ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 9, Issue 6, June 2022

A Survey on Security in Wireless Sensor Networks

Venkateswari. P,

Research Scholar, A V S College of Technology

profvenkykarthik@gmail.com

Abstract

Wireless Sensor Networks (WSNs) are working in plentiful applications in special areas together with military, ecology, and health; for instance, to control of important information like the human assets position in a building, as a end result, WSNs need protection. However, several limitations such as low capability of calculation, small memory, incomplete resources of energy, and the untrustworthy channels employ communication in using WSNs can effect difficulty in use of security and protection in WSNs. It is especially vital to keep WSNs from malicious attacks in distant situations. Such networks require security plan due to different limitations of assets and the major characteristics of a wireless sensor network which is a significant test. Also it has various major security services provided by a system to give a precise kind of protection to system assets. It was categorized in to Authentication, Access control, Data Confidentiality, Data Integrity and Non Repudiation. Amongst these a range of security services integrity shows some extraordinary applications. In this lesson, we will describe integrity, their types, their process, execution, and uses.

Keywords: WSNs, Attacks, Malicious nodes, Security mechanisms, Cryptographic approaches

1.INTRODUCTION

A wireless sensor network (WSN) is also called a wireless sensor or wireless sensor advance network (WSAN) and is a collection of free sensors that screen physical or steady conditions, such as temperature, sound, and weight. This information is transmitted through the network to a focal area. Current networks are bi-directional and enable sensor control. Advanced WSNs have been used for military applications as battle zone affirmation. Such networks are also used in various mechanical and customer

applications for event monitoring, network status assessment, machine accomplishment sensing, etc. [1] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking.

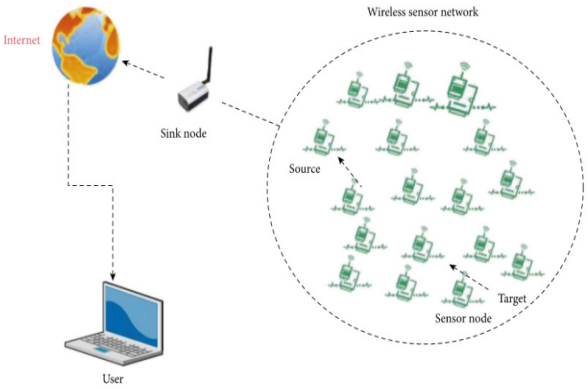

Fig 1 Wireless sensor network architecture

A security standard is one of the most important factors to consider in designing any information and networking system. The three primary dimensions of information security are confidentiality, integrity and data availability, which are known collectively as the CIA triad.

Most security attacks on WSNs are similar to those in wired networks, although WSNs are more susceptible to attack due to the deployment of sensor nodes in unprotected areas. Furthermore, WSNs used for transmission in unguided media are more vulnerable than are those for guided media. Cryptography is one of the fundamental techniques to secure data and communications. [3] discussed because of various appealing focal points, agreeable correspondences have been broadly viewed as one of the promising systems to enhance throughput and scope execution in remote interchanges. The hand-off hub (RN) assumes a key part in helpful interchanges, and RN determination may considerably influence the execution pick up in a system with agreeable media get to control (MAC).

The important factors and some of the security attacks were highlighted with an overview of security solutions to establish a secure infrastructure for WSNs. This began with the following security requirements:

- **Data Authentication:** message authentication is a critical dimension for sensor networks. This refers to the ability of each communication host to verify the other's identity.

• **Integrity:** this focuses on the correctness of the data to ensure that no changes are made by adding, altering or deleting information during the transmission.

• **Data Confidentiality:** this ensures that any message is known by the sender and receiver only. The standard approach for achieving this requires use of encryption techniques.

• **Availability:** this ensures that data is available at all times or at the time of any request. Some security attacks such as denial of service will affect data availability, but weak network designs and security mechanisms can also result in unavailability of data. Protecting availability requires avoiding a single point of failure in the design phase for any system, as well as avoiding computation-heavy algorithms that lead to energy consumption of the sensor nodes.

In the end, we present a comparison of data integrity techniques and their performance in a large network based on parameters.

3. Comparative Analysis

TABLE1:Summary of the recent research on security goals

S.No	Author &Year	Research focus	Algorithms / Protocols Developed	Outcomes
1	Sundeep Desaiand ManishaJ. Nene, (2021)	Multi-hoptrustevaluationonWSNusing Memory integrity	TEAM& TEAPalgorithms using prescriptive and experiential approaches	• It illustrates the steadiness and pliability againstnodememory tampering.
3	M. VasimBabu	IDAF-FT algorithm evaluation on clustered based techniques in	ASLPP-RR & SDA-PCA algorithm	• The overall performance of the proposedmethodologyisexpressedas20%packet

	et al., (2021)	WSN		transferrate,15% packet droprate,18% residualenergy,22% networklifetime,and10%reduction in powerconsumption comparedto the existing method. 16%
5	TanusreeChatterjee et al., 2021	Evaluation ofNamedData Networking (NDN)onWSN to improve datacentric communications.	NDN-CS, Pending Interest Table(PIT), Forward Information Base(FIB), and Light Weight One-way Cryptographic Hash Algorithm (LOCHA)	• Simulation results show that our scheme doesnotcompromise with networkperformance suchas packet loss rate, network lifetime, end-to-end delay, etc. • The results are comparedwith three competing schemesandtheresults confirm the scheme's supremacy in termsofbothdesign performance as well as network performance.
7	VipinKumar *etal*., (2021)	Evaluation of cryptographic techniques to improvescalableand storage efficientdynamic key management forWSN	Proposed SSEKMS algorithms	• It illustrates that SSEKMS is a dynamic key management system that alsosupportsthe inclusion of thenew nodeandrefreshesthe keysasper requirements.
8	S.NinishaNelsand J. Amar Pratab Singh, (2021)	Evaluation of Data aggregation inWSN	Hierarchical Fractional quantizedkernel least mean square (HFQKLMS)	•Besides,dataredundancyisattainedby broadcasting therequireddatausing datapredicted at the sink node. •Besides, the performance of the developedHFQKLMStechni

				que for dataaggregation obtained less energy consumption of 0.021 J, and a predictionerrorof7.45basedo n100
9	Yulin Tong, (2021)	Toevaluateandimproveth eenergy balanceinWSN	LEACH routing algorithm	• The results show that the improved algorithmproposedinthis paper can notonlyachievenode energybalance, butalso effectively extend the life of wireless sensor networks and strengthen theintegrity ofthe network in the working phase.
10	AseelHamoud Hamzaetal., 2021	To evaluate the environmental sustainabilityof securityin WSN	Tiny sec, SPINS, LEDS, Minisec, LEAP,MASA, Lightweight LCG, VEBEK of WSN	• It shows that the current studies on securityof WSN focuseson(secure routing, secure data aggregation, key management),security services and qualityof servicemust beall together valuated inWSNs.

4. CONCLUSION:

Of the security threats, data integrity is paramount in critical applications such as military surveillance. Due to the limitations of sensor nodes, traditional complex computational security mechanisms are not deployed in WSNs. Recently, researchers have developed new, less complex methods to ensure and improve data integrity using various cryptographic approaches. Integrity is regard as the honesty and faithfulness or correctness of one's actions. It can express the status of your data—e.g., suitable or null—or the process of ensure and preserve the power and correctness of data. Error checking and validation, for example, If your company’s data is misused or delete, and you comprise no way of deliberate how,

when and by whom, it can have a most important shock on data-driven business decisions. This is why data integrity is important. This article is a broad analysis about troubles of WSNs security, which examine in recent times by researchers and an enhanced perceptive of future guidelines for WSN security.

REFERENCES:

[1] Christo Ananth, M.Danya Priyadharshini, “A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks”, International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254).

[2] M.Kallahalla,E.Riedel,R.Swaminathan,Q.Wang,andK.Fu,Plutus:Scalablesecure file sharing on untrusted storage”,Proc. FAST, 2003, pp. 29–42.

[3] Christo Ananth, Dr. G. Arul Dalton, Dr.S.Selvakani, “An Efficient Cooperative Media Access Control Based Relay Node Selection In Wireless Networks”, International Journal of Pure and Applied Mathematics, Volume 118, No. 5, 2018,(659-668).

[4] S.S.DesaiandM.J.Nene,"Multihop Trust Evaluation Using Memory Integrity in Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security,vol.16,pp.4092-4100, 2021, doi:10.1109/TIFS.2021.3101051.

[5] Srinivasan,T.K.Ramesh,R.PaccapeliandL.Fanucci,"Functional Safety Integrity Assessment for Industrial Wireless Sensor Network Using QoS Metrics,"2021IEEE 3rd PhD Colloquiumon Ethically Driven Innovation and Technology for Society(PhDEDITS),2021, pp. 1-2, doi:10.1109/PhDEDITS53295.2021.9649625

[6] Babu, M.V., Alzubi,J.A.,Sekaran, R.etal.An Improved IDAF-FIT Clustering Based ASLPP-RR Routing with Secure Data Aggregation in Wireless Sensor Network.Mobile NetwAppl 26, 1059–1067 (2021).https://doi.org/10.1007/s11036-020-01664-7.