iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33693

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue IV Apr 2021- Available at www.ijraset.com

Security Analysis in Wireless Sensor Networks: Challenges, Threats and Security Issues

S. Pragadeswaran[1], S. Gopinath[2], S. Keerthivasan[3], R. Premkumar[4], M. Vinoth[5]
[1, 2, 3, 4, 5]*Department of Electronics and Communication Engineering, Karpagam Institute of Technology, Coimbatore*

Abstract: ***The rise of wireless sensor networks (WSN) as a dominant technology trend in the coming decades has presented researchers with a number of specific challenges. The combination of sensing technology, computing power, and wireless connectivity makes it lucrative to be used in large quantities in the future. Incorporating wireless networking technology often introduces a number of security risks. The aim of this paper is to look at security-related problems, challenges, and strategies for securing the WSN against these security threats. Although there are numerous problems in sensor networks, this paper focuses solely on the protection of wireless sensor networks. The aim of this paper is to present the idea of a Wireless Sensor Network (WSN), as well as its components and architecture. The paper then looks into some of the big security concerns affecting wireless sensor networks (WSNs). In addition, some security goals for Wireless Sensor Networks are proposed, as well as a threat analysis of Wireless Sensor Networks. Finally, it suggests some measures against these threats.***
Keywords: Sensor, Security, Attack, Challenge, Issues, Wireless Sensor Network (WSN).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are establishing themselves as a significant new tier in the IT ecosystem as well as a burgeoning field of active research encompassing hardware and device architecture, Networking, data management, security, distributed algorithms, programming models, and social factors are some of the topics covered in this course. [1], [2], [3]. The basic principle behind a sensor network is to distribute small sensing devices, capable of sensing changes in incidents/parameters and interacting with other devices, over a specific geographic area for purposes such as target tracking, surveillance, environmental monitoring and military applications [4]. Temperature, humidity, soil makeup, vehicular activity, noise levels, lighting conditions, the presence or absence of specific items or substances, mechanical stress levels on attached objects, and other properties may all be monitored with today's sensors [5]. Wireless transceivers are used to communicate among the sensors in a wireless sensor network. The appealing characteristics of wireless sensor networks attracted a large number of researchers to work on various issues relating to these networks. Though routing strategies and wireless sensor network modeling are receiving a lot of attention, security concerns have yet to receive much attention. A description of the article is given below. It offers an overview of WSN as well as information about basic components and architecture of WSN. Then the different types of threats and attacks that can be used against a wireless sensor network. The security issues of implementing WSN are discussed. WSN's security targets and several security mechanisms for dealing with these risks are discussed. Finally, concludes the highlighted issues by outlining the study problems and potential developments in wireless sensor network security research.

II. WIRELESS SENSOR NETWORKS

A. WSN Architecture

The following network components can be found in a typical WSN: Field devices (sensor nodes) – A radio transceiver with just an internal antenna or a link to an external antenna, a microcontroller, and an electronic circuit for each sensor network node are typical components.

1) Interfacing with sensors and an energy source, which is typically a battery or a type of embedded energy harvesting.
2) *Gateways or Access Points:* A gateway is an interface that allows contact between the Host application and the field devices.
3) *Network Manager:* A Network Manager is in charge of network configuration, scheduling communication between devices (i.e., configuring super frames), routing table management, and network monitoring and reporting.
4) *Security Manager:* The Security Manager is in charge of key development, storage, and management. The WSN's base stations are one or more distinct components with significantly more computational, electricity, and communication resources. They usually forward data from the WSN to a server, serving as a portal between sensor nodes and the end user. Routers, which compute, measure, and distribute routing tables, are other unique components in routing-based networks. Mobile phone networks, satellite phones, radio modems, high-power Wi-Fi connections, and other means are used to communicate to the outside world. WSN's design is depicted in Fig.1.

©IJRASET: All Rights are Reserved

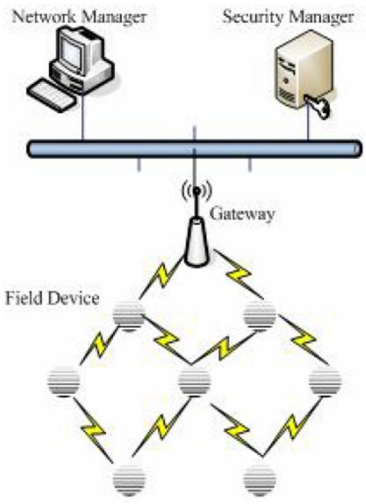


Fig.1 : Architecture of WSN

B. Operation

A WSN is a wide network of resource-constrained sensor nodes that perform multiple pre-programmed functions, such as sensing and processing, to achieve various application goals. The sensor nodes and base stations are the most critical components of a WSN. In reality, they can be thought of as the network's "sensing cells" and "brain," respectively. Sensor nodes are typically installed by an authority in a specified area and then automatically form a network via wireless communications. A deterministic scheme may be used to deploy homogeneous or heterogeneous sensor nodes at random or at pre-determined locations. The majority of the times, sensor nodes are static, while mobile nodes can be deployed according to application needs. With the network, one or more static or mobile base stations (BSs) are deployed. After being deployed, sensor nodes continue to track the network area. After an event of interest occurs, one of the sensor nodes in the area will detect it, generate a report, and send it to a BS through multihop wireless links. If several surrounding nodes are detected, collaboration can be carried out. In this case, after collaborating with the other nodes, one of them produces a final report. The BS will process the report before sending it to the outside world for further processing through high-quality wireless or wired links. The WSN authority may send commands or queries to a BS, which disseminates them across the network. As a consequence, a BS serves as a connection between the WSN and the outside world. Fig.2 illustrates an example.

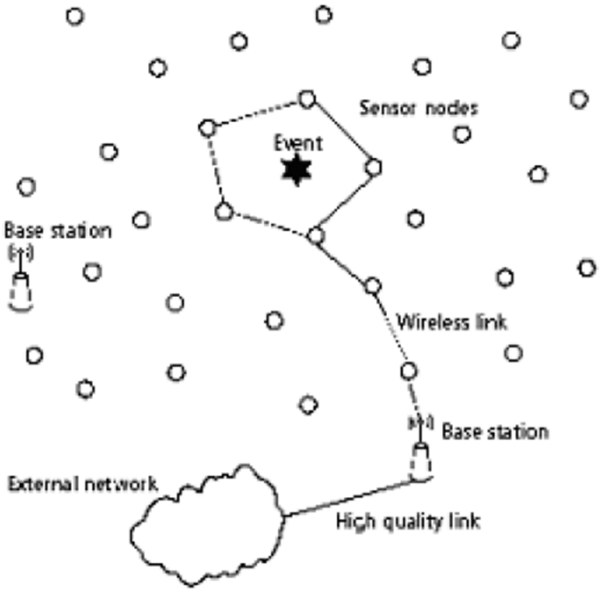


Fig. 2: A Wireless Sensor Network

©IJRASET: All Rights are Reserved

C. Hardware Components of Sensor Node

The application criteria obviously play a deciding role when selecting hardware components for a wireless sensor node. Sensing, data processing, and communication are all done by a sensor node, which incorporates hardware and software. For transmitting and receiving data from other nodes, they depend on wireless channels. The basic structure of a sensor node is shown in Fig. 3.

Since the battery life of a sensor node is so significant, adopting energy-efficient information processing strategies is critical. As shown in Fig.3, a sensor node consists of a sensing unit, a processing unit, a transceiver unit, and a power unit.

They can also include application-specific components including a position finding device, a power generator, and the ability to mobilize. The ADC converts physical parameters of the environment into digital signals, which are then fed into the processing unit. Sensors are the real interface to the physical world: instruments that can observe or monitor physical parameters of the environment.

The processing unit, which is usually connected to a small storage unit, controls the procedures that enable the sensor node to collaborate with other nodes to complete the assigned sensing tasks. The node is connected to the network by a transceiver unit. Power scavenging units, such as solar cells, can be used to support power units.

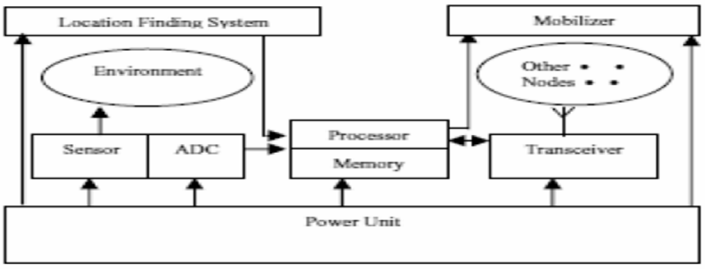


Fig. 3: Sensor Node Architecture

The majority of sensor network routing strategies and sensing tasks necessitate high-accuracy location awareness. As a result, a sensor node with a position finding system is popular. When moving sensor nodes is needed to complete the assigned tasks, a mobilize will be required.

D. Software Components of Sensor Node

1) Operating System/Software: Traditional OS aren't suitable for wireless sensor networks because WSNs have constrained resources and diverse data- centric applications, additionally to a variable topology. WSNs need a replacement sort of OS, considering their special characteristics. Sensor operating systems (SOS) should embody the subsequent functions, bearing in mind the limited resource of sensor nodes:

a) Should be compact and little in size
b) Should provide real-time support
c) Should provide efficient resource management mechanisms.
d) Should have a generic programming interface up to sensor middleware or device software
e) Should support consistent and effective code delivery
f) Should support power management
g) Should support multiprocessing along side threading when a sensor is deployed for multiple purposes.

2) Querying Sensor Network: For the location, management, and processing of the sensor data, a knowledge storage, management and query processing policy is important. A sensor database is required which will store dynamic information. An internet accessible query processing system is required to supply replies to high-level user queries. Unfortunately, the resource constraints associated with sensor nodes like computation, communication, power consumption, uncertainty in sensor readings have posed a numerous challenges in query processing for sensor networks.

E. Sensor Node Types Desirable Functionality of sensor nodes during a WSN Include

Simple installation, self-indication, self diagnosis, reliability, time awareness for coordination with other nodes, some software functions and DSP, and standard control protocols and network interfaces. There are many sensor manufacturers and it's too costly for them to form special transducers for each network on the market. IEEE 1451, the quality for smart sensor networks was the result. Commercially available sensors of the many types are suitable for wireless network applications.

©IJRASET: All Rights are Reserved

III. FEASIBILITY OF BASIC SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS

Authentication, reliability, confidentiality, non-repudiation and anti-playback are all that security can encompass [6]. The more the dependency on the knowledge provided by the networks has been increased, the more the danger of secure transmission of data over the networks has increased. For the secure transmission of varied sorts of information over networks, several cryptographic, steganographic and other techniques are used which are documented. During this section, we discuss the network security fundamentals and the way the techniques are meant for wireless sensor networks.

A. Cryptography

The encryption-decryption techniques devised for the normal wired networks aren't feasible to be applied directly for the wireless networks and especially for wireless sensor networks. WSN contains tiny sensors which really suffer from the shortage of processing, memory and battery power [7], [8], [9]. Applying any encryption scheme requires transmission of additional bits, hence extra processing, memory and battery power which are vital resources for the sensors' longevity. In wireless sensor networks, using safety mechanisms such as encryption can increase delay, jitter, and packet loss [10]. Furthermore, when using encryption schemes on WSNs, some important questions arise, such as how keys are produced and disseminated. How the keys are managed, revoked, assigned to a replacement sensor added to the network or renewed for ensuring robust security for the network. As minimal (or no) human interaction for the sensors, may be a fundamental feature of wireless sensor networks, it becomes a crucial issue how the keys might be modified time to time for encryption. Adoption of pre-loaded keys or embedded keys couldn't be an efficient solution.

B. Steganography

If cryptography aims to conceal a message's meaning, steganography [11], [12] aims to conceal the message's nature. Steganography is that the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.) [13]. the most objective of steganography is to switch the carrier during a way that's not perceptible and hence, it's a bit like ordinary. It hides the existence of the covert channel, and furthermore, within the case that we would like to send a secret data without sender information or once we want to distribute secret data publicly, it's very useful. However, securing wireless sensor networks isn't directly associated with steganography and processing multimedia data (like audio, video) with the inadequate resources [14] of the sensors is difficult and an open research issue.

C. Physical Layer Secure Access

Physical layer secure access in wireless sensor networks might be provided by using frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping), dwell time (time interval per hop) and hopping pattern (the sequence during which the frequencies from the available hopping set is used) might be used with a touch expense of memory, processing and energy resources. Details in physical layer safe access include an efficient design that allows the hopping sequence to be changed in less time than it takes to receive it, and both the sender and receiver must maintain a synchronized clock in order to use it. A scheme like the one proposed in [16] could be used to implement safe physical layer access using singular vectors and channel synthesize.

IV. SECURITY THREATS AND ISSUES

In WSN Wireless Sensor Networks are susceptible to security attacks thanks to the printed nature of the transmission medium. Basically, attacks are divided into two groups. i.e. active attacks and passive attacks. This paper points out both of those attacks in details.

A. Passive Attacks

The monitoring and listening of the channel by unauthorized attackers are referred to as passive attack. A number of the more common attacks against sensor privacy are:

1) *Monitor and Eavesdropping:* This is that the commonest attack to privacy. The adversary could easily discover the communication contents by snooping on the data.
2) *Analysis of Traffic:* Even if the messages are encrypted, there is always a good chance that the contact patterns can be analyzed. Sensor activities can disclose enough information to allow an adversary to damage the sensor network maliciously.
3) *Camouflage Adversaries:* One can insert their node or compromise the nodes to cover within the sensor network. Then these nodes can copy as a traditional node to draw in the packets, then misroute the packets, conducting the privacy analysis.

©IJRASET: All Rights are Reserved

B. Active Attacks

The unauthorized attackers monitors, listens to and modifies the info stream within the channel are referred to as active attack. the subsequent attacks are active in nature.

1) *Routing Attacks in Sensor Networks:* The attacks which act on the network layer are called routing attacks. the subsequent are the attacks that happen while routing the messages.

a) *Attacks on Information in Transit:* In a way or network, sensors monitor the changes of specific parameters or values and report back to the sink consistent with the need. The information in transit could be changed, spoofed, replayed, or disappeared while the report was being sent. Due to the vulnerability of wireless communication to eavesdropping, any attacker may track the traffic flow and take action to interrupt, intercept, alter, or fabricate packets, thus providing false information to the bottom stations or sinks.

b) *Selective Forwarding:* A malicious node can selectively drop only certain packets. Particularly effective when combined with a node-based attack that gathers a lot of traffic. It is believed that nodes in sensor networks faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.

c) *Black hole/Sinkhole Attack:* In this attack, a malicious node acts as a region to draw in all the traffic within the sensor network. In fact, this attack can affect even the nodes those are considerably far away from the bottom stations. Fig.4 shows the conceptual view of a black hole/sinkhole attack.

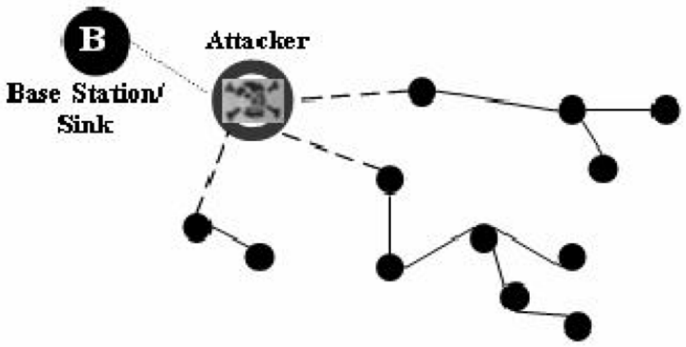


Fig.4: Conceptual view of Black hole Attack

d) *Wormholes Attacks:* Wormhole attack is a crucial attack in which the attacker records packets (or bits) at one network location and tunnels them to another.

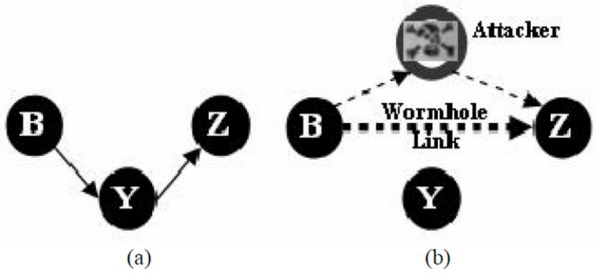


Fig.5: Wormhole Attack

Fig.5 (a and b) shows a situation where a wormhole attack takes place. When a node B (for example, the bottom station or the other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be within the range of Node B, and can mark this node as its parent. Hence, albeit the victim nodes are multi-hop aside from B, attacker during this case convinces them that B is merely one hop far away from them, thus creates a wormhole.

e) *HELLO flood attacks:* An intruder uses more energy to send or replay HELLO packets from one node to another in a routing protocol. To persuade the sensors in the WSN, this attack uses HELLO packets as a tool.

©IJRASET: All Rights are Reserved

2) *Denial of Services:* Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. In wireless sensor networks, several sorts of DoS attacks in several layers could be performed.
3) *Node Subversion:* Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the entire sensor network. a specific sensor could be captured, and knowledge (key) stored thereon could be obtained by an adversary.
4) *Node Malfunction:* A malfunctioning node will generate inaccurate data that would expose the integrity of sensor network especially if it's a data-aggregating node like a cluster leader.
5) *Node Outage:* Node outage is that the situation that happens when a node stops its function. Within the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the consequences of node outages by providing an alternate route.
6) *Physical Attacks:* Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, therefore the losses are irreversible. As an example, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming within the sensors, or replace them with malicious sensors under the control of the attacker.
7) *Message Corruption:* Any modification of the content of a message by an attacker compromises its integrity.
8) *False Node:* A false node is created when an adversary adds a node and injects malicious data into it. An attacker could introduce a node into the system that feeds false data or prevents true data from passing. One of the most dangerous attacks that can occur is the insertion of a malicious node.
9) *Node Replication Attacks:* Conceptually, a node replication attack is sort of simple; an attacker seeks to feature a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated during this approach can severely disrupt a sensor network's performance. Packets are often corrupted or maybe misrouted.
10) *Passive Information Gathering:* An adversary with powerful resources can collect information from the sensor networks if it's not encrypted. To attenuate the threats of passive operation, strong encryption techniques must be used.

V. SECURITY CHALLENGES

In WSN The nature of huge, ad-hoc, wireless sensor networks presents significant challenges in designing security schemes. A wireless sensor network may be a special network which has many constraint compared to a standard network.

A. Wireless Medium

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple [14]. An adversary can easily intercept, change, or replay any transmission. An attacker can simply intercept legitimate packets and inject malicious ones using the wireless medium. Traditional solutions must be modified to run efficiently on sensor networks, despite the fact that this issue is not special to sensor networks.

B. Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure is often statically defined. Nodes could also be deployed by airdrop, so nothing is understood of the topology before deployment. Since nodes may fail or get replaced the network must support self configuration. Security schemes must be ready to operate within this dynamic environment.

C. Hostile Environment

The next challenging factor is that the hostile environment during which sensor nodes function. Motes face the likelihood of destruction or capture by attackers. The highly hostile environment represents a significant challenge for security researchers.

D. Immense Scale

The proposed scale of sensor networks poses a big challenge for security mechanisms. Simply networking tens to many thousands of nodes has proven to be a considerable task.

VI. CONCLUSION

Security in Wireless Sensor Network is significant to the acceptance and use of sensor networks. Sensor nodes deployed in an unattended environment leave networks vulnerable. Wireless sensor networks are increasingly getting used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks also as wireless ad-hoc networks. Security is a crucial feature for the deployment of Wireless Sensor Networks.

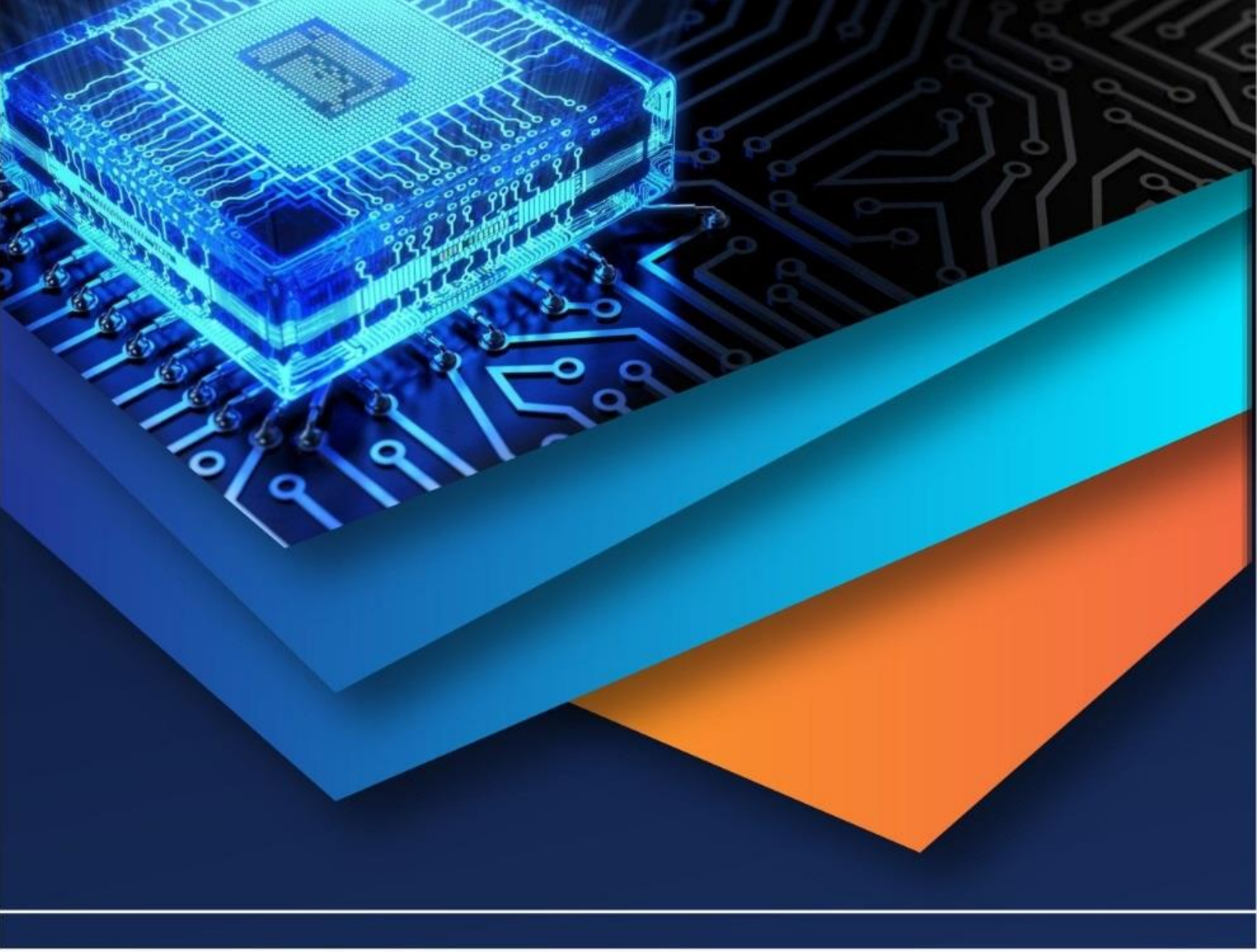
©IJRASET: All Rights are Reserved

Especially, Wireless Sensor Network product in industry won't get acceptance unless there's a full proof security to the network. This paper summarizes the attacks and their classifications in wireless sensor networks and also an effort has been made to explore the safety mechanism widely wont to handle those attacks. Wireless Sensor Networks' problems are also discussed briefly. This paper motivates future researchers to return up with smarter and more robust security mechanisms and make their network safer. Even though holistic security can be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to use such mechanisms could still pose great research challenge within the coming days.

REFERENCES

[1] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E.,"Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002,pp. 393-422.
[3] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp.407-411.
[4] Mr.S.Pragadeswaran, Ms.S.Madhumitha and Dr.S.Gopinath, "Certain Investigation on Military Applications of Wireless Sensor Network", International Journal of Advanced Research in Science, Communication and Technology, Volume 3 and Issuse No 1, 2021 pp.14-19.
[5] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S.,"A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.
[6] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at, http://www.cs.sfu.ca/~angiez/personal /paper/sensor-ids.pdf
[7] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS:Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no.5, 2002, pp. 521-534.
[8] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340.
[9] Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M., and Tuan, T., "PicoRadios for wireless sensor networks: the next challenge in ultra-low power design" 2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 –201.
[10] S Pragadeswaran, N Suma, MS Madhumitha, S Gopinath, "Fuzzy based Fault Tolerant Routing Protocol for Node Realiability in MANET", Annals of the Romanian Society for Cell Biology, Volume 25 and Issuse No 1, Pages 7223 - 7232,2021,1583-6258.
[11] Saleh, M. and Khatib, I. A., "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September 26-28, Dubai, 2005.
[12] Kurak, C and McHugh, J, "A Cautionary Note on Image Downgrading in Computer Security Applications", Proceedings of the 8th Computer Security Applications Conference, San Antonio, December, 1992, pp.153-159.
[13] Mokowitz, I. S., Longdon, G. E., and Chang, L., "A New Paradigm Hidden in Steganography", Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41 – 50.
[14] S.Pragadeswaran, MM Kamalanathan, Disguised Characteristic Randomness From Routing Data in Mesh, International Journal of Engineering Research and Technology, Volume 06 and Issuse No 05,1-4, 2018,2278-0181.
[15] Kim, C. H., O, S. C., Lee, S., Yang, W. I., and Lee, H-W., "Steganalysis on BPCS Steganography", Pacific Rim Workshop on Digital Steganography (STEG'03), July 3-4, Japan , 2003.
[16] Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A., "On handling QoS traffic in wireless sensor networks", Proc. of the 37th Annual Hawaii International Conference on System Sciences, 2004, 5-8 January, 2004, pp. 292 – 301.
[17] Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., "Channel synthesized modulation employing singular vector for secured access on physical layer", IEEE GLOBECOM 2003, Volume 3, 1-5 December,2003, pp. 1226 – 1230.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)