# Security Paradigm and Challenges in Wireless Sensor Networks: A Novel Approach

Mohd Muntjir

College of Computers and Information Technology
Taif University, Taif, Saudi Arabia
muntjir.m@gmail.com

*Abstract:* **A wireless sensor network (WSN) is a network combination of distributed autonomous devices using sensors to recognize physical or environmental trends.Sensor networks are compiled wireless networks of small and low-cost sensors that gathered and originate atmospheric data. The enhanced area of wireless sensor networks combines sensing, communication and computation into a single mechanism. The power of wireless sensor networks clarifies in the ability to utilize many numbers of small nodes that cooperate and construct all nodes. Wireless sensor networks analyze controlling and managing of physical environments from remote locations with efficiency. Security protocols related to sensor network are investigated in this paper.**

*Keywords:* **Application areas, system evaluation metrics, sensor nodes, security protocols**.

## I. INTRODUCTION

A sensor network is a synthesis of huge number of sensor nodes that are regardless extended either inside the exception or very near about to it. Arbitrary deployment in elusive domain or calamity relief operations of sensors is been done. Sensor nodes are assembling with an onward processor. On the contrary, transferring the raw data to the nodes compelling for the integration, they use their processing expanse to sectional carry out simple calculations and transmit only the necessary and partly refined data [1].

Sensors combined into machinery, structures, and the situation, consolidated with the sufficient delivery of perceived information, could maintain huge interest to environment. Lurking asset append: minimum fatal collapse, supervision of natural resources, evolved manufacturing abundance, changed emergency vibes and increased homeland security and safety. Although, barriers to the over limit use of sensors in structures and machines prevail. Bundles of lead wires and fiber optic "tails" are exposed to havoc and connector disasters. Lengthy wire bundles illustrate an expressing installation and long term conservation expenses, limiting the number of sensors that may be arranged and consequently decreasing the total aspects of the data exposed. Wireless sensor networks can eliminate these costs, improving installation and rejecting connectors. The ideal wireless sensor is associated and delivering, expanded very little capability is smart and software programmable, competent of rapid data possession, decisive and positive over the long period, expenditure short to yield and install, requires no real preservation. Selecting the ideal sensors and wireless communications link, needs knowledge of the application and penetration definition. Sensor update rates, Battery life, and size are all comprehensive design consideration. Examples of low data rate sensors collect, humidity temperature, and magnify twist secured quietly. Examples of high data rate sensors gathered acceleration, pulled, and fluctuation. The procedure of wireless sensor networks is positioned on a simple equation;

Sensing + CPU + Radio = Huge numbers of potential applications.

At the very moment, the people differentiate the abilities of a wireless sensor network; thousands of applications come to mind. It casts like a real multiplication of modern technology trend. A wireless sensor network (WSN) consists of a base station (or "gateway") that can interact with a huge numbers of wireless sensors via a radio network. Data is positioned at the wireless sensor node, decreased and send to the gateway directly or if required, uses other wireless sensor nodes to transmit data to the gateway. In turn, the gateway agent then gives the transmitted data to the system. The major aim of this chapter is to given a sharp technical introduction to wireless sensor networks and exist a few applications in which wireless sensor networks are sanctioning.

## II. WIRELESS SENSOR NETWORK ARCHITECURE

There are many topologies for radio communications networks. Some discussions of the network topologies that apply to wireless sensor networks are given below.

### A. Star Network (Single Point-to-Multipoint):

The star topology is useful in WSN, basically in the progress of Wireless Body Area Networks (WBAN).According to this topology, a main node has the liability of the allotment with the medical sensors and the communication over the BAN. The favor of this type of network for wireless sensor networks is in its clarity and the capacity to preserve the remote node's power isolation to a least possible. It also permits for low interruption communications between the remote node and the base stations. The removal of such a network is

that the base station must be within radio transmission range of all the respective nodes and is not as fit as other networks in view of its need on a single node to create the network. The star network topology, usually used in Body Area Networks (BAN) also called Body Sensor Network (BSN), where sensors are allotted on the body of a unit.


Figure 1: Star Network

B. Mesh Network:

A mesh network allots for any node in the network to transmit to any other node in the network area that is within its radio transmission domains. This network topology has the favor of reliability and excess. If a permanent node fails, a remote node still can transmit to another node in its range; can send the message to the needed location. On this contrary, the range of the network is unlimited by the range in between single nodes; it can simply be enhanced by adding more nodes to the system.

The loss of this type of network is in power exhaustion for the nodes that create the multichip communications are largely higher than for the nodes that don't have this capacity, basically limiting the battery life. Henceforth, as the number of communication merges to terminal increases; the time to change the message also increased, primarily if low power operation of the nodes is an essential. The latest enhancements in WSN are also consolidating on mesh network topology because it acquires for the broadcasting between devices without a central node for routing using a mesh of nodes. Hence, this feature rejects the central failure and collaborates self-healing and self-organization.

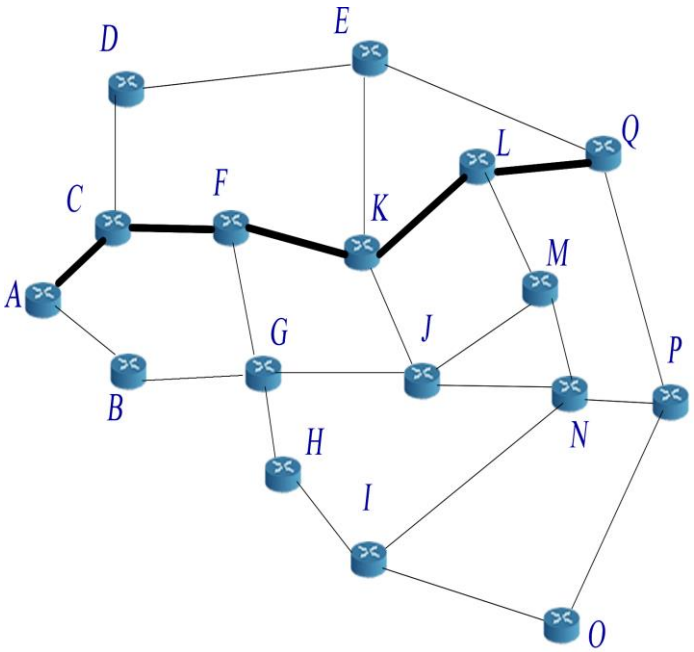


Figure 2: Mesh Network

## III. NETWORK APPLICATION AREAS

### A. Applications Classification

It might be ordered into two categories: spatial process estimation SPE and event detection (ED). In event detection, sensors are spread to emphasize an event such as an earthquake and fire in a forest, etc. [2–3]. A Signal processing within tools is very easy; each device has to compare the precise quantity with a given source and to send the binary information and other required information to the sink(s).

The frequency of nodes must satisfy that the event is recognized and transferred to the sink(s) with an applicable probability of success while managing a low probability of wrong alarms. The recognition of the phenomenon of interest (POI) could be finished in a dispensed way.

In SPE the WSN decided at calculating a given physical event that can be designed as a bi-dimensional random mechanism. It emphasizes the all nature of the spatial mechanisms based on the samples taken by sensors that are frequently combined in random positions [3–4].

## IV. SYSTEM EVALUATION METRICS

Meantime the key evaluation metrics for wireless sensor networks are full time, cost and ease, coverage of distributions, physical accuracy, response time, effective sample rate, and security.

### *A. Lifetime*

Energy is the combined factor for the lifetime of a sensor network. Each and every node must be fashioned to create its chain of local supply of energy. All Nodes can be permanently powered or self-powered.

### *B. Coverage*

Multi-hop networking protocols sophisticate the power utilization of the nodes that may decline the network for lifetime.

### *C. Cost and ease of deployment*

Wireless sensor network must compose itself. All through the lifetime of a distribution, nodes may be divided or huge physical objects may be designed so that they prevent with the communication between two nodes.

In a real deployment, a part of the total energy budget must be delivered to verification and system maintenance. The generation of individual and reconfiguration traffic depresses the network for lifetime. This can also reduce the permanent sample rate.

### *D. Response Time*

In spite of, low power operations, nodes must be adept of having prompt, high-priority messages transferred across the network as soon as possible response time must be as low as possible.

Network lifetime can be expanded by having nodes only restrain their radios for limited periods of time but it decreases the acceptance of the system.

### *E. Temporal Accuracy*

The network must be efficient of creating and managing a global time base that can be used to regularly events and order fragments. In a distributed system the energy must be shared to maintain this widen clock.

The time synchronization information must be regularly transmitted between nodes. The frequency of the synchronization messages is based on the strived accuracy of the time clock.

### *F. Security*

Encryption and cryptographic authentication are used for security, but it charged both network bandwidth and power [8-9]. The calculation must be received to encrypt and decrypt data and extra authentication bits must be transferred with each and every packet.

### *G. Effective Sample Rate*

Effective sample rate is defined as the sample rate that sensor data can be taken at each and every sensor and transmitted to an additional point in a data collection network.

In a data collection tree, a node must acquire the data of all of its descendants. Network bit rates connected with maximum network size end up smashing the effective per node sample rate of the whole system [10].

Various forms of spatial and temporal compression can be used to decrease the communication bandwidth stipulate while managing the same quick sampling rate. A Local storage can be used to combine and store data at a high sample rate for limited periods. The data can then be initialized over the multi-hop network as bandwidth permits.

## V. SENSOR NODES

The trend to manufacture, low power and low cost possessed are likely the most precise technical problem for sensor nodes.

### A. Device Classes

Two forms of device classes are Commodity devices and Custom built nodes from manufacturing-available electronics sectors.

#### *1) Commodity Devices*

Commercially available commodity devices are used to combined functions and prototypical sensor network algorithms. Furthermore, Commodity devices include mobile phones, laptop computers, PDAs and camera. Many commodity devices manage organized wired, wireless interfaces and application protocols that permit using the device's accessibility without a huge programming act.

#### *2) COTS Sensor Nodes*

COTS compresses for the custom-built sensor nodes. COTS nodes are designed from different commercially off-the shelf (COTS) electronic equipment. COTS node extension arranges commonly applicable and an adaptable sensor node.

A classical system subsists of an RF transceiver and antenna, minimum one sensor, as well as a battery and power regulating circuitry possessed around a general-function processor.

Those processors are often 8-bit microcontrollers having internal memory, leavings with some external memory.

#### *3) Sensor-Node Systems-on-a-Chip*

The research groups have recently distressed the expansion of whole sensor-node systems-on-a-chip (SOC). Such designs co-operate most sensor-node subsystems on a multiple dies or single die in one package. This coordinates microcontrollers and memories but also unique sensor designs as well as wireless receivers and transmitters. For examples of sensor-node SOCs are smart Dust, the Spec Mote, and SNAP.

B. Sensor-Node Components

*1) Processors*

A Sensor node layout have 8-bit RISC microcontroller as their major processor. The microcontroller may also have to control a condensed RF radio.

The calculating power of 8- bit microcontrollers is often as limited as to execute complex functions, some sensor nodes designs use 16 or even 32-bit microcontroller or they have additional ASICs, DSPs, or FPGAs.

*2) Memories*

Sensor nodes are basically based on microcontrollers that generally have Harvard architecture.

Maximum novel microcontroller designs feature composed data and instruction memories, but do not have a memory management unit (MMU), thus cannot increase memory security. Basically the sensor-node manufactures to increase external data memory or dependable memory just like as FLASH-ROM.

Microcontrollers used in COTS sensor nodes shelter between 8 and 512 Kbytes of non-volatile program memory and up to 4 Kbytes of volatile SRAM. Memory consumes a significant fraction of the chip; the die area is a dominant cost factor in chip manufacturing.

*3) Wireless Communication Subsystems*

Thousands of sensor networks handle radio frequency (RF) transmission; even light and sound have also been intended as physical communication medium. Sensors Boards, Sensor and Sensor Interface:

All the sensor node composes are Application-specific, General-purpose node design are minor with external interfaces. The external interface allows to connect numerous sensors or actuators correctly or to attach a preconfigured sensor board.

The sensors-node constructs are for infrared, audio, visible light, temperature, pressure, position, acceleration, (e.g., GPS).

Some common sensor types consolidate barometers, hygrometers, heart-rate sensors and oxygen saturation sensors magnetometers; Simple analog sensors are tested by the processor via an analog-to-digital converter (ADC).

## VI. SECURITY PROTOCOLS IN SENSOR NETWORKS

### A. Key Management

Key management is headmost to ensure pureness of sensor data and secured communication through cryptographic techniques random key pre-distribution, authentication protocol and localized encryption. RKP (Random Key Pre-distribution) designs have much variation. Eschenauer and Gligor introduced a key pre-distribution scheme that commits on probabilistic key allotment among nodes within the sensor network.

These system works by moving; a key ring to each and every participating node in the sensor network before formation. RKP scheme is divided into three states: first one is key setup and second is shared-key discovery, and third one is path-key establishment. Hence, it provides the key retraction phase.

• *Key Setup*

Each node's key ring acknowledges of a number of randomly chosen keys from a big pool of keys designed offline.

The main purpose of key setup phase is to assure that a limited number of keys are usable to probabilistically design a common key between two or more sensors during shared key discovery phase.

• *Shared-key Discovery*

Each node telecast a key identifier list and analyzes the list of identities possessed to the keys in their key chain.

• *Path-key Establishment*

In this establishment, a node tries to connect through intermediate nodes that already have a link created through the preceding phase.

• *Key Revocation*

A mediate sensor node can be cause for a lot of lost to the network. So reversal of a composed node is very useful in key distribution scheme.

When an opponent compromises a node, the key ring must be eliminated. Each and every neighbor should eliminate the key of a compromised node from his or her key area. Localized Encryption and Authentication Protocol (LEAP) developed by Zhu et al. (2003) as a key management protocol for sensor network. Inconsequential, robustness and energy sufficient operation, survivability are the major design targets of this protocol.

A standard implementation of LEAP (LEAP+) was designed on the Berkeley Mica2 motes. CBC-MAC is uses by the protocol for authentication and RC5 is uses for the encryption.

Four different keying structures arranged by LEAP:

1) Group Keys, 2) Individual Keys, 3) Pair wise Shared Keys and 4). Cluster Keys

The Group Key is a publically shared key that is followed by the base station for sending encrypted messages to the whole sensor network this may be stated to send queries or interests, or to create a goal to the nodes of the network.

The Individual Key is a unique key that each and every node distributes with the base station. These orders for private transmission between the base station and individual nodes, helpful for major instructions or keying material.

A Pair wise Shared Key is a key, which every node distributes with each of its current neighbors.

A Cluster Key is unique but is shared between a node and its neighbors. This is basically worked for securing private broadcast messages [12].

These keys are used under this program for secure communications that order privacy or source authentications. E.g. it could also use this key to separate a Cluster Key. The use of these keys introduces reserved participation.

### B. Cryptography & Authentication

TINYSEC Karlof et al. (2004) developed the restoration for the weak SNEP as known as TinySec and a Link Layer Security Architecture for Wireless Sensor Networks [12]. SNEP controls all services, as like access control, confidentiality scalability and message integrity.

Access control and integrity are considered through authentication and confidentiality through encryption. Semantic security is required through the use of a many initialization vector (IV) for each command of the encryption algorithm. TinySec permits for two unique variants:

TinySec-Auth, bears for authentication only, and the second, TinySec-AE, adopt both authentication and encryption. For TinySec-Auth, the whole packet is authenticated using a MAC but the charged data is not encrypted; even though using authenticated encryption, TinySec encrypts the charged data and then authenticates the packet with a MAC.

The Security Protocols for Sensor Networks (SPINS) [11] activity consists of two major threads of work: an encryption protocol for Smart Dust motes called Secure Network Encryption Protocol (SNEP) and a broadcast validation protocol that is called micro-Timed Efficient streaming learnt Authentication (TESLA).

In SPINS, each and every sensor node contributes various master keys with the base station. On this contrary, the keys need by the SNEP and the TESLA protocols are replicate from this master key.

1) SNEP is based on Cipher Block Chaining developed in the Counter mode (CBC-CTR), with the function that the initial value of the counter in the sender and receiver is the comparable.

To obtain authenticated broadcasts, TESLA uses a time-released key chain and provides authenticated cascading telecast, and Secure Network Encryption Protocol (SNEP) that arranges data confidentiality, two-edge data authentication, and data freshness with low aerial.

In Sensor Network Encryption Protocol (SNEP) the encrypted data has the following equation: E = {D}(Kencr,C), whereas D is the data and encryption key is Kencr and the counter is C. Furthermore, The MAC is M = MAC (Kmac,C|E).

The both keys Kencr and Kmac are obtained from the master secret key (K). The complete message that A sends to B is: A_B : {D}(Kencr,C),MAC(Kmac,C|{D}(Kencr,C)). Secure Network Encryption Protocol (SNEP) has aspects like Semantic security and Weak freshness, Data authentication, Replay protection, and Low transmission overhead.

2) μTESLA contend asymmetry through the delayed

disclosure of symmetric keys and serves as the broadcast authentication service of SNEP.

μTESLA needs that the base station and the nodes be closely time synchronized and each node knows an upper bound on the big error for synchronization.

The base station calculates a MAC on the packet with a key that private at that point in time. Again, when a node gets a packet, it can ensure that the base station did not yet reveal the corresponding MAC key, using its closely synchronized clock, and the time at which the keys are to be revealed and maximum synchronization error.

The node preserves the packet in a buffer and aware that the MAC key is only known to the base station, and that no contestant could have firmed some packets during the broadcasting. When the keys are to be revealed, the base station broadcast the key to each and every receiver.

Furthermore, the receiver can then validate the righteousness of the key and use it to authenticate the packet in the buffer system [11].

Each MAC key from the keys is a member of a key chain that has been created by a one way function F. Based on to create this chain, the sender choose the end key, Kn, of the chain at random and implies F regularly to calculate all other keys:

Ki = F (Ki+1)

Maintain the SNEP building block, each and every node can smoothly compose time synchronization and deliver an authenticated key from the key chain for the "commitment in a protected and authenticated manner" [12].

## VII. CONCLUSION

This paper will help the people to know about the information in detail about the sensor network and about the security protocols for WSNs: RKP, LEAP, TinySec, SPINS used and maintain in sensor network.

The above-discussed work comprises our primary work related to the security protocols. Furthermore, Open-source creations of the protocols are in the process of being made available for different work. LEAP includes collapses and what we do allegation is that LEAP is a very good solution for our problem related to Wi-Fi. The LEAP protocols are shortly available for the industry requirements; neither can

they grow into a better solution. Now days, as for wireless sensor networks, TinySec is a very important extended protocol for data link security. In this paper work a gentle key update scheme for TinySec is given based on the weight synchronization model.

## REFERENCES


[1] Akyildiz, I.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. IEEE Commun. Mag. 2002, 40, 102–114.

[2] Lucchi, M.; Giorgetti, A.; Chiani, M. Cooperative Diversity in Wireless Sensor Networks. In Proceedings of WPMC'05, Aalborg, Denmark, 2005, pp. 1738–1742.

[3] Toriumi, S.; Sei, Y.; Shinichi, H. Energy-efficient Event Detection in3DWireless Sensor Networks. In Proceedings of IEEE IFIP Wireless Days, Dubai, United Arab Emirates, 2008.

[4] Behroozi, H.; Alajaji, F.; Linder, T. Mathematical Evaluation of Environmental Monitoring Estimation Error through Energy-Efficient Wireless Sensor Networks. In Proceedings of ISIT, Toronto, Canada, 2008.

[5] Perrig, A., et al., SPINS: Security protocols for sensor networks. Proceedings of MOBICOM, 2001, 2002.

[6] Rivest, R., The RC5 Encryption Algorithm. 1994: Fast Software Encryption. P.86-96.

[7] Doherty, L., Algorithms for Position and Data Recovery in Wireless Sensor Networks. UC Berkeley EECS Masters Report, 2000.

[8] A. Perrig, R. Szewczyk, V.Wen, D. Culler, and J. D. Tygar. SPINS: Security Protocols for Sensor Networks.Wireless Networks Journal (WINET), 8(5):521.534, September 2002.

[9] Deng, J., Han, R., Mishra, S. (2004) 'Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks', The International Conference on Dependable Systems and Networks, 1 July, 2004, Florence, Italy.

[10] Karlof, C., Sastry, N., Wagner, D. (2004) 'TinySec: A Link Layer Security Architecture for Wireless Sensor Networks', Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, 03 – 05 November 2004, New York, NY, USA: ACM Press, 162 – 175.

[11] Zhu, S., Setia, S., Jajodia, S. (2003) 'LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks', CCS '03, Washington D.C., USA, 27 – 31 October 2003, New York, USA: ACM Press, 62-72.

[12] L. Eschenauer and V.D. Gligor, "A key management scheme for distributed sensor networksm" In Proceddings of the 9th ACM conference on Computer and communications security, pp. 41-47, Nov. 2002.

[13] Zhu, S., Setia, S., Jajodia, S. (2006) 'LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks', ACM Transactions on Sensor Networks TOSN, 2(4), 500-528.