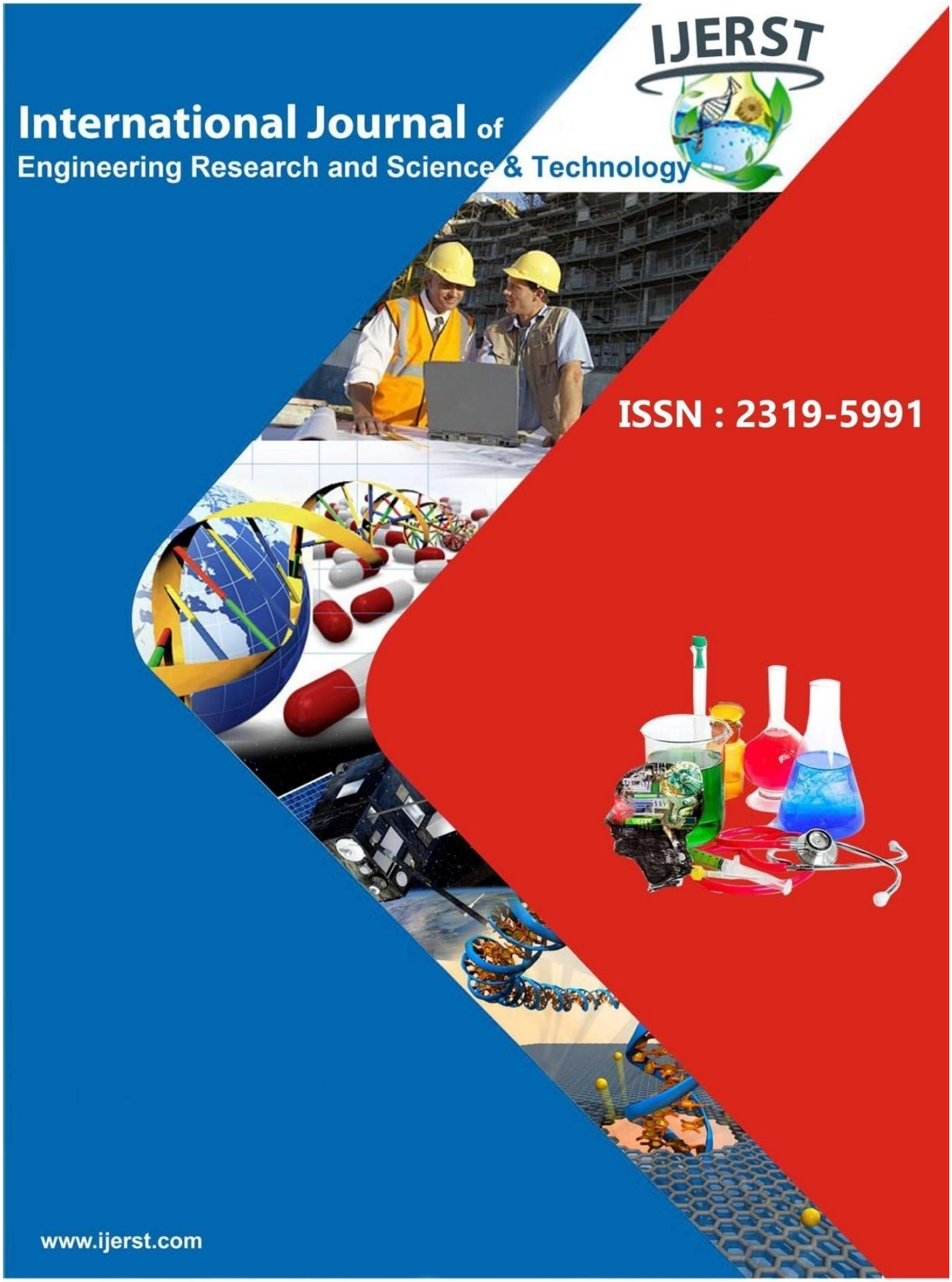
ISSN 2319-5991 www.ijerst.com

Vol. 4, Issuse.2,April 2016



Email: editor@ijerst.com or editor.ijerst@gmail.com

ISSN 2319-5991 www.ijerst.com
Vol. 4, Issuse.2,April 2016

Safety Methodologies and Obstacles in Wireless Sensor Networks

Mohsin
Department of Electrical Engineering, Sarhad University of Science & IT, Peshawar,

ABSTRACT

Recent developments in wireless communications, digital electronics, and micro-electro-mechanical systems (MEMS) have allowed for the creation of low-cost, low-power, multifunctional sensor nodes that are both compact and capable of short-range communication. The concept of sensor networks based on the collaborative effort of a large number of nodes is influenced by these tiny sensor nodes, which comprise of data processing, sensing, and communication components. When compared to conventional sensors, sensor networks are a major improvement. Large numbers of sensor nodes are deployed in close proximity to or inside the phenomenon to create a sensor network. Instead than being fixed in one spot, the sensor nodes may move about on their own will. The military, the environment, and even health care are just a few of the numerous potential uses for WSNs. Limitations in compute power, memory size, available energy, the ability to avoid physical capture, and the usage of unsecured wireless communication routes are just a few of the issues plaguing WSNs. Due to these limitations, securing WSNs might be difficult.

Keywords: Wide Area Network, Sensor Node, Symmetric Key, and Asymmetric Key.

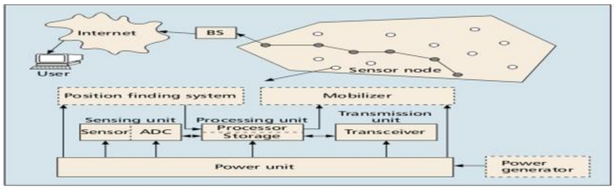
INTRODUCTION

Traditional approaches to software development have Because of technological advancements in wireless communication and electronics, low-cost, low-power, multifunctional sensor nodes are now feasible. Because of these miniaturized sensor nodes, which have sensing, data processing, and communication capabilities, Wireless Sensor Networks may be deployed, which is a huge step forward over cable sensor networks. Due to the fact that the environment being monitored does not need the communication or energy infrastructure often associated with such systems, WSNs may substantially simplify the design and operation of such systems.

Mohsin
Department of Electrical Engineering, Sarhad University of Science & IT, Peshawar,

1. Wired connections. Wireless sensor networks (WSNs) are seen as potential solutions to a wide variety of problems, including but not limited to detecting and tracking enemy soldiers and tanks on a battlefield, monitoring environmental conditions, gauging traffic congestion on roads, and determining where employees are located inside a building. The security of sensor networks is essential because many of them perform vital functions.

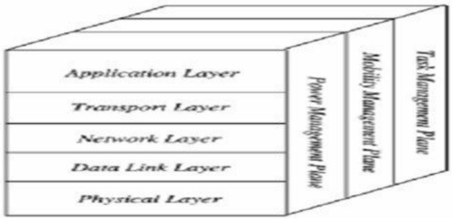
2. Information leakage and erroneous findings may come from the improper use of information or the use of fake information.
3. The following features distinguish WSNs from ad hoc networks:
4. • WSNs have a far larger number of nodes than ad hoc networks, perhaps by many orders of magnitude.
5. WSNs have a high density of nodes.
6. • The extreme conditions under which sensor nodes operate increase the likelihood of failure, especially when compared to ad hoc networks.
7. • Sensor nodes are restricted in their ability to compute, store data, and process information.
8. • Mobility may cause topological changes to occur regularly.
9. • There may be a lack of universal identifiers for sensor nodes.



10. ARCHITECTURE OF SENSOR NODE

Hundreds of sensor nodes, each with the capacity to gather data and forward it to a router or end user, compose a WSN. There are four main components that make up a sensor: the sensing unit, the processing unit, the power unit, and the transceiver unit. Depending on the use case, it may additionally feature a locator system, power generator, and mobilizer.

Sensors and analog-to-digital converters (ADCs) are the two main components of a sensing unit. Based on the observed occurrence, the analog-to-digital converters (ADCs) transform the analog signals provided by the sensors into digital signals. The processing unit, often paired with a tiny storage unit, controls the processes that enable the sensor node to cooperate with the other nodes. The node communicates with the network through a transceiver. The power unit is a crucial component. Power sources might be limited (like a single battery) or renewable (like solar panels). Knowledge of position is essential for most routing strategies in sensor networks and sensing activities, and this is what a location finding system provides. Finally, depending on the use case, a mobilizer may be required to relocate the sensor node.



ISSN 2319-5991 www.ijerst.com
Vol. 4, Issuse.2,April 2016

Fig. 1. The components of a Sensor Network.

The physical, data connection, network, transport, and application layers of the protocol stack used by sensor nodes are as follows: Selecting and generating a carrier frequency, bending and modulating signals, and encrypting data all fall within the purview of the Physical Layer.

• Data link layer: responsible for establishing and maintaining reliable point-to-point and point-to-multipoint connections; also handles multiplexing of data streams, data frame detection, media access, and error management.

• **Network layer:** controls how packets are routed and how addresses are assigned.

The Transport Layer is in charge of defining the parameters for secure packet delivery.

• **Application Layer:** Defines the Method by Which

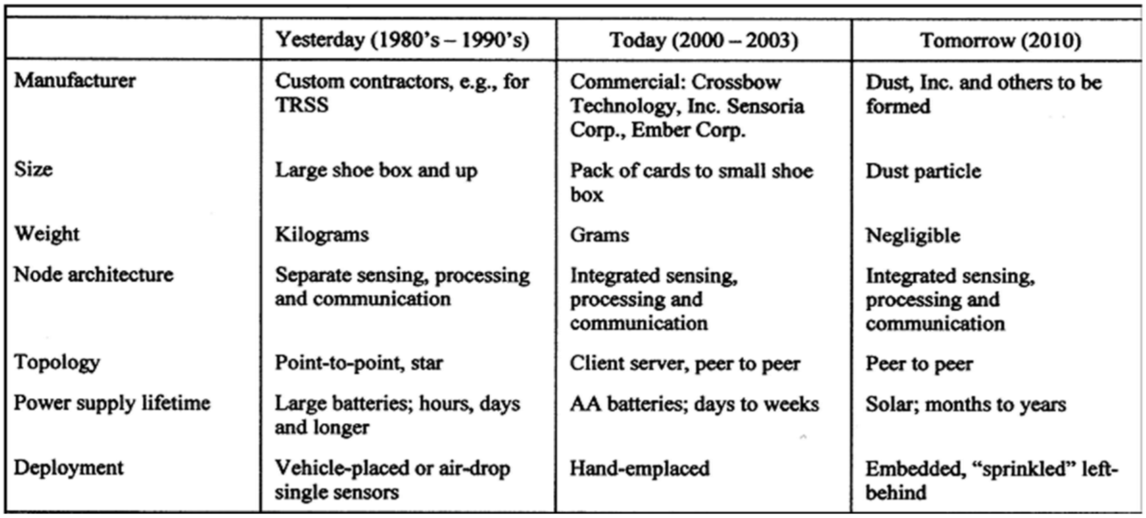
(Chong Y.C., et al., 2003).

The energy per bit needed for either communication or processing has decreased, however, as chip capacity and processor manufacturing capabilities have increased. The ability to conduct sensing, communication, and processing on a single chip has greatly lowered the price, enabling for wider adoption. Future developments in MEMS technology are expected to provide sensors with even more capability and versatility (Chong Y C et al, 2003). Three different sensor node generations are shown in Table 1. (Chong Y.C., et al., 2003).

2.1 Technology Trends

Twenty years ago, the technology needed for modern sensor networks was not even conceived of, much alone developed. Sensors, processors, and communication devices are all shrinking and becoming more affordable. Small sensor nodes and systems are being developed and deployed by a variety of private enterprises. Companies like these have a vision for how our everyday lives might be improved via the use of tiny networks of embedded sensor nodes. Their wares, including Pocket PC and Palm OS-powered personal digital assistants (PDAs), pack a lot of computational muscle into a very compact form factor. Some of these gadgets even come equipped with sensors and cameras. Together with large databases and a communication platform, these potent computers usher in a new age of technologically advanced sensor networks when connected to MEMS devices and machines.

Table 1: Three Generations of Sensor Nodes.



	Yesterday (1980's – 1990's)	Today (2000 – 2003)	Tomorrow (2010)
Manufacturer	Custom contractors, e.g., for TRSS	Commercial: Crossbow Technology, Inc. Sensoria Corp., Ember Corp.	Dust, Inc. and others to be formed
Size	Large shoe box and up	Pack of cards to small shoe box	Dust particle
Weight	Kilograms	Grams	Negligible
Node architecture	Separate sensing, processing and communication	Integrated sensing, processing and communication	Integrated sensing, processing and communication
Topology	Point-to-point, star	Client server, peer to peer	Peer to peer
Power supply lifetime	Large batteries; hours, days and longer	AA batteries; days to weeks	Solar; months to years
Deployment	Vehicle-placed or air-drop single sensors	Hand-emplaced	Embedded, "sprinkled" left-behind

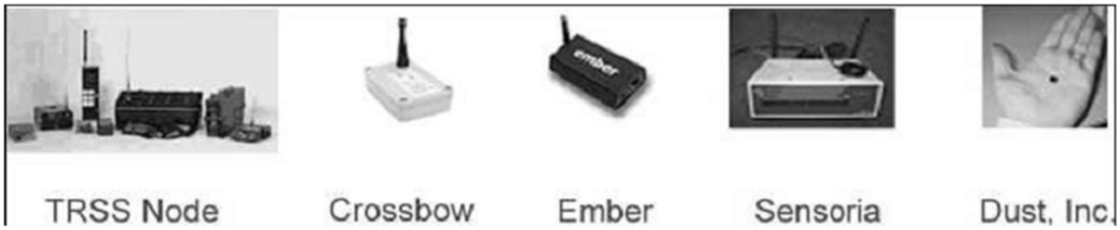


Fig. 3. Three Generations of sensor nodes.

11. The ability to analyze data inside the network itself is a key component of wireless sensor networks. When opposed to sending all the raw data to the final node, it may significantly save energy usage.

12. The above-mentioned characteristics provide sensor networks a wide variety of potential uses. Some of the applications sectors include health, military, home, environment, security and other business. It's more convenient for the patient if the doctor can check up on their vitals from afar. In addition, it helps the clinician grasp the patient's present state. Foreign chemical substances in water and air may be detected by sensor networks as well. The end user will get knowledge and insight into their surroundings thanks to the sensor network.

13. CONSTRAINTS IN WSNS

In a WSN, the sensors themselves have limited resources. They are restricted in what they can do and how much data they can store or send. And These are often the result of two factors: low power and compact dimensions. The hardware limitations of the sensor nodes must be taken into account during the design of security services in WSNs.

• **Computation:** sensor nodes often have less potent embedded processors than nodes in a wired or ad hoc network. This precludes the use of sophisticated cryptographic techniques in WSNs.

• **Power:** there are three distinct uses for electricity in sensor nodes.

Power supply for transducer sensors

· Power for inter-sensor network transmission

• **Memory:** a sensor node's memory typically consists of flash memory and RAM. o Power for microprocessor calculation. Application code transferred to flash memory is utilized for long-term storage, whereas application programs, sensor data, and intermediate calculations are kept in random-access memory (RAM). After installing the operating system and all of the applications, there is frequently not enough memory to perform complex algorithms. Because of this, the vast majority of existing security techniques are impracticable.

The transmission range of sensor nodes is limited by technological constraints and the need to preserve energy. The actual distance might be affected by variables like climate and topography.

14. SECURITY REQUIREMENTS

15. The purpose of security services in WSNs is to prevent unauthorized access to data and other malicious activity. WSNs must meet the following security requirements:

16. • Availability, which guarantees that network services will continue to function despite DDoS assaults. That is, there will be no inoperable parts of the network.

17. Only approved sensors are allowed to provide data to the network, thanks to authorization.

18. • Authentication, which guarantees the integrity of the communication between the nodes and prevents a hostile node from eavesdropping.

19. • Integrity, which guarantees that hostile intermediary nodes cannot alter or corrupt a message en route from one node to another.

20. • Non-repudiation, which means that a node can't say it didn't transmit a message it really did send.

21. • Newness, which means information is up-to-date and no stale messages are transmitted. Forward secrecy indicates that a node cannot read the future messages of the network after leaving the network, while backward secrecy means that a node cannot read the prior data sent after entering the network.

22. THREAT MODEL

It is often expected that an attacker in a WSN will be familiar with the security measures in place inside a sensor network. An adversary may take valuable data and resources from a node either by compromising it or by seizing it outright. This is why there has been so much effort put into studying how to safely route data between WSN nodes.

There are many distinct types of attacks that may be launched against sensor networks.

• Attacks from nodes on the network's perimeter against those launched from inside the network's own nodes, known as "insider attacks" and "outside attacks," respectively.

• Active attacks entail making changes to the data stream or introducing a fake stream into a WSN, whereas passive attacks include things like eavesdropping on or monitoring packets transmitted inside a WSN.

• Mote-class attacks, in which an adversary uses a small number of nodes with capabilities comparable to those of the network nodes, as opposed to laptop-class attacks, in which an attacker may utilize more powerful devices, such as a laptop, to attack a WSN.

23. EVALUATION OF THE SECURITY (WSNS)

A security technique is assessed by the following metrics whether it is acceptable in WSNs or not. The following are some measures:

• Resilience: a security strategy must be able to withstand assaults even if some nodes have been hacked.

Maximum node and network lifespan can only be achieved with the use of an energy-efficient security strategy.

Key management has to be adaptable so that various network deployment strategies may be supported.

A security scheme's capacity to grow without sacrificing security is essential.

A security strategy should be fault tolerant if it is to continue protecting a network in the face of problems like failing nodes.

24. Self-repair functionality, since sensors might lose power or stop working. It's possible that rearranging the remaining sensors is necessary to keep the same degree of safety.

25. • Confidence comes from knowing you can provide information with consumers at varying depths.

26. ATTACKS IN SENSOR NETWORKS

There are several forms of assaults against WSNs. These attacks may be broken down further in accordance with the security standards for WSNs as follows: Standard cryptography algorithms can prevent eavesdropping, packet replay attacks, and the alteration or spoofing of packets, all of which may compromise the confidentiality and validity of a communication channel.

Availability attacks, often known as denial-of-service attacks (DoS), target a network's ability to function normally. Denial-of-service attacks may affect a sensor network at any level. The purpose of a stealth attack on service integrity is to trick the network into believing a fabricated data value.We will start by talking about denial-of-service attacks and the methods that may be used to stop or at least mitigate them. A denial-of-service (DoS) assault is a kind of cyberattack in which the target network is disrupted or destroyed. Layered organization of sensor networks makes them vulnerable to Denial of Service assaults at any level. The assaults and defenses against each tier are detailed.

7.1 Physical Layer

7.1.1 The physical layer handles the selection of frequencies, the creation of carriers, the detection and modulation of signals, and the encryption of data. It's also possible for nodes in WSNs to be placed in unsafe or unfriendly surroundings, where an attacker might get simple access to the network

7.1.2 ***Jamming***

Jamming is an attack method in which the radio frequencies used by network nodes are disrupted. It's possible for a jamming source to be strong enough to interrupt the whole network, or it might be weaker and affect just a subset of the system. It just needs a little amount of electricity to disrupt the network and compromise a few nodes. Frequency hopping and code spreading are two examples of spread-spectrum communication used as anti-jamming countermeasures. In frequency-hopping spread spectrum (FHSS), a carrier is quickly hopped across numerous frequency channels according to a pseudo-random sequence that is shared between the transmitter and receiver. An attacker can't disrupt the active frequency unless they know where that frequency falls in the frequency selection sequence. However, there is only so much room in the frequency spectrum. Although code spreading is another method used to protect against jamming assaults, it is not employed in WSNs because of the restricted energy and additional design complexity it requires.

7.1.3 ***Tampering***

Tampering is a kind of physical layer assault. An attacker may steal cryptographic keys or other data stored on a node if they get physical access to it. Altering or replacing the node is another option for the attacker to gain control of the network. Tamper proofing the node's physical packaging is one way to prevent this kind of attack, although such protection is typically rarely implemented owing to the expensive expense of such measures. Therefore, sensor node compromise should be included into the security architecture.

7.2 Link Layer

Multiplexing, frame detection, medium access, and error control are all tasks that fall within the purview of the data link layer. It safeguards the integrity of communication links between individual nodes and between nodes in a network. This layer is vulnerable to the following attacks

7.2.1 ***Collisions***

When two or more nodes try to use the same radio frequency at once, an interference or collision results. When packets collide, the data within may be altered, leading to a checksum mismatch when the two packets are finally received. The package will be deemed invalid and thrown away. Collisions in certain packets, such as ACK control messages, may be intentionally caused by an attacker.

The employment of error-correcting codes is a common anti-collision measure. However, there is an extra computational and communication cost associated with using these codes. An adversary may almost certainly compromise more data than can be repaired at any one time. There are currently no effective countermeasures known to exist.

7.2.2 ***Exhaustion***

An attacker may drain resources via repeated collisions as well. A simple link-layer implementation may, for instance, keep trying to send the same faulty packets over and over again. Unless these fruitless retransmiss- ions are detected or stopped, the energy reserves of the transmitting node and those around it will be swiftly drained.

Applying rate restrictions to the MAC admission control might help solve this problem by allowing the network to ignore excessive requests and therefore save power. Second, time-division multiplexing may be used such that each node has its own dedicated transmission window. However, it may still be damaged by impacts.

7.2.3 *Unfairness*

7.3 An adversary may introduce bias into a network by sporadically launching one of the aforementioned link-layer assaults. The DoS attack is weaker in this case. Degrading it may give an attacker a leg up, for example by making other nodes in a real-time MAC protocol miss their transmission deadline. By limiting the time an attacker has to take control of the communication channel, tiny frames mitigate the impact of these types of assaults.

7.4 Network and Routing Layer

7.4.1 The following guidelines are often used when designing the network and routing layer of sensor networks:

7.4.2 • Power consumption should be minimized wherever possible.

7.4.3 • Information plays a crucial role in sensor networks.

7.4.4 • The best sensor networks know where they are and can address sensors based on their attributes.

7.4.5 The following are examples of attacks against the network and routing layer:

7.4.6 *Spoofed, Altered, or Replayed Routing Information*

Attacking routing data in transit between nodes is the most straightforward method of disrupting a routing protocol in any network. An attacker may cause traffic disruption by spoofing, modifying, or replaying routing information. These disruptions include the formation of routing loops, attracting or repelling network traffic from chosen nodes, extending and shortening source paths, creating bogus error signals, splitting the network, and increasing end-to-end latency.

Including a message authentication code (MAC) at the end of a transmission may prevent spoofing and tampering. A communication's legitimacy may be confirmed by its recipients with the use of a message authentication code (MAC).

7.4.7 whether there was any tampering with the communications. Information on the MAC will be provided below.

7.4.8 *Selective Forwarding*

7.4.9 In multi-hop networks, a key assumption is

7.4.10 that every node in the network will faithfully relay communications. An adversary may plant malicious nodes in the network, which would only relay specific messages while discarding the rest.

7.4.11 Using several pathways to transmit data is a good way to prevent selective forwarding attacks. The second line of defense is to identify the bad node or to presume it has failed and look for an other path.

7.4.12 *Sinkhole*

An attacker conducting a sinkhole attack will forge routing information to make a compromised node seem more desirable to neighboring nodes.The outcome is that other nodes will choose the hacked node as the node via which to send their data next. When an attacker can force all traffic from a significant section of the network to pass via their node, selective forwarding becomes trivial.

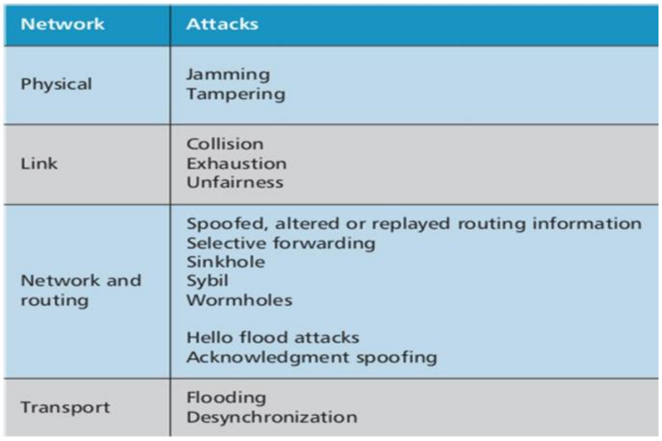
7.4.13 *Sybil*

In a Sybil attack, a single node pretends to be many different entities inside the network. Fault-tolerant protocols, distributed storage, and network-topology-maintenance techniques are all vulnerable. In order to provide a certain amount of data redundancy, a distributed storage system could need three copies of all data. Algorithms may falsely determine redundancy has been achieved if a hacked node masquerades as two of the three nodes.

7.4.14 *Wormhole*

A wormhole is a low-latency link between two points in a network that may be used by an attacker to repeat messages between those points. This link may be established by direct communication between two nodes in different parts of the network, or through the use of a relay node to send and receive messages between two nodes in close proximity but are not directly connected. In the second scenario, a node adjacent to the base station may use a sinkhole attack technique to provide another node in a faraway part of the network a direct link to the base station. To identify and prevent wormhole attacks, packet leashing is utilized. There are now geographical leashes and temporal leashes available. WSNs are also suitable for the suggested mechanisms.

Table 2: Sensor Network Layers and Denial of Service Defenses.



Network	Attacks
Physical	Jamming Tampering
Link	Collision Exhaustion Unfairness
Network and routing	Spoofed, altered or replayed routing information Selective forwarding Sinkhole Sybil Wormholes Hello flood attacks Acknowledgment spoofing
Transport	Flooding Desynchronization

7.4.15 Hello Flood Attacks

7.4.16 Many systems that rely on HELLO packets incorrectly assume that the sender is a neighbor simply because they are in radio range. An attacker may employ a high-powered transmitter to mislead a vast region of nodes into thinking they are neighbors of that transmitting node. Even though many of these nodes are really out of radio range from the attacking node, they will all try transmission to the attacking node if the attacker fraudulently broadcasts a better route to the base station.

7.4.17 Acknowledgment Spoofing

7.5 Acknowledgments are a feature of various sensor network routing methods. Overheard packets meant for nearby nodes may be spoofed by an attacker node, giving other nodes incorrect information. Claiming that a node is alive while it is really dead is an example of such misleading data.

7.6 Transport Layer

7.6.1 The transport layer is in charge of handling all of the handoffs between nodes. Both flooding and de-synchronization are mentioned as potential assaults on this layer.

7.6.2 Flooding

Any time state must be maintained on either end of a connection, a protocol opens itself up to memory corruption attacks. flooding-induced fatigue. An attacker may flood a system with connection requests until its resources are used up or a predetermined limit is reached. Maximum allowable. One possible solution to this issue is to have all connected clients prove their dedication to the connection by answering a riddle. The goal is to ensure that a connected client doesn't squander resources by establishing connections that aren't essential. There is more processing time involved due to these challenges, but this method is preferable than extensive communication.

De-synchronization

27. The term "de-synchronization" describes the breaking of a previously stable link. It is possible for an attacker to trick a target host into continually requesting retransmission of frames by sending forged messages. The attacker may degrade or even prohibit the end hosts from effectively exchanging data by timing their attacks, leading them to expend energy recovering from faults that never really occurred.

28. Having all data sent between hosts go through authentication is one way to prevent this kind of attack. Assuming the authentication procedure is safe, an adversary will be unable to deliver faked messages to target computers. Authentication is elaborated upon further down.

29. CRYPTOGRAPHY

8.1 All security services in WSNs are guaranteed by cryptography, making it crucial to choose the most suitable cryptographic technology. WSN cryptography should be analyzed in terms of code size, data size, processing time, and power consumption to ensure it is efficient and does not overburden sensor nodes. Here, we analyze how to decide on a cryptographic method for use in WSNs. This article focuses on two subfields of cryptography:

8.2 Cryptography, Symmetric and Asymmetric Key

8.3 Symmetric Key Cryptography

A method of communication encryption and decryption in which the sender and recipient both have access to the same key. In contrast, public-key cryptography relies on a pair of keys—a public key for encryption and a private key for decryption—to secure communications.

The fundamental downside of symmetric-key systems is that they need an insecure method of key exchange between the two parties, while being easier and quicker to implement. This is not an issue with public-key encryption since the public key may be shared insecurely and the private key is never sent over the network.

Secret-key cryptography is another name for symmetric-key cryptography. The Data Encryption Standard (DES) is by far the most widely used symmetric-key scheme

Public key cryptography's use in WSNs is constrained by the computational and power requirements of sensor nodes. As a result, symmetric key cryptography has been the primary focus of sensor network research. Six different microprocessors with word sizes ranging from 8 bits (Atmel AVR) to 16 bits (Mitsubishi M16C) to 32 bits (StrongARM, XScale) were used to test five standard encryption techniques. The speed of each algorithm's execution and the amount of memory used by its code were measured. The trials showed that the cost of cryptography was the same across all categories of encryption and all categories of architecture. and ((((((((" and (in " In addition, the overhead for hashing techniques (MD5 and SHA-11) was almost an order of magnitude greater than that for encryption methods (RC4, RC5, and IDEA).

Symmetric key cryptography is preferable in a WSN because of the limitations of sensor nodes.

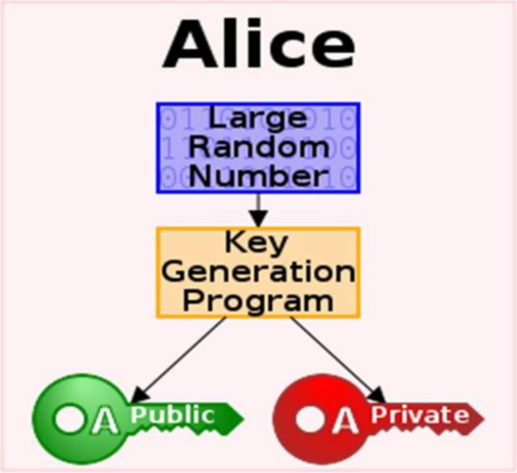


Fig. 4. Public Key Cryptography.

8.4 Public Key Cryptography

One definition of public-key cryptography is any cryptographic system that makes use of a pair of keys, one of which is kept secret while the other is made available to the general public. The two keys make up a pair that is mathematically related despite their apparent dissimilarity. The cipher-text may be locked with one key and unlocked with another. Neither one of the keys can do both by itself. The private key must be kept secret, but the public key may be made public without compromising security.

Public key algorithm approaches, such as the Diffie-Hellman key agreement protocol or RSA signatures, are often seen as unfavorable for use in WSNs because to concerns about code complexity, data size, processing time, and power consumption.

In order to complete a single security action, public key algorithms like RSA often execute hundreds or even millions of multiplication instructions. Furthermore, the amount of clock cycles needed to execute a multiply instruction is a primary determinant of a microprocessor's public key algorithm efficiency. Brown et al. discovered that restricted wireless devices are susceptible to DoS attacks because public key techniques like RSA take on the order of tens of seconds to execute encryption and decryption operations. Contrarily, Carman et al. discovered that even a microprocessor's most basic multiply function yielding a 128-bit output often consumes

30. computing resources than public key methods, functions are far more efficient.

31. In comparison, it is predicted that encrypting a 128-bit AES block uses just 0.104 mJ of energy on the same MC68328 DragonBall processor used for the 1024-bit RSA encryption

32. Recent research has shown that with careful algorithm and parameter selection, optimization, and low-power approaches, public key cryptography may be used to sensor networks. Elliptic Curve Cryptography (ECC), RSA, and Rabin's Scheme are some of the public key algorithms that have been studied. Most research in literature concentrate on RSA and ECC algorithms. ECC is appealing because it can provide the same level of security with a much lower key size, which in turn reduces processing and communication overhead.

33. Although public key cryptography could work in sensor nodes, the cost of public key operations prevents widespread use at now. In certain implementations, the assumptions may not hold true. Therefore, we no longer use its utilization.

34. INTRUSION DETECTION

Data security requires more than just authentication and encryption. Another technique to defend WSNs comprises systems for detecting and responding to intrusions.

An Intrusion Detection System (IDS) keeps an eye on a host or network in search of unusual or malicious behavior. IDS works on the premise that malicious and benign network users exhibit distinct patterns of behavior that may be matched by a set of rules, either hardcoded or learnt over time. Ad hoc network IDSs may be broken down into rule-based and anomaly-based categories, depending on the kind of analytical model used to sift through audit data in search of intrusions. When looking for intrusions, rule-based systems look for established patterns, whereas anomaly-based

thousands of nano-joules. Hash functions and symmetric key cryptography

systems look for anything out of the ordinary. The false-alarm rate of a rule-based IDS is lower than that of an anomaly-based system, but the intrusion-detection rate of an anomaly-based IDS is higher than that of a rule-based system.

However, WSNs are often designed for a single purpose and hence lack fundamental details such as topology, typical operation, anticipated communication patterns, etc. Preloading sensors with a set of predetermined patterns is unrealistic.Learning and detecting these factors after deployment is also time and resource intensive because of sensor limitations. So, it's possible that current ad hoc network IDSs can't be modified for use with WSNs. Intrusion detection in wireless sensor networks is still in its early stages of study. Current

The goal of this study is to identify and remove intentionally fabricated data. Keep in mind that every sensor network is vulnerable to having false information injected into it by hacked nodes. In order to determine the reliability of a report, it is required for sensors, and particularly nearby nodes, to work together. Intrusion detection methods for WSNs are discussed here.

35. INTRUSION DETECTION IN WSNS

Interleaved hop-by-hop authentication (IHOP) is a method suggested by Zhu et al. If less than t of the nodes are compromised, the IHOP protocol ensures that the base station will identify any spoofed data packets. The sensor network is structured in a hierarchical clustering fashion. Each cluster leader creates a path to the hub, and every node in between has an associate node that is closer (by t hops) and one that is farther (by t+1 hops). IHOP requires the following sharing keys to function properly:

Each node has a secret key that it shares with the network's hub, and it has also formed a pairwise key with each of its immediate neighbors.

• A pair wise key may be established between a node and a node that is many hops distant. In addition, IHOP presumes that the base station provides a method for verifying the authenticity of broadcast messages (like TES -LA).

When at least t+1 sensors detect the same outcome, the cluster head compiles the data from its nodes and reports it to the home base. Additionally, a cluster head gathers MACs from nodes that do detection. Two MACs, one using the key shared with the base station (the individual MAC) and one using the key shared with its higher associate nodes (the pair wise MAC), are sent from each detecting node to the cluster head. The cluster head then XORs together the t + 1 individual MACs to condense the report. The pair wise MACs, however, are not sent with any compression. A relaying node wouldn't be able to extract the pair wise MACs of relevance to it if they were encrypted. This means that a valid report will include both the base station's compressed MAC and the t + 1 pair wise MACs. An intermediate node checks the MAC of its subordinate associate node when it gets a report. If it doesn't work, the report is deleted. If not, it deletes the MAC and appends a new one generated using the pair wise key of the node's upper associate.

IHOP assures that the base station can identify bogus data packets when no more than t nodes are hacked

However, the article does not show how to select the parameter t for a sensor network.

36. FUTURE DIRECTIONS

Many applications see WSNs as a potential option, however security is typically a worry. There are still several difficulties to be resolved in WSN cryptography, key management, safe routing, secure data aggregation, and intrusion detection, despite the efforts of researchers. First, there is no one-size-fits-all solution for sensor networks since choosing the right cryptographic algorithms relies on the processing power of sensor nodes. Instead, the safeguards are tailor-made for each individual program. Second, sensors are defined by their limitations in terms of power, processing speed, storage space, and data transfer rate. These requirements must be taken into account while designing security services for WSNs. Third, the vast majority of today's protocols presuppose a static relationship between the sensor nodes and the base station. However, there may be cases when the base station and maybe the sensors need to be mobile, such as in a war setting. Many concerns concerning safe routing methods arise because the mobility of sensor nodes has such a profound effect on the architecture of sensor networks. In particular, we outline several potential avenues for further research into security concerns in WSNs.

Recent research in public key cryptography suggests that public key operations may be feasible in sensor nodes; this presents an opportunity to make use of private key operations already available in these devices. However, performing private key operations in a sensor node is still too costly. As public key cryptography may substantially facilitate the design of security in WSNs, boosting the efficiency of private key operations on sensor nodes is very desired. Streaming data safety in wireless sensor networks Security research in sensor networks is now focused on handling discrete events like temperature and humidity. Things that happen in a continuous stream, like video and pictures, aren't covered. There may not be many WSNs that use video and image sensors right now, but that may change. There will be disparities between continuous stream security and the existing protocols in WSNs due to the fact that authentication and encryption are handled quite differently for continuous events compared to discrete events.

Quality of Service and Security Adding security services to WSNs usually results in a performance drop. Key management, safe routing, secure data aggregation, and other particular subjects are the focus of much current

research on WSN security.

security breach identifiers. Security and quality of service (QoS) assessments must go hand in hand in WSNs.

REFERENCES

[1] The following is a direct quote from "Security in Wireless Sensor Networks" by Adrian Perrig, John Stankovic, and David Wagner, published in Communications of the ACM, Volume 47, Issue 6 (June 2004), Pages 53–57.

[2] "Tinysec: A Link- Layer Security Architecture for Wireless Sensor Networks," SenSys '04: Proc. 2nd Int'l. Conf. Embedded Networked Sensor Sys - tems, New York: ACM Press, 2004, pp. 162-75. [2] C. Karlof, N. Sastry, and D. Wagner.

[3] According to [3] "Assessing Security-Critical Energy- Efficient Sensor Networks," presented at the 18th IFIP TC11 International Conference on Information Security, Privacy, and Privacy in an Era of Uncertainty (SEC) in Athens, Greece in May 2003, pages 459–463.

[4]

[5] "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," by W. Du et al., "[4]" New York: ACM Press, 2003, pp. 42-51, CCS '03: Proceedings of the Tenth ACM Conference on Computer and Communications Security.

[6] To that end, consider the following reference: [5] R. Blom, "An Optimal Class of Symmetric Key Generation Sys-tems," Proc. EUROCRYPT '84 Wksp., Advances in Cryptology, New York: Springer-Verlag, 1985, pp. 335-38.

[7] "Attack Analysis and Detection for Ad Hoc Routing Protocols," by Y. Huang and W. Lee, [6]. Recent Advances in Intrusion Detection (RAIS) '04: Proceedings of the Seventh International Symposium, Sophia Antipolis, France, September 2004.

[8] According to [7] "A Performance Evaluation of Intrusion-Tolerant Routing Wireless Sensor Networks," written by J. Deng, R. Han, and S. Mishra. IPSN '03: Proceedings of the 2003 IEEE International Symposium on Information Processing Sensor Networks, Palo Alto, California, 2003, pages 349–364.

[9] "The Sybil Attack in Sensor Networks: Analysis and Defenses," by J. Newsome et al. Information Processing in Sensor Networks (IPSN '04) Proceedings, IEEE, April 2004.

[10] According to [9] "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks," published in Proc. IEEE INFOCOM 2003 in April 2003, Y.-C. Hu, A. Perrig, and D. B. Johnson.

[11] Reference: [10] "A Survey on Sensor Setworks," I. F. Akyildiz, et al., IEEE Communications Magazine, volume 40, issue 8, August 2002, pages 102-114.

[12] According to [11] "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," published in Commun. ACM, volume 26, issue 1, pages 96-99, 1983, the concept of digital signatures was first proposed.

[13] [12] IEEE Communications Surveys, 2nd Quarter 2006, "A Servey Of Security Issues in Wireless Sensor Networks," Yong Wang, Garhan Attebury, and Byrav Ramamurthy.