IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol. 9, Issue.4, April 2021 E-ISSN: 2347-2693

A Literature Survey on Security Issues in Next Gen WSN

Beant Kaur[1]*, Ramanjot Kaur[2]

[1]M.Tech (Scholar), [2]Assistant Professor

[1,2]Department of Computer Science Engineering/IT, DIET, Kharar, Punjab India

*Corresponding Author: kaurbeant71@gmail.com

DOI: https://doi.org/10.26438/ijcse/v9i4.5659 | Available online at: www.ijcseonline.org

Received: 15/Apr/2021, Accepted: 20/Apr/2021, Published: 30/Apr/2021

***Abstract*—** Next Gen WSN plays an important role in many fields like environment monitoring, transportation security, military, catastrophic area, health, medical, industry so on. However, the most noticeable feature of Next Gen WSN propagates various types of data such as text, image , videos. There are a lot of papers about Next Gen WSN and maximum papers have focused on how to save the energy of WSN. Saving energy in the form of batteries is challenging when integrating security mechanisms. For efficient secure mechanisms we conducted a survey in this paper and tried to find a solution through which we can propose an approach in which secure communication performs with low battery consumption.

***Keywords*—**WSN; Security; Authentication; Attacks, Next Gen WSN;

I. INTRODUCTION

Wireless Sensor Network is a network which is deployed in an unattended environment with small sensor nodes in large numbers for collecting the information that is impossible for human beings to reach [5]. It is very useful because they are wireless in nature and can easily gather information. Each sensor node has a capability to gather information in analog form and forward to ADC (Analog to Digital Converter) which is an internal part of the sensor node that ADC converts analog data into Digital for processing and storing. Each sensor node has four modes - transmit, receiving, sleep, idle. During transmission sensor in transmit stage and receiving sensor in receiving stage. Whereas after transmission, it goes into sleep mode to save energy and when the sensor gets weak due to limited power it gets into idle stage or dormant stage. During transmission data, energy consumed by sensors is more than during receiving data. The main work of Next Gen WSN is to gather information and that work is done by each sensor node which is deployed in the sensor field (area where sensors are deployed). In sensor field sensor nodes are deployed with different architecture, hierarchical architecture is one of them which are very popular due to energy consumption of sensor nodes. In hierarchical there are a number of routing protocols such as LEACH, PEGASIS, TEEN, APTEEN. These protocols help to collect data information from neighbour nodes.In Next Gen WSN there are a number of nodes and each node passes data to their coordinates and each coordinate pass date to their cluster head. After gathering all the data from different clusters, the cluster head aggregates the data and sends that aggregated data to the Base station.

II. ATTACKS ON WSN

There are various threats that can affect a Wireless Sensor Network, few of them are:

A. Spoofed, altered, or replayed routing information:
In this attack an attacker can create routing loops, generate false messages regarding routing updates, increase end to end delay, etc.[6]

B. Selective forwarding:
Some malicious nodes can delay or stop the transmission of messages by refusing to forward certain messages. In this case some messages are not propagated further. The malicious node can also behave like a black hole which rejects all the received messages. It will result in loss or drop of messages.[6]

C. Sinkhole attacks:
In this the attacker forces all the traffic of a specific area to pass through a compromised node.[6]

D. Sybil attacks:
In this a single node presents multiple identities to other nodes.[4]

E. Wormholes:
In this an attacker can capture messages and replays them to different nodes or in different parts by means of a tunnel.[6]

F. Replay Attack:
An attacker copies a forwarded packet and sends out the copies of the captured or intercepted traffic repeatedly

and continuously to the destination node in order to exhaust the power source i.e. battery of the node , or to base stations in order to block the communication which results in degradation of network performance.

G. Denial of service attack:

The goal of this is to make the network unavailable for the legitimate users. One common method of implementing this attack is to consume all the resources by sending a large number of false requests so that the network is not able to provide the intended services and cannot communicate with the authenticated entities in the network [6]. The most common attack in Wireless sensor networks is to flood the base station or the sink node by sending a large number of false communication requests so that it cannot communicate with registered sensor nodes which lead to the failure of tasks assigned to the network.

H. Man in Middle Attack:

The man-in-the-middle attack is a form of active attack in which the attacker establishes connections with the entities and transfers messages between them and makes the entities believe that they are communicating with each other outside a private connection. The attacker will be able to intercept all messages exchanging between the two entities and also sends new
Messages.

I. Traffic Analysis Attack:

In this the attacker node attempts to examine the traffic to know the message length, communication delay, message pattern, message encoding techniques, frequency of communication etc. Traffic analysis helps in implementing other attacks which involves violation of integrity and confidentiality of messages.

J. Acknowledgement spoofing:

The goal is to convince the sender that a dead node is still alive. All the information sent to the weak links or dead node can be removed by the attacker. [6]

K. Brute Force Attack:

A Brute Force attack is a type of password guessing attack and it consists of trying every possible code, combination, or password until you find the correct one. This type of attack may take a long time to complete. A complex password can make the time for identifying the password by brute force long.[2]

III. SECURITY REQUIREMENTS IN WSN

Following are the security requirements in WSNs

• *Availability:* It ensures the availability of the services offered by wireless sensor networks or by a single sensor node. Resources should be available whenever required. The availability of resources can be mollified by denial of service attack [6].

• *Authentication:* It ensures that the entities involved in the communication are authenticated prior to the transmission of messages. The data and information should not b e available to the unauthorized no des. Only the authorized or registered no des should b e given available resources. Sensor nodes, Base station and cluster heads should b e authenticated through a proper mechanism to avoid a number of attacks possible such as impersonation attack, man in the middle attack, information theft etc. Authentication mechanism ensures that the control information or data is originated from the correct source as well as received by authenticated node [6],[7].

• *Authorization:* It ensures that only authorized nodes are involved in the communication[9].

• *Integrity and freshness:* It ensures that the received message has not been changed i.e. the message must be received as it was sent by the source node. The message should be a fresh message. The sensor node or the base station must be capable of rejecting the replayed message. Adversary should not be able to forge the communication packet.

•*Confidentiality:* It provides privacy for wireless communication channels so that the messages are not dropped or changed by an adversary. The messages exchanged between the sensor nodes or with the base station must be kept secret. The communication information must be known to the source and the destination nodes.

•*Re-authentication:* Re Authentication must involve less communication and computational overhead than the initial authentication.

•*Untraceability:* In re-authentication of a node, source should only be able to remember the identity of the node but not direction.

•*Key Freshness:* The communicating entities should be able to verify whether the key is generated during the current session or not.

•*Node/Sink Resiliency:* If a node is compromised by an adversary it should not have any effect on the network. It is a practical threat as sensor nodes are deployed in remote areas or hostile environments.

IV. RESEARCH PAPERS

Paper I:

Shabana et al, discuss WSN security issues like major design challenges, security goals, threats and attacks (performance oriented, goal Oriented and Layer Oriented attacks) while collecting and processing data in Wireless Sensor Networks (WSNs) [9].

Paper II:
For Medical care Body area network consisting of small sensing and computing devices which collect various part of human body data and that data are are personal and should be private. To protect this privacy, such data are usually encrypted when transmitting it over a wireless link. One-time pads (OTPs) were mathematically proven to be secure and impossible to crack. In this paper, they present a concept for securing data transmission in BANs by utilizing OTPs. We delineate a system for generation, distribution, and utilization of OTPs in wireless sensor network (WSN) and BAN scenarios, and we show the implementation and evaluation of such a system[10].

Paper III:
Next Gen WSN generates large and different type of data. To handle such big data Hadoop is introduced to handle. As data from WSN collected in Base station. In-between Base Station and HDFS there is no security mechanism. To overcome this problem they used a trust based model, through which Namenode of HDFS verified that Base Station is genuine or not. This will enhance the security of the whole mechanism and make the system secured [11].

Paper IV:
WSN condition is restricted in its ability to deal with conceivably touchy data because of light security framework. Consequently, this examination has been intended to empower the office of mysterious client verification and session enter appropriation in the transmission of touchy information all the more safely by methods for correspondence matching with sensors. It also provides user anonymity on the network so that the identity of the sender or recipient cannot be verified, and proposes a secure protocol against denial-of-service attacks and spoofing attacks [12].

Paper V:
WSN comprises thousands of sensors and one base station. Sensors are conveyed in the system to monitor target zone and sense data as per the connected application at that point send this data to the base station. Enemies can infuse false data in the system or trade off the directing data between hubs or amongst hubs and base stations. Along these lines influence the remote sensor to organize secure is viewed as a critical issue. This paper introduces an authentication protocol and simple key distributed scheme between sensor nodes. Node mobility has been taken into consideration and the work proposes a re-authentication protocol that is more efficient than the initial protocol [13].

Paper VI:
This paper presents a lightweight Authentication Framework which supports node registration, entity authentication, key establishment, new node injection and broadcast authentication of messages diffusing from base towards nodes in WSN. The proposed framework is compared with other similar Schemes like Novel Access Control Protocol for secure Sensor Networks (NACP) [14].

Paper VII:
Wireless sensors arrange security and economy of aggregate vitality are two critical and essential viewpoints; node to node verification is a vital in WSN that guarantee security. This paper proposes a node to node authentication protocol with the concept of cryptography and cluster head that resolve the weakness of Diffie-Hellman key exchange scheme. The Performance of the proposed solution has been evaluated and simulated to provide a better network performance.[15]

Paper VIII:
In this paper, a low overhead encryption based security solution is proposed for node authentication. The proposed node authentication scheme at the sender side consists of three modules viz. dynamic key generation, encryption and embedding of key hint [16].

Paper IX:
IoT devices quite similar to WSN or Next Gen WSN. In order to protect the WSN, a mutual authentication between devices is required during the association of a new device. The exchanged data should be authenticated and encrypted. In this they propose a robust, lightweight and energy-efficient security protocol for the WSN systems [17].

V. CONCLUSION AND FUTURE SCOPE

Security is an extremely important aspect, whenever sensitive information is transferred between two nodes. There are a number of security protocols which protect from attackers. WSN is a collection of sensor nodes deployed on sensor fields and they communicate wirelessly, Its effect that intruders can easily destroy the sensitive information or network. To propose a secure mechanism we look at various possible attacks on WSN. There are a number of security protocols which protect from attackers. In future we will propose an approach for securing communication at every level and protecting it from attacks by attackers.

REFERENCES

[1] Akyildiz, Ian F., et al. "A survey on sensor networks." Communications magazine, IEEE 40.8 : **102-114, 2002.**
[2] Ling, Chung-Huei, et al. "A Secure and Efficient One-time Password Authentication Scheme for WSN." *International Journal of Network Security*19.2 : **177-181, 2017.**
[3] Tsuji, Takasuke, and Akihiro Shimizu. "One-time password authentication protocol against theft attacks." *IEICE transactions on communications* 87.3 : **523-529, 2004.**
[4] Arampatzis, Th, John Lygeros, and Stamatis Manesis. "A survey of applications of wireless sensors and wireless sensor networks." *Intelligent Control, 2005. Proceedings of the 2005 IEEE International Symposium on, Mediterrean Conference on Control and Automation*. IEEE, **2005.**
[5] Tsudik, Gene. "Message authentication with one-way hash functions." *INFOCOM'92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE*. IEEE, **1992.**
[6] Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A

survey of security issues in wireless sensor networks." **(2006).**

[7] Dogra, Heena, and Jyoti Kohli. "Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey." *Indian Journal of Science and Technology* 9.47 (2016).

[8] Lamport, Leslie. "Password authentication with insecure communication."*Communications of the ACM* 24.11 (1981): 770-772.

[9] SHABANA, K., FIDA, N., KHAN, F., JAN, S., REHMAN, M.. Security issues and attacks in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), North America, 5, jul. **2016.**

[10]F. Büsching and L. Wolf, "The Rebirth of One-Time Pads—Secure Data Transmission from BAN to Sink," in *IEEE Internet of Things Journal*, **vol. 2, no. 1, pp. 63-71, Feb. 2015.**

[11]V. P. Singh, M. Hussain and C. K. Raina, "Authentication of base station by HDFS using trust based model in WSN," *2016 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, **pp. 1-5, 2016.**

[12]G. W. Choi and I. Y. Lee, "A key distribution system for user authentication using pairing-based in a WSN," *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, Kuta Bali, Indonesia, 2017, pp. 1-4.

[13]S. S. Abd El dayem, M. R. M. Rizk and M. A. Mokhtar, "An efficient authentication protocol and key establishment in dynamic WSN," *2016 6th International Conference on Information Communication and Management (ICICM)*, Hatfield, 2016, pp. 178-182.

[14]A. H. Moon, U. Iqbal and G. M. Bhat, "Light weight Authentication Framework for WSN," *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, 2016, pp. 3099-3105.

[15]P. Joshi, M. Verma and P. R. Verma, "Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN," *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, Kumaracoil, 2015, pp. 527-532.

[16]P. Banerjee, T. Chatterjee and S. DasBit, "LoENA: Low-overhead encryption based node authentication in WSN," *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Kochi, 2015, pp. 2126-2132.

[17]Mohamed Hammi, Erwan Livolant, Patrick Bellot, Ahmed Serhrouchni, Pascale Minet. A Lightweight IoT Security Protocol. *1st Cyber Security in Networking Conference (CSNet2017)*, Oct 2017, Rio de Janeiro, Brazil.

[18]Armando, Alessandro, et al. "The AVISPA tool for the automated validation of internet security protocols and applications." *International conference on computer aided verification*. Springer, Berlin, Heidelberg, **2005.**

AUTHORS PROFILE

Er. Beant Kaur is presently working as a Business Analyst in a Multinational Company, India. She received the degree of Bachelor of Technology(B.Tech.) in Computer Science and Engineering from the PTU. She is presently pursuing her M.Tech in Computer Science & Technology at DIET ,Kharar, Punjab India. Her research interests include NLP, Network Security, SDN, Big Data and Computer Applications.

