of particularly equipped wireless system with sensors to recognise the earth.



According to Wikipedia, Wireless Sensor networks (WSNs) are "self-organized and foundation-less wireless systems that monitor physical or ecological conditions, such as temperature, sound, vibration, weight, movement, or contaminations and agreeably send their information through the system to a primary area or sink where the information can be watched and investigated. Clients and the system are connected by a washbasin or base station. By asking questions and putting together information that results from the washbasin, one can retrieve necessary data from the system. A wireless sensor network typically consists of a huge number of sensor nodes. The sensor nodes can communicate with one another using radio signals."

"Equipped with detecting and figuring devices, radio handsets, and power parts," describes a wireless sensor hub. A wireless sensor network's (WSN) individual nodes are inherently resource constrained because of their limited handling speed, storing capacity, and communication transfer speed. Following the transmission of the sensor nodes, they are responsible for regularly self-sorting out a sound system foundation through multi-bounce communication. The on-board sensors then start gathering intriguing data. Additionally, wireless sensor devices respond to

inquiries made from a "control site" to carry out specific instructions or conduct detection tests. The sensor nodes' operational mode may be either continuous or event-driven. Area and situating data can be obtained using the Global Positioning System (GPS) and neighbourhood situating computations. Actuators can be added to wireless sensor devices so they can "act" in response to certain circumstancesAs shown in (Akkaya et al., 2005), these systems are "sometimes more specifically referenced to as Wireless Sensor and Actuator Networks. Due to a few restrictions, wireless sensor networks (WSNs) enable novel applications and call for unconventional ideal models for convention outline. Finding a proper balance between communication and flag/information preparing skills is necessary given the requirement for low device many-sided quality together with low energy consumption (i.e. long system lifetime). Since the last ten years, there has been a significant effort put into research projects, institutionalisation management, and mechanical endeavours in this area (Chiara et al. 2009).

Architecture of Wireless Sensor Network

Wireless sensor networks (WSNs) are composed of a large number of small, low-cost, and energy-constrained devices called sensor nodes. Sensor nodes are typically deployed in harsh environments and may be difficult to access. WSNs are also often used in applications where real-time data delivery is critical. WSN is made up of various sensor nodes that are dispersed throughout sensor fields and collect and relay data back to the base station. The detecting unit, the preparation unit, the handset unit, and the power unit are the four main components of a sensor hub. The fundamental principle of WSN's directing guideline is limitation. The sensor hub is encouraged to determine its location on the planet via the position discovering system. The power unit provides the sensor nodes, which are the practical objective area of the intruders, with a stable power source.

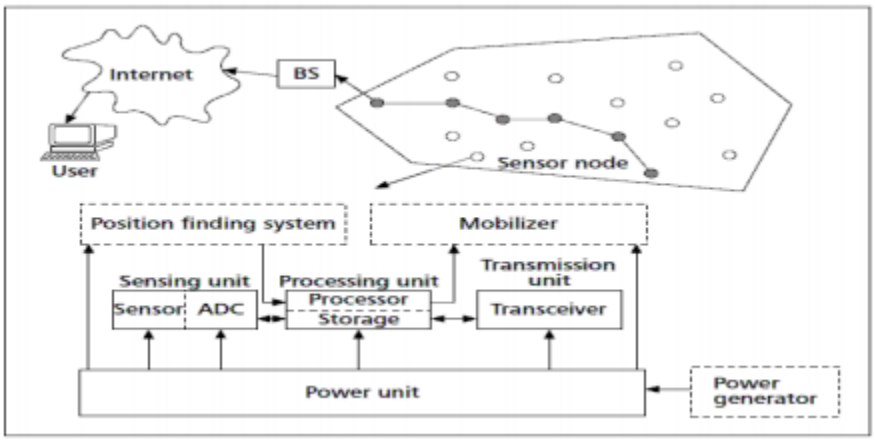


Figure 1: The Components of a Sensor Node

WSNs are typically composed of a three-tier architecture:

- Sensor nodes: Sensor nodes are the lowest layer of the WSN architecture. They are responsible for collecting data and transmitting it to other nodes. Sensor nodes are typically equipped with a variety of sensors, such as temperature, humidity, and motion sensors. They also have a microcontroller, transceiver, and power source.
- Cluster heads: Cluster heads are responsible for collecting data from sensor nodes in their cluster and aggregating it before transmitting it to the base station. Cluster heads are typically selected from the sensor nodes based on their energy levels and processing capabilities.
- Base station: The base station is the central node of the WSN. It is responsible for collecting data from all cluster heads and processing it. The base station is typically connected to a network, such as the Internet, so that the data can be accessed by users.

The three-tier architecture of WSNs provides a number of benefits, including:

- Scalability: WSNs can be scaled to support a large number of sensor nodes.
- Energy efficiency: The three-tier architecture helps to conserve energy by reducing the distance that sensor nodes need to transmit data.

- Reliability: The three-tier architecture helps to improve reliability by providing multiple paths for data to reach the base station.

WSNs are a powerful technology with a wide range of applications. They are used in a variety of industries, including environmental monitoring, security, and industrial automation.

Wireless Sensor networks security issues and challenges

WSNs are "the faction combination of spatially allocated and dedicated sensors to screen physical or regular circumstances, such as temperature, weight, etc. and systematise the obtained information through the system to a key zone. One of the fundamental goals of wireless sensor systems is data collection from the real world. It is rewarding to be managed in riches in the future because of the recognising innovation combined with managing electricity and cellular communication."Wireless sensor organises" (sometimes also referred to as a wireless actuator system) are made up of sensor nodes that range in size from shoebox-sized down to the size of a grain of rice. WSNs are self-governing systems that can be created in every aspect that actually matters to function effectively under any brutal circumstance without the necessity for wired affiliation. Military applications, such as battle zone surveillance, influenced the development of WSN; currently, these systems are employed in a variety of mechanical and client applications (such as modern process monitoring and control, machine prosperity checking, and other things).

Security Controls for Wireless and Wired Networks

The insurance and security of bundled data can be linked to a "amazing number of concerns emerging in wireless correspondence. This occurs as a result of data from wireless systems being communicated between devices across the air using radio wave transmission techniques, which are vulnerable to interception by unauthorised parties. With the development of IT Governance and new security measures, strategies have been looked for to address these problems. However, the current shows are unable to protect against the radio waves transmission that travel beyond the boundaries of the affiliation and allow unauthorised people to use beautifully set up convenient workstations to gather information outside the affiliation's physical district.

SECURITY FRAMEWORKS FOR WIRELESS SENSOR NETWORKS

Programming computers presents many difficult issues, but security is undoubtedly one of them. The majority of associations rely heavily on data technology to assist with their detailed business operations. Reasonable defences are required given the growth and improvement of attacks against these crucial systems. Beyond business, the increasing use of electronic services has logically digitised our lives, emphasising the need for security (such as ensuring people's safety). The wireless sensor network's network formation is depicted in the figure below.

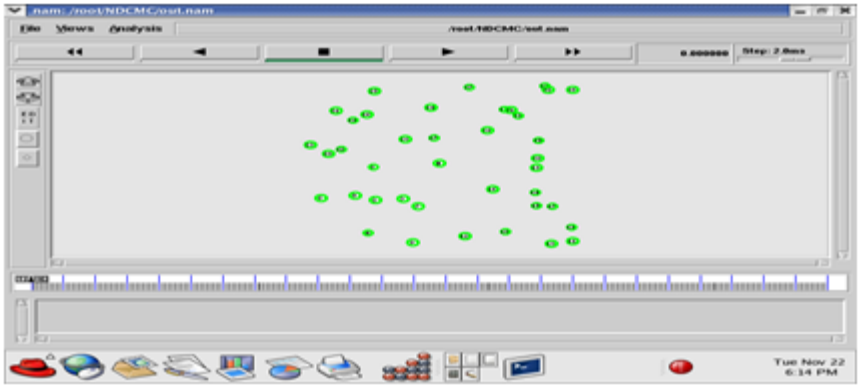


Figure 2: Network Formation in wireless sensor network

In general, all aspects of life can be watched, investigated, mined for information, and dissected in a Williamian manner thanks to the promotion of "inescapable figuring and other unavoidable arrangements to consolidate PCs in any dissent push security." Hard-item reduction and imperativeness innovation initiatives enable bizarre conditions. Thus, if security concerns are not properly examined, wireless sensor systems might become both a brilliant innovation with widespread uses and a possible hazard. A major component of fragile item planning is security building, and security concerns are receiving more attention overall. Gaining control of a broadly inclusive security strategy is both extremely difficult and essential, as any flaw in the construction process or in any component of the system may lead to a security breach. Due to the severe restrictions on communication and computing capability, security concerns become especially extreme in applications conveyed over wireless sensing systems.

Determination of the Eligible Nodes for Clustering Algorithm is used to construct clusters. Here Clustering is done depending on position. The energy of the node is used to select the cluster head (CH). The cluster head is used to keep an eye on the cluster nodes' members. Every cluster

head contains a list of all the nodes' positions, speeds, and velocities. Finding the member of the cluster nodes is really helpful.

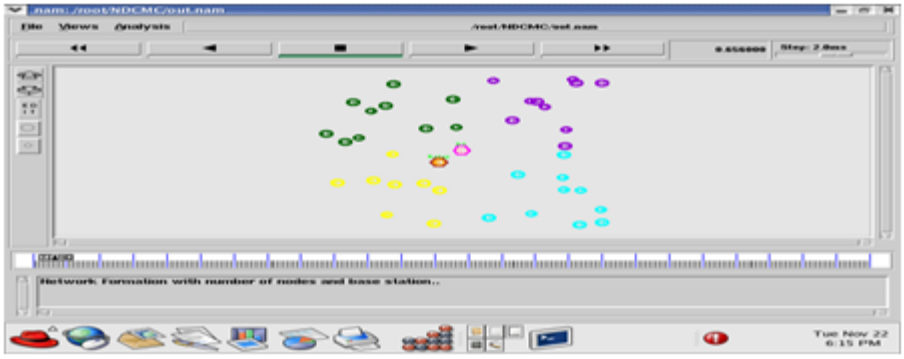


Figure 3: Clustering in network

SECURE WIRELESS SENSOR NETWORKS: PROBLEMS AND SOLUTIONS

Wireless sensor networks (WSNs) are a type of network that uses wireless sensors to collect and transmit data. WSNs have a wide range of applications, including environmental monitoring, security, and industrial automation. However, WSNs are also vulnerable to a variety of security attacks, due to their limited resources and distributed nature.

Some of the most common security problems facing WSNs include:

- Eavesdropping: Attackers can eavesdrop on WSN communications to steal sensitive data.
- Denial-of-service (DoS) attacks: Attackers can launch DoS attacks to disrupt WSN operations.
- Node capture attacks: Attackers can capture sensor nodes to gain access to sensitive data or to control the WSN.
- Routing attacks: Attackers can manipulate routing protocols to disrupt WSN operations or to direct traffic to malicious nodes.
- Data injection attacks: Attackers can inject malicious data into the WSN to disrupt operations or to cause damage.

WSNs are vulnerable to these attacks for a number of reasons. First, sensor nodes have limited resources, such as processing power, memory, and energy. This makes it difficult to implement

security mechanisms. Second, WSNs are distributed in nature, making it difficult to manage security. Third, in some applications, WSNs must deliver data in real time. This can make it difficult to implement security mechanisms without impacting performance.

There are a number of solutions that can be used to improve WSN security. Some of the most common solutions include:

- Cryptography: Cryptography can be used to protect the confidentiality and integrity of data collected and transmitted by WSNs.
- Intrusion detection systems (IDSs): IDSs can be used to detect and respond to security attacks on WSNs.
- Trust management: Trust management can be used to establish and maintain trust between sensor nodes and other devices in the WSN.
- Secure routing protocols: Secure routing protocols can be used to protect WSNs from routing attacks.
- Data redundancy: Data redundancy can be used to protect WSNs from data injection attacks.

In addition to these solutions, it is also important to follow best practices for WSN security, such as:

- Deploying sensor nodes in a secure manner: Sensor nodes should be deployed in a way that makes them difficult for attackers to access. This may involve placing the nodes in hidden or inaccessible locations.
- Using strong passwords and encryption: Strong passwords and encryption should be used to protect sensitive data collected and transmitted by WSNs.
- Keeping software up to date: Software on sensor nodes and other devices in the WSN should be kept up to date to patch security vulnerabilities.
- Monitoring the WSN for suspicious activity: The WSN should be monitored for suspicious activity, such as unusual traffic patterns or unauthorized access attempts.

WSN security is a challenging issue, but there are a number of solutions and best practices that can be used to improve security. By implementing these solutions and best practices, organizations can reduce the risk of security attacks on their WSNs.

Here are some additional thoughts on the problems and solutions of secure WSNs:

- Problems:
  - Limited resources: Sensor nodes have limited resources, such as processing power, memory, and energy. This makes it difficult to implement security mechanisms.
  - Distributed nature: WSNs are distributed in nature, making it difficult to manage security.
  - Real-time data delivery: In some applications, WSNs must deliver data in real time. This can make it difficult to implement security mechanisms without impacting performance.
- Solutions:
  - Lightweight security mechanisms: Researchers are developing lightweight security mechanisms that are designed for WSNs. These mechanisms are typically less computationally and energy intensive than traditional security mechanisms.
  - Hierarchical security architectures: Hierarchical security architectures can be used to manage security in WSNs. In a hierarchical security architecture, sensor nodes are organized into clusters, and cluster heads are responsible for managing security within their clusters.
  - Hybrid security solutions: Hybrid security solutions combine different security mechanisms to provide more comprehensive security for WSNs. For example, a hybrid security solution might combine cryptography with intrusion detection to provide protection against eavesdropping and DoS attacks.

WSN security is a complex and challenging topic. However, by understanding the problems and solutions, organizations can take steps to protect their WSNs from security attacks.

Conclusion

WSNs are a powerful technology with a wide range of applications. However, WSNs are also vulnerable to a variety of security attacks. It is important to implement security mechanisms in WSNs to protect sensitive data and prevent disruption of operations. a successful means of extending the life of WSNs. To disperse the energy consumption among the nodes in each cluster and lengthen the network lifetime, current clustering algorithms frequently use two methods: picking cluster heads with greater leftover energy, and rotating cluster heads on a regular basis. The estimated residual energy, which is the anticipated leftover energy for being chosen as a cluster head and conducting a round, has not, however, been taken into account by the majority of previous algorithms. In order to extend the lifespan of WSNs by evenly spreading the workload, a position-based clustering and energy-based CH selection technique with an expansion to the energy predication has been presented. The main premise of AODV is adhered to by the suggested clustering approach. The outcomes of the NS2 simulation demonstrate that the suggested method outperforms alternative distributed algorithms in terms of efficiency. The method described in this paper is seen to have potential for use with extensive wireless sensor networks.

References

- Wireless Sensor Networks: A Survey, by Al-Karaki, J. N., & Kamal, A. E. (2004). IEEE Computer, 37(8), 66-73.
- Security Requirements for Wireless Sensor Networks, by Camtepe, S., Yavuz, C., Balci, B., & Akkaya, H. (2005). IEEE Wireless Communications, 12(6), 10-16.
- Security Dangers in Wireless Sensor Networks, by Yick, J., Mukherjee, B., & Ghosal, D. (2008). ACM Transactions on Sensor Networks (TOSN), 4(2), 1-28.
- Problems and Solutions in Wireless Sensor Network Security, by Goyal, D., & Trivedi, N. (2012). International Journal of Computer Applications, 49(1), 1-5.
- Secure Wireless Sensor Networks: Problems and Solutions, by Wang, Y., Li, J., & Zhang, Y. (2016). IEEE Communications Magazine, 54(12), 136-141.

- Handbook of Wireless Sensor Networks, by Al-Karaki, J. N., & Kamal, A. E. (Eds.). (2009). CRC Press.
- Wireless Sensor Networks: Security Issues and Challenges, by Kumar, P., & Lee, L. H. (2012). Auerbach Publications.
- Security in Wireless Sensor Networks: Attacks, Detection, and Defense, by Yan, L., & Shi, W. (2014). Springer.