iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VI **Month of publication:** June 2014

DOI:

www.ijraset.com

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

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Study of Security in Wireless Sensor Networks

Vandita Grover and Sugandha Gupta[#1]

[#]*Department of Computer Science, University of Delhi*

Abstract— Wireless Sensor Networks (WSN) is an incipient technology that shows great potential for various futuristic application both for military and mass public. Security plays a vital role in a WSN. The intent of this paper is to discuss the security goals and attacks encountered by WSN. We also identify the constraints and list various security schemes which consider these constraints in order to achieve security goals and function efficiently.

Keywords— Wireless Sensor Network, Attacks, Sensor Nodes

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are collections of small sized, moderately inexpensive nodes that sense local environmental conditions or other parameters and forward the result to a central point for further processing. It is an emerging technology which is at its full pace now a days with a wide domain of applications. Some of the specific applications are object tracking, traffic monitoring, context-aware computing, industrial sensing and diagnostics, military purposes etc.

A Wireless Sensor Network is composed of a base station (also known as sink) and a large number of sensor nodes distributed within the sensing field. The sensor nodes are an integral element of a Wireless sensor network (WSN). End user queries the sensor nodes for the required information through the base station, i.e. base station acts as an interface between the sensor nodes and the end user. Sensor nodes perform the function of sensing, processing and routing the data back to its respective base station (sink). Base station collects data from all the sensor nodes and analyse this data to draw conclusion about the activity in the area of interest of the user.

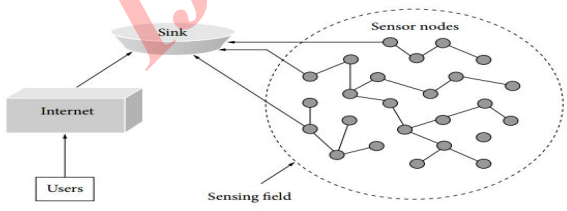


Fig. 1 Architecture of Wireless Sensor Network (WSN)

Two sensor nodes can either communicate with each other directly (if within each other's vicinity) or indirectly using the intermediate sensor nodes. A sensor node consists of four basic components: a sensing unit (sensor, ADC), a processing unit (memory, microcontroller), a communication unit (usually radio transceivers), and a power unit (battery). Sensing unit senses the environment through transceiver and produce a measurable response to a change in the environment. The analog signal produced by the sensors is digitized by an analog-to-digital converter (ADC) and sent to microcontrollers. Microcontroller performs tasks, processes data and controls the functionality of other components in the sensor node.

The more the dependency on the information provided by WSNs has been increased, the more the risk of secure information over the networks has increased. Security is obligatory in a WSN due to a number of reasons like, only authentic nodes should transmit data, data should not be modified by any intermediate node while its transmission, any kind of attacks should not affect WSN's performance and so on.

This paper reviews constraints involved in wireless sensor networks in Section II, security objectives in Section III, attacks on WSN in Section IV, security schemes for WSN in Section V. In Section VI we conclude the paper.

II. CONSTRAINTS IN WIRELESS SENSOR NETWORKS

In this section, we will discuss various constraints imposed on the design of any protocol or algorithm for wireless sensor networks.

IJRASET: ISSN: 2321-9653

A. Network Topology

It refers to the arrangement of various nodes in a wireless sensor network. Different WSN topologies are bus, tree, star, ring, mesh, circular and grid. It may also assist routing operations. Sensor nodes are susceptible to failures, thus topology maintenance is a task.

B. Fault Tolerance

It is the ability of a WSN to function without any interruption due to failure of a sensor node. A sensor node may fail or be blocked due to physical damage, lack of energy, communication problem or environmental interference.

C. Limited Memory and Storage Space

A sensor node is a small sized node with only a lesser amount of memory and storage space for the code. Thus in order to design an effective security mechanism, it is mandatory to limit the code size of the security mechanism.

D. Scalability

A WSN can consists of a dynamic number of sensor nodes, dispersed within the sensing field. Protocols must thus be able to work in such large-scale WSNs.

E. Power Consumption

It is the main concern in developing wireless sensor network applications. The energy available in the sensor nodes of a WSM is limited. An application can take years to drain the battery of the sensor node or consume it in few days. Thus, the application developer should use methodologies so as to reduce the power consumption as much as possible.

F. Computation

Sensor nodes of a WSN are not as powerful as the nodes of a wired or ad hoc network. Thus, complex cryptographic algorithms can't be used in WSNs.

G. Data Aggregation

It is a process used to cater the problem of data redundancy in a wireless sensor network and avoid multiple data transmissions. In this, data from multiple sensor nodes are aggregated and the fused information thus obtained is transmitted to the base station. This process is also known as data fusion.

H. Latency

The network congestion and processing done by sensor nodes can lead to greater latency in the network, thus making it challenging to accomplish synchronization between the nodes present in the sensing field. The synchronization issues can be acute to sensor security where the security mechanism count on cryptographic key distributions.

I. Quality of Service Requirements

A critical event should be conveyed in a given period of time. Otherwise, the information would become obsolete and unusable.

J. Managed Remotely

Remote management of a sensor network makes it practically unmanageable to discover the physical tampering and physical maintenance disputes.

K. Unreliable Transfer

Packet-based routing of WSN is connectionless and thus inherently unreliable. Packets may get smashed due to channel errors or dropped at highly congested nodes. The result is lost or missing packets.

III. SECURITY OBJECTIVES IN WIRELESS SENSOR NETWORKS

A. Security Goals

The security goals of wireless sensor networks or any communication network are confidentiality, integrity, availability, authentication and non-repudiation. In this section we briefly describe various security objectives of WSNs.

1) Confidentiality: The access or disclosure of the message is limited only to the intended recipient. The message appears in unintelligible form to a node for which it is not intended. Sensor should not leak information to adjacent sensors and public information about sensors should be encrypted to elude traffic analysis attacks.

2) Integrity: The transmitted message is received in the same form without any modifications during transmission. An adversary can generate a new message or tamper with the existing one, so mechanisms like checksum message authentication codes or hash should be used.

3) Availability: The data and services are available whenever they are required.

4) Authentication: A node should be able to identify itself

IJRASET: ISSN: 2321-9653

as a genuine participant in communication. Authentication helps receiver ensure that the message was indeed send by the "claimed" sender. In static WSN authentication is easier to achieve as compared to MSN, as mobile nodes keep moving. Resource crunch is also a limitation in such cases.

5) Non-Repudiation: A node cannot deny a message sent by it previously.

6) Privacy: ensures that the sensed information is accessible only to the trusted parties. Access policies can be implemented to guide who can use data and for what purpose.

7) Forward and Backward Secrecy: Forward secrecy means that a sensor should not be able to read future messages once it leaves the sensor network. A sensor joining the network should not have access to previously transmitted messages, maintaining backward secrecy.

8) Freshness of Data: Message or data has not been generated as a result of replay attack and is latest. This is particularly important while sharing keys.

9) Time Synchronization: Sensor nodes are highly collaborative in nature and thus need to coordinate on sensing tasks, scheduling, tracking applications etc. Various algorithms like Reference Broadcast Synchronization (RBS), Timing Sync Protocol for Sensor Networks (TPSN) etc. have been proposed.

10) Location Discovery: A sensor node should be able to locate each sensor node in the network for various applications like environment monitoring, target tracking etc. Special nodes called beacon nodes are used for location estimation.

B. Security Parameters

A comprehensive security planning of WSN's should address the following requirements:

1) Resilience: Security scheme should continue to guard against the attacks even if there a few malicious nodes in the network.

2) Assurance: Different information should be provided to users at different levels.

3) Energy Efficiency: Power conservation is a significant constraint in sensors, the security scheme should be such that it addresses security goals and maximizes node lifetime.

4) Self-Healing: If a sensor fails or runs out of power, the remaining sensors should reorganize themselves to adapt to change in configuration and maintaining predefined security level.

C. Security Techniques and Measures:

1) *Cryptography:* Applying encryption and decryption techniques for preserving data confidentiality is a challenging task in WSNs, owing to constraints on memory, processing and battery power. Cryptographic functions could also increase delay and jitter during data transmission.

- Key Establishment and Management: Cryptographic schemes and authentication requirements pose a challenge on secure exchange of keys. Establishing keys and managing their exchange is an essential pre-requisite for applying cryptography based data exchange, digital signatures, entity and message authentication. Key Management is typically challenging in WSNs as even if one node is captured there is a possibility of the entire network being compromised. Moreover, computational and storage complexity of schemes used, key exchange in the dynamic network topology adds to non-triviality key management schemes. Following is an overview of some key management schemes.
- Trusted Server Schemes: A trusted and secure server generally the base station, serves as a key distribution centre. Sensor nodes are embedded with keys with which they can authenticate themselves to the server and server in turn generates session key for secure communication between two nodes. Major drawback of the scheme is that if the server is compromised the entire network security is in danger.
- Key Pre-distribution Schemes are a secure option where the keys are pre-distributed among all nodes prior to network deployment.
- Self-Enforcing Schemes are based on asymmetric cryptography: Sensor nodes exchange public keys and master public key after deployment and can be authenticated using the master key's signatures. For communication amongst two sensor nodes, a key is generated by a node, encrypted using public key of the receiver and sent across the network. Receiver can decrypt the session key using its private key and data can be exchanged using this key. Though secure,

IJRASET: ISSN: 2321-9653

this scheme is computationally intensive and hence not desirable.

- Public Key Cryptography schemes require no pre-distribution of keys, pair-wise key sharing but are too expensive because of extensive computations. Recently many groups have implemented public key cryptography in WSNs. Gura et al. depict that RSA and elliptic curve cryptography are possible using 8 bit CPUs. Watro et al. have implemented portions of RSA on sensors while a laptop was used to implement private operations which required heavy computations. TinyPK system implements Diffie-Hellman Key Exchange and the design allowed authentication and key exchange between resource constrained sensors.

2) Physical Layer Secure Access: Hopping sequence can be modified in time less than that required to discover it, by synchronizing sender and receiver clock. Hopping set, dwell time and hopping pattern may be changed dynamically.

3) Secure Routing: Routing protocols in WSNs have focused on efficiency and data communication. Secure routing protocol design must consider ability to isolate unauthorised nodes, concealing network topology, message authentication, integrity of routing message and frequent updation of paths to ensure an adversary has not misdirected to form loops. SPINS is a protocol suite optimized for sensor networks.

4) Secure Group Management: WSN may be split in groups for load balancing, increase network performance, consume fewer resources and achieve a task (eg. data aggregation) together as a group. Group management's protocols have to be efficient and adaptive in terms of adding or removing group members. While transmitting group's computation outcome to a base station, authentication must be done to ensure that it comes from a valid group. Also the solution must be cost effective in terms of computation and communication cost.

5) Intrusion Detection: A typical Intrusion Detection System (IDS) continually monitors the network for anomalies and security breaches. IDS is expected to identify system vulnerabilities, assess integrity of various system elements, recognize attack patterns and abnormality patterns and keep a track of policy violations. WSN IDS should be distributed and inexpensive and should have following properties: Localised and partial data audit (can be managed with groups). Use small amount of resources. Should not trust any node to be secure in cooperative algorithms. Resist hostile attack. Data collection and aggregation should be distributed.

6) Secure Data Aggregation: In-network aggregation approach is followed, where instead of transmitting entire data, data is aggregated (e.g. sum, average) so as to approximate the derivative as close as possible to the source. A compromised aggregator may inject false aggregate into the network thereby corrupting the resultant aggregate. A Secure Hop by Hop scheme was proposed where sink can detect non authorised inputs. Secure Information Aggregation (SIA) has been described which detects forged aggregation values.

7) Secure Time Synchronization: Many of time synchronization schemes have been designed for homogeneous systems and are prone to attacks in hostile environments.

8) Secure Localization: Many proposed Location discovery protocols work in two stages. Non-beacon nodes receive reference messages from beacon nodes based on which they make measurements about distance. An attacker may modify these messages and subvert the operation of the network. Approaches like Minimum Mean Square Estimation (MMSE) use mean square error to identify and remove malicious references. Voting Based Estimation technique is used to phase out malicious references sent by the attacker. Verifiable Multi alteration technique can be used to discover a node manipulating the localization protocol. SPINE (Secure Positioning for sensor Networks) is used for larger sensor networks.

IV. Attacks in Wireless Sensor Networks

A large scale Wireless Sensor Network has numerous nodes spanning a wide area and are prone to various attacks. These attacks can be categorised as physical or logical attacks, inside or outside attacks, ability of attacker to target at mote or laptop level and attacks at various layers. In this section we classify attacks based on various network layers.

A. *Denial of Service Attacks:* An event that thwarts network's ability to perform essential functions. A DoS may be triggered by unintentional failure of nodes or may be perpetrated by a malicious entity. DoS attack compromises the availability goal by preventing access to resources, resource exhaustion and limiting network's capability to provide services. Prevention of DoS attacks could be defended against by defining policies like traffic identification and authentication, payment for network resources etc.

IJRASET: ISSN: 2321-9653

B. *Physical Layer Attacks:* Physical layer is responsible for transmitting signals for communication. WSNs have wireless nodes with unidirectional antennas that transmit radio signals in all directions.

1) *Eavesdropping:* An adversary may monitor messages being exchanged between two sensor nodes, in unauthorised manner violating confidentiality. Using directional antennas, decrease the probability of eavesdropping.

2) Jamming: A jamming source may interfere with radio frequencies of either a subset or the entire network, thus disrupting the network. Jamming is an example of DoS. Defense techniques include varying frequency selection sequence in Frequency Hopping Spread Spectrum and Code Spreading. WSN's are at high risk of jamming because they generally use single-frequency owing to limitations of low cost and power.

3) Tampering: compromises the integrity. Attacker may access keys or other data or may create a compromised node controlled by her. Tamper-proofing and hiding may be applied as defense.

4) Node Capture Attacks: Adversary has a full command on a sensor node by direct physical access and has unlimited hold on information stored in the memory chip and may cause damage to entire system.

5) Side Channel Attacks: are type of Tampering attacks which exploit the vulnerability of implementation of cryptographic system rather than algorithm weakness. Eg Simple and Differential power analysis can be used to extract several bit keys. Countermeasures include randomization of power consumption, randomizing instruction set execution, CPU clock randomization and randomizing register memory use.

X. *Link Layer Attacks:* Link layer involves data multiplexing, framing and point to point communications.

1) Collision: An adversary may plan a collision to cause exponential back-off in some MAC protocols. Error correction codes may be used at low levels of collision but no complete defense is known as adversary may be able to corrupt more than what can be corrected.

2) Exhaustion: Repeated collisions may be strategized to deplete energy reserves. Rate limits may be applied to MAC admission control.

3) Unfairness: Attacker may capture the communication channel by using above attacks and thus forcing sensor nodes to miss their transmission deadline. Small frames may be used which will reduce the time adversary has on the medium, but this may reduce efficiency.

Δ. *Network Layer:*

1) Manipulation of Routing Information: An attacker may spoof, replay, modify or inject corrupt routing information to cause network disruption. Message authentication codes may be appended with messages to check with integrity. Timestamps may be applied to check for replay attacks.

2) Selective Forwarding: Sensor nodes in WSNs forward the received messages. Attacker may use a compromised node to selectively forward some messaged and drop others. To counter this attack multiple paths may be used to forward data. Secondly, malicious node may be detected and labelled as failed and messages forwarded through alternative path.

3) Sinkhole Attack: A compromised node may be made to work as a sinkhole where it appears as a better node to neighbouring sensors to route information. All nodes forward information to the malicious node and adversary may use selective forwarding.

4) Sybil Attack: A node presents itself with multiple identities by claiming false identities or impersonating. Many protocols may be compromised like distributed storage, routing, data aggregation etc. To counter sybil attack radio resource testing may be done which assumes each device has single radio. Key pre-distribution which will identify a node with a key and validates key to check the authenticity of node. Node registration may be done at base station.

5) Wormholes: Attacker records traffic from one region of a network and replays it on other region using a low latency link between the two regions. Packet leashes based on geographic and temporal information may be used where additional information to restrict distance travelled by packet is added to packet. This packet leashing scheme is a proposed solution against wormhole attack.

6) HELLO flood: Protocols use HELLO packets to inform neighbours about a shorter route. Assumption is that the sender is within the radio range and hence the receiving nodes will try to send packets through this node. In reality the attacker might have used a high powered transmitter to advertise that it is a neighbouring node, even though it's not in the vicinity. All nodes will try to send message to malicious node and in effect disrupt WSN.

IJRASET: ISSN: 2321-9653

7) Acknowledgement Spoofing: An adversary may send false acknowledgement on hearing messages meant for its neighbouring node claiming that the receiver is alive, even though it is dead or it may send acknowledgement to spoof a bad link.

8) Traffic Analysis Attacks: The attacker tries to gather information on network topology or base station location based on traffic volumes and patterns. Rate monitoring and Time Correlation are two types of traffic analysis attacks. To thwart traffic analysis attack randomness and multiple paths in routing may be used. Injecting fake messages and probabilistic routing are also some techniques.

9) Spoofing and Replay attacks: A malicious attacker may record previously valid messages and replay or alter them causing the receiver to lose energy. It may ask nodes to update routing table to stale routes.

10) Blackhole Attack: A destination node can be made unreachable if a compromised node does not forward packets it is expected to relay thus creating a black-hole. This can severely downgrade network performance.

E. *Transport Layer:*

1) Flooding: Attacker makes many connection requests to flood the connection queue of the node and exhaust its resources thereby denying legitimate clients to form a connection. A scheme to handle flood attacks is that the clients are asked to solve a puzzle before forming a connection. The attacker is expected to have limited resources to solve many puzzles before forming many connections, so it would not be possible for the attacker to cause resource starvation.

2) De-synchronization: The attacker tries to disrupt the existing connection by spoofing messages eg. Connection requests, missed frames etc. Attacker may thus make the node perform requests which were not needed thus wasting resources. A possible solution is to authenticate all packets between communicating nodes.

Φ. *Application Layer:*

1) Software Attacks: The attacker may try to exploit vulnerabilities in code or modify memory using program flaws like buffer overflow etc. TinyOS (operating system) for sensor nodes does not provide memory control. Regher et al suggest an environment where untrusted code could be run without affecting the kernel.

Also, in TinyOS there is no check on authentication of a user who is trying to open a port to a node. Following measures may be taken to protect from exploitation of software vulnerabilities: authenticate and validate software, define clear trust boundaries for users and components, sandboxing like in JVM, run time encryption/decryption of code to prevent attacker understand the code and study its flaws.

2) Clone Attack: When a node is compromised it may be cloned by the attacker and these nodes which look like legitimate nodes may be used to plan more attacks on the network.

V. Security Schemes in Wireless Networks

Wireless Sensor Networks' security is an important issue. Many schemes have been proposed as counter-measure for various kinds of attacks. We describe a few schemes:

A. *Jammed Area Mapping:* JAM handles DoS attacks caused due to jamming. Nodes use this mapping protocol to determine if they are under attack based on parameters like collisions, inability to access medium, low SNR, checksum failures etc. By detecting jammed region, the faulty region may be quarantined.

B. *Statistical Enroute Filtering:* detects and drops false reports during forwarding.

C. *SPINS:* is a security suite that includes SNEP and µTESLA protocols.

1) SNEP preserves confidentiality, data authentication, integrity and data freshness. SNEP achieves confidentiality by, a using encryption and preventing eavesdroppers from listening the messages. Randomization is done before encryption by preceding a random string before the message.

2) µTESLA provides authentication for data broadcasting. The base station uses a secret key to compute a MAC on packet and transmits it to the node. Based on clock, synchronization error and key schedule the node can verify that key was not disclosed by base station and hence be assured that the packet was not altered in transit. Packet is stored in node buffer. The base station broadcasts the verification key to all receivers and the correctness of the key can be verified. Each node can easily perform time synchronization and retrieve an authenticated key of the key chain for the commitment in a secure and authenticated

IJRASET: ISSN: 2321-9653

manner, using the SNEP building block.

D. *REWARD:* receives, watch and redirect, for sinkhole attack. Node transmission is directed to immediate previous and next neighbours to detect sinkhole attack. SAMBA message is forwarded by previous node if a node does not forward the message, thus giving location of sinkhole attack.

E. TinySec: is a link layer security mechanism for sensor networks which uses an efficient symmetric key encryption protocol. It provides for message authentication, maintaining integrity and confidentiality.

F. *Radio Source Testing and Random Key Pre-distribution:* Node verifies that none of its neighbours are sybil entities using radio resource.

D. The random key pre-distribution, in the key set-up stage, every node is able to discover or calculate the general keys that are allocated by its neighbours. The common keys will be used as a shared secret session key to make sure node-to-node secrecy.

G. *Bidirectional Verification Security Schemes:* Every sensor node creates a set of neighbour nodes and thus messages because of HELLO Flood attack will be unobserved. Every request message through a node is encrypted, which neighbouring nodes can decrypt but attacker node cannot.

H. *TIK:* requires accurate time synchronization amongst communication nodes and implements symmetric cryptography and temporal leashes.

I. *PADS:* MAC is computed using static part of the packet and appended to the data. A key is generated using time synchronization based on a secret key shared between communicating nodes. To break the encryption an attacker would have to be time synced with the network. A basic detection algorithm in the base station locates the embedded pad, strips it from message, and recomputes the original value. This is possible because base station shares the secret key value with the sensor nodes.

J. *SOWSN:* is a Range-Based Algorithm using point-to-point distances. Sensors perform detection with high frequency allowing alerts to be correlated with target position and collection points. A multifactor dimensionality reduction (MDR) algorithm is applied to allow nodes to route messages to the nearest base station.

VI. CONCLUSION

Unlike other networks, WSNs are designed for specific applications. As WSNs grow in competence and are used more recurrently, the requirement for security in them becomes more specious. However, the nature of nodes in WSNs gives rise to constraints such as limited energy, processing capability, and storage capacity. These constraints make WSNs very dissimilar from traditional wireless networks.

We have surveyed in this paper, various security goals and attacks in a wireless sensor network. And, the security schemes to solve these issues have also been surveyed. There are quiet many issues to be resolved around WSN applications such as communication architectures, security, and management. By solving these issues, we can close the gap between technology and application

REFERENCES

[1] ADRIAN PERRIG, ROBERT SZEWCZYK, J.D. TYGAR, VICTOR WEN and DA VID E. CULLER, "SPINS: Security Protocols for Sensor Networks", Kluwer Academic Publishers, 2002

[2] Daniel E. Burgner, Luay A. Wahsheh, "Security of Wireless Sensor Networks", Eighth International Conference on Information Technology: New Generations, 2011

[3] Chris Karlof*, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Elsevier, 2003

[4] Amar Agrawal, Ruizhong Wei, "Scalable Trust-Based Secure WSNs", Journal of Computer and Communications, 2014

[5] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: TheCaseofJammers", IEEE Communications Surveys & Tutorials, 2011

[6] Gursewak Singh, Rajni Bedi, "A Survey of Various Attacks and Their Security Mechanisms in Wireless Sensor Network", International Journal of Emerging Science and Engineering, 2014

IJRASET: ISSN: 2321-9653

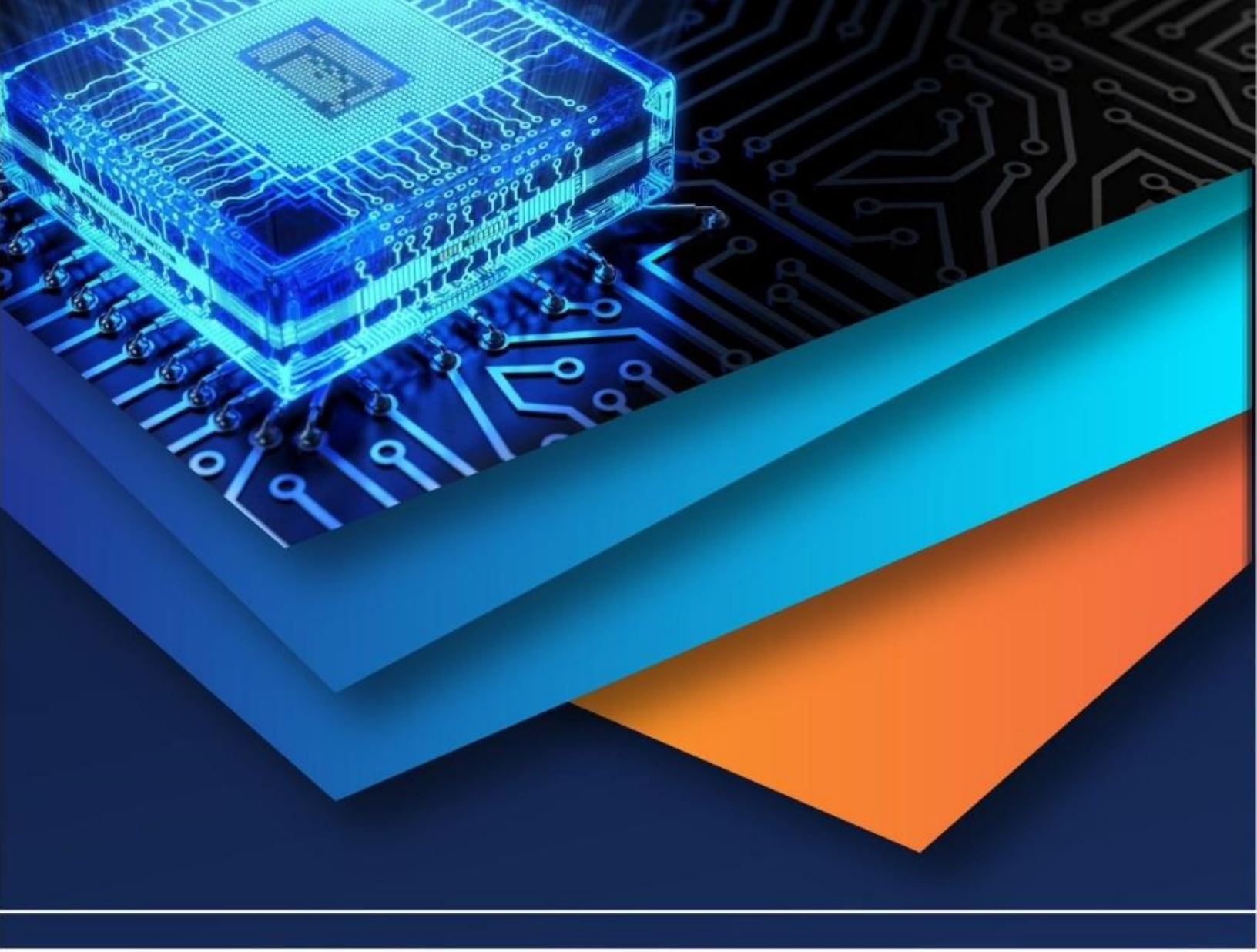
[7] Yong Wang, Garhan Attebury, Byrav Ramamurthy, "A Sur vey of Securit y Issues In Wireless Sensor Networks", CSE Journal Articles, 2006

[8] Yazeed Al-Obaisat, Robin Braun, "On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management"

[9] Kashif Kifayat, Madjid Merabti, Qi Shi and David Llewellyn-Jones, "Security in Wireless Sensor Networks, Chapter 26"

[10] Yogesh Kumar, Rajiv Munjal, Krishan Kumar, "Wireless Sensor Networks and Security Challenges", Proceedings published in International Journal of Computer Applications, 2011

IJRASET: ISSN: 2321-9653



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)