International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-11, Issue-5 (October 2021)
www.ijemr.net https://doi.org/10.31033/ijemr.11.5.7

Review of Wireless Sensor Networks

Khairi Salem Ahmed
Faculty of Science, Department of Information Technology, Bani Waleed University, LIBYA

Corresponding Author: loronjem@gmail.com

ABSTRACT

This article presents a study of the state of the art of sensor networks wireless systems, which continue to develop and present a wide variety of Applications. These networks constitute a current and emerging field of study where combines the development of computers, wireless communications and devices mobile phones and integration with other disciplines such as agriculture, biology, medicine, etc. I know presents the main concept, components, topologies, standards, applications, problems and challenges, then delves into security solutions and concludes with basic simulation tools.

Keywords-- Sensor Nodes, Security, Applications, Wireless

I. INTRODUCTION

Sensors have traditionally been elements indispensable in industrial processes due to the ability they provided to monitor and manipulate the physical quantities involved in the different production processes. The connectivity between the sensors was performed through the use of traditional wired networks. Currently the continuous technological advances have encouraged the development of devices with wireless communication capabilities, arranged in any location, more and more small, autonomous, more powerful and with a more efficient battery consumption; from there arises the wireless sensor networks (WSN, Wireless Sensor Network), which are composed of a series of thousands, even millions of sensors, called nodes, which have the capacity to storage, processing and energy limited.

The continuous development of these particular networks has caused its incorporation and use in areas very disparate. From environmental monitoring (humidity, temperature, light, etc.) essential for the development of home automation, going through military, industrial, medical or commercial [1].

In this article, we present a study of the fundamental concepts of sensor networks wireless, applications, standards main, challenges, basic problems, latest solutions raised on the subject of security, simulation tools, and others Research topics.

II. BASICS OF SENSOR NETWORKS

2.1 Definition

A wireless sensor network is a network of small embedded computer systems placed in the physical world, and capable of interact with this [2]. Gómez, [3], presents another definition as a set of autonomous elements (nodes) interconnected wirelessly, measuring variables such as movement, pressure, temperature and humidity, etc.

If the sensors used are of a size that measured in millimetres or micrometres, the technology necessary is already of the nanotechnology type. Instead of sensor networks, the name dust is often used smart (smart dust). If they are robots, they talk about fog utility (utility fog). The sensor networks are distributed in a specific area and nodes can be stationary or mobile. A network of mobile nodes, form an ad hoc network capable of routing between them. His training is by auto-configuration on a physical topology arbitrary, under frequent modification by node movements, departures, arrivals and failures participants.

Sensor networks have the following tasks typical [4]:

- Determine an environmental parameter: heat, pressure, light, radiation, presence of smoke, humidity, noise, friction
- Detect events: presence, arrival, movement, vibration, flow
- Estimate parameters: speed, direction
- Classify detected objects
- Follow the path of a detected object the network itself has no value, but the outputs.

2.2 Characteristics

Among the characteristics of the networks of sensors are the following [1], [3], [5]:

Topology and Maintenance: In general, the nodes that form the sensor networks are characterized for being randomly distributed without following no regular topology. Because of this recommends that maintenance and configuration is completely autonomous (does not require the human intervention) by using distributed algorithms.

Energy Limitations: One of the main bottlenecks that we find in the operations performed by the sensors is, the energy availability of nodes. The sensors in most cases have batteries that are characterized by not being able to be recharged, which makes this problem the main restriction when developing new protocols. Increase the lifetime of a sensor will therefore involve reducing the

levels of tolerance or limiting the precision of results obtained.

Hardware and Software Specific: The microcontroller, operating system, and applications developed for WSN's must consider energy limitations previously exposed. The operating system more used as a basis for the construction of applications in wireless sensor networks, is TinyOS [6], developed at the University of Berkeley [7].

Synchronization of Devices: So that the treatment of information that is spread by a network of sensors is carried out correctly, nodes must be synchronized. Therefore, in the WSN's must impose processes of access to the mean by multiple division in time (Time Division Multiple Access, TDMA) and sorting temporary so that the detection of the events is produce unambiguous.

Dynamic Routing: Sensor Networks must be able to adapt to changes in node connectivity. Therefore, the protocols routing used must be prepared to include or exclude nodes from your routes.

Temporal Restrictions: Although the WSN's must support real-time communications between the different nodes, this should not harm to delay characteristics, bandwidth u other quality of service parameters of networks (Quality of Service, QoS).

Safety: Considering the end use for which the sensor network is developed, the security in communications can be a very important when determining protocols that will develop in the different layers of the nodes. This is the clear example of the networks of sensors used in the military field.

2.3 Elements

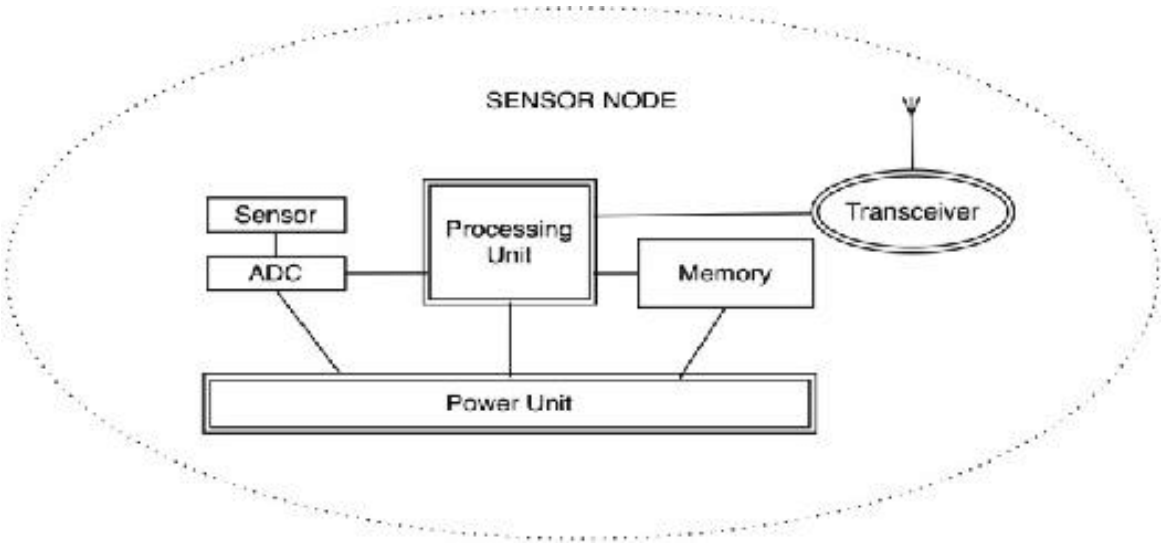

Figure 1: Components of a Sensor Network wireless

Sensors: Of different nature and technology take the information from the medium and convert it in electrical signals.

Motes: Or radio processors, take the sensor data through your gates data, and send the information to the station base.

Node: It is a sensor / mote

Gateway: Elements for interconnection between the sensor network and a TCP / IP network

Base Station: Data collector based on a common computer or embedded system.

Wireless Network: Typically based on the 802.15.4 standard, ZigBee.

2.4 Topology

Wireless sensor networks have the following types of devices [8], as shown in figure 2:

Full-Function Devices (FFD):

- Any topology
- Able to act as a network coordinator (in personal area network, PAN)
- Talk to any other device
- Reduced function device (RFD):
- Only in star topology
- Cannot be a network coordinator
- Only speak to network coordinators
- Very simple implementation.

Personal Area Network Coordinator (PAN): the main coordinator node of the network.

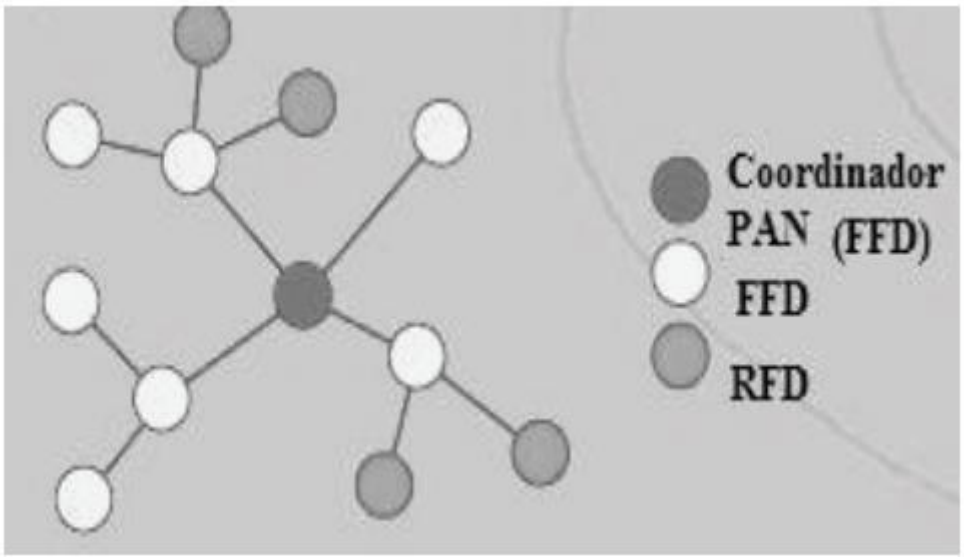

Figure 2: Device types

The topology can be mesh, star, cluster of stars, illustrated in figure 3 respectively.

Figure 3: Mesh topologies (left), star (centre) and star cluster (right).

In topologies then, there is a coordinator or direct communication between nodes (peer-topeer) [1].

2.5 Standards

The network is based on some of the standards wireless, indicated in table 1, where there will be to reach a compromise between [2]:

- Transmission speed
- Coverage
- Energy cost per package sent.

Currently the standard chosen for this type of networks, it is IEEE 802.15.4, which is supported and promoted by ZigBee [9]:

- 20-250 Kbs
- 1-100 Meters
- Up to 2 years of battery

Zigbee: Technology addressed to the needs of low-cost wireless network market based on the IEEE 802.15.4 standard, [3]. Was initiated as a non-profit industrial consortium to define global specifications of reliable, economical and affordable wireless applications low power based on the IEEE 802.15.4 standard.

2.6 Routing

Conventional distribution protocols for data or routing is not efficient in this type networks with such high restrictions on the energy consumption [8]. Instead they have developed other more specific protocols that they partly solve that problem. In a very simple, protocols based on negotiation using descriptors before transmit the information, thus avoiding part of the redundancy; direct broadcast based on reactive routing originated at destination; the one of energy saving also of the reactive type but based exclusively on probabilities of energy consumption; the multipath based on increase network availability when the optimal path is not available; and finally Control of access to the medium but specific to sensor networks and called: S-MAC . [5]

Routing on Networking Ad hoc Wireless: [10] A Wireless Ad Hoc network is understood as a set of distributed nodes randomly in a D-dimensional space. On the same, communication can be generated by any node of the network, which therefore acts as source, to any other node, which assumes the target paper. This communication occurs using a multi-hop scheme in which the data are relayed by a series of nodes intermediate until reaching the latter. The protocols from routing plus representative, classified according to whether it is uniform or non-uniform.

Uniform or planar structure classification, figure 5, indicates that all nodes in the network perform the same functions and possess the same characteristics. In this case, no at no cost of structure maintenance of the network; however, they adapt very little measure to extensions while preserving their same benefits.

Non-uniform classification, figure 6, is typical of hierarchical structures in which some nodes develop special roles and can even be endowed with particular capacities in terms of computing, energy or storage among others. This allows them to support more algorithms complex, reduce the overload due to communication and offer the possibility of balancing load while maintaining their characteristics even with increases in the number of nodes in network; on the contrary, they generate a certain cost of many cases the availability of nodes heterogeneous.

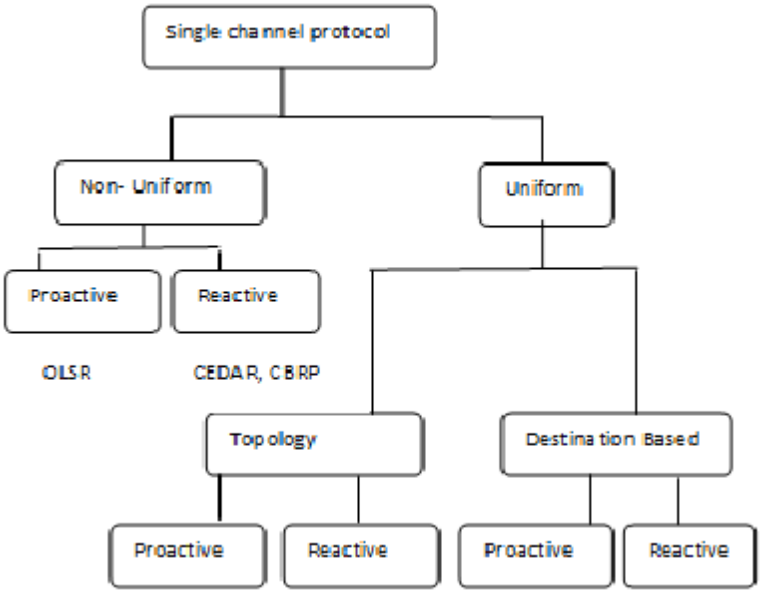

Figure 5: Uniform and Non-uniform routing protocols

In each of the classifications, in uniform and non-uniform, protocols present a new peculiarity regarding the procedure adopted for the discovery of the path to establish and its maintenance. From this point of view, you can differentiate between:

Proactive: its operation is based on tables, created from an original phase of route discovery, which house the information referring to the roads in the network based on different criteria. This information is scoped global and therefore all nodes retain possible paths to the rest. For the dissemination of the same, the nodes exchange these data either periodically or before the appearance of a change in her. Protocols assets make sending data to occur with a negligible delay due to the fact that the information about the route to follow is available previously; however, they consume resources from the network, energy, computing, storage, etc., Regardless of the degree of use of the route.

Reagent: also called "on demand". Routes are only built in the moment where a node needs to establish a communication. It is at that precise moment when a discovery phase of route that ends once the source receives the fate response including the chosen path for sending data. Maintenance cost routes decreases greatly, at the cost of introduce a latency produced by the generation initial road and a possible problem of saturation of the network as a result of the flooding of the same with route request messages

Hybrid: generally used for protocols not uniforms. Includes both procedures above at different levels of routing. Thus, it is possible to reduce the overhead of the network with control messages presented by protocols active, while the latency of search operations displayed between reagents.

In the case of uniform protocols, whether it is reactive or active, there is a classification that obeys the type of network status information that they drive the nodes for proceed to the routing. According to this criterion, a protocol uniform is based on:

Topology: nodes maintain information referred to the global set of the network. A group important of these protocols are those based on the link status, in which the information on the connections established by each node with its neighbours is disseminated throughout the network in such a way that any node knows the link scheme of the same. This approach is not optimally adapted to the dynamic nature of this type of network; without However, information of such calibre affects very positively in the selection of the best route, the load balancing or quality management service.

Destination: knowledge in this case is restricted at the local level. The largest group among this class of protocols are called "Distance-vector" since, instead of

paths complete, maintain a certain measure of distance to different destinations (usually the number jumps) and the direction vector towards them (the identifier of the next hop node).

Position: knowledge of each node is based on the geographic coordinates of himself and the rest. The principle of routing consists of the sequential approach to the destination by implementing jumps to the neighbour that is closer to it. In topology networks homogeneous is a very efficient technique; without However, in the presence of discontinuities u obstacles must be supported by algorithms specific to improve your performance; the same time, this approach requires a system of absolute or relative positioning, which limits considerably its application.

For their part, non-uniform protocols can be classified according to the type of organization present, differentiating them according to their basis in:

Zone: nodes are grouped according to zone geographical area they occupy. Thus, the path to scope maintenance overhead local of the same. Once again, you need the knowledge of the position of the nodes and the consequent system that provides it.

Group: the association of nodes is carried out around one of them (cluster head) who acts as leader of the group, taking responsibility for the high and low nodes in the group and of certain functions routing hierarchies. This hierarchy reduces network control overhead from nodes that, in most cases, require capabilities wider than the rest.

Spinal Column: a set of nodes are dynamically selected to form a backbone of the network. To said nodes are assigned special functions such as construction of roads and the spread of control and data packages. The rest of the nodes are supports them to carry out their establishment of path for desired communication. One more time, a high capacity to adapt to network extensions and control of the routing at a lower cost; Conversely, a certain expense of structure maintenance.

III. SECURITY PROBLEMS AND SOLUTIONS

Below is a study of the main problems and latest solutions raised on the issue of security in network wireless sensors, key management and encryption, analysis of handling mechanisms of keys, authentication and discovery.

a. Key Management and Encryption

Much of the security implementations in WSNs, they use encryption and handling schemes of keys. The main problem to solve is make the management scheme efficient enough so that if a intruder manages to capture a node, it is not possible access all the keys of the network and therefore the confidential system information. The different authors investigating solutions for WSN security, they perform assumptions regarding the capacity of different nodes. As stated above, the sensors possess capabilities from processing, storage and a source of limited energy, however, it is possible to find a small group of nodes, whose resources are not are so limited, called superior or cluster head (cell). For these cases, the network it is heterogeneous [19], [20].

Unlike [13] where only one is used Key pool, in [17], two pools are managed, one transmission and one return. Before the deployment, each node is given, randomly, two rings of m / 2 keys of each pool (where m is the total number of keys per node). The pools are updated through a Hash function [11], after a period of time or generation. Each pool has P / 2 keys, where P is the total number of keys in the system. The Return keys are generated using string Lamport based on Hash [12], starting with the keys that correspond to the latest generation. After deployment, each node starts the recognition of your neighbours by sending a message with your ID and the generation number in the which was deployed. If a neighbour finds keys common, send a reply message with your ID and his generation.

Following the line, in [13] two schemes where they use different pools. The first scheme is called ABAB, due to the use of two pools of keys, A and B, and a third set (S) that is composed of the keys shared by A and B. m keys are chosen of A and are stored in a node and m keys of B and they are stored in another node. It continues the same process until all the sensors of the net.

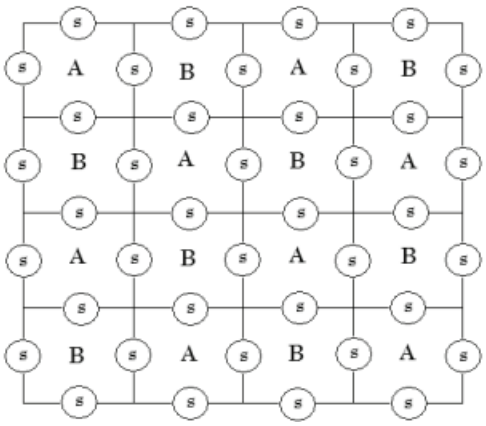

Figure 13: ABAB diagram

The ABCD scheme, for its part, uses 2r pools, where r is the number of rows of nodes to display. In this case, the set S, comprises the keys shared by the 2nd pools. The deployment is shown in figure 14. Once the deployment, the protocols of [13], [14] to establish even keys between nodes.

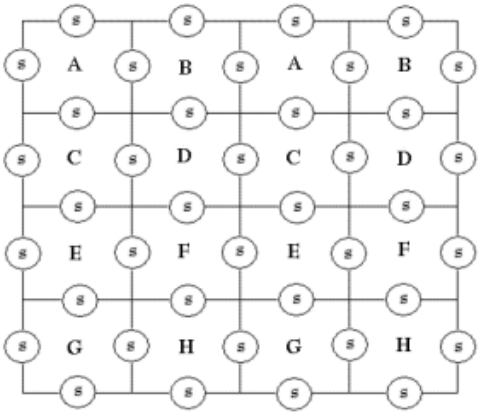

Figure 14: ABCD scheme

For encryption, in [18] it is assumed that the nodes share a symmetric key with the base station and they know the public key of the BS, in addition they have key pairs symmetric with the neighbours. Another simple consideration is found in the scheme of [19], where before deployment, select a master key and decide the maximum size of each cell. Each sensor is assigned a key, encrypted in the master key. The BS gives the nodes a group key and compute a polynomial function f (x) of a field finite or Galois GF [20], which are obtained through of m + 1 points (x, y) random (the points correspond to node locations). The functions f (1), f (2) and f (m), together with the time value current t, encrypted in the group key and without encrypt, they are sent as broadcast to the nodes. Each sensor, according to the Shamir scheme [21], determine the key with the functions received. Then check if the found key is authentic, decrypting the current time t and comparing it with the received. If it is necessary to send or renew the keys, they are encrypted with the old key. Whether finds a corrupted node, recalculates the polynomial function excluding the locations of the affected nodes.

b. Analysis of Management Mechanisms of Keys

The key handling mechanisms they use the key pool concept, they must have nodes with big capabilities from storage, which is impossible in the Insofar as the sensors have limitations in the memory. However, when the keys are renewing every certain period and the nodes that die are replaced, the number of nodes compromised decreases considerably, as in [17]. If, in addition, as in [13], work with more than one pool, which can be reused in different areas, the rings of keys of each node can increase achieving greater security and better connectivity. The mechanisms that need nodes have prior knowledge of their location, they can only be used in applications where the network is deployed in a manual and premeditated. However, they have a advantage over other mechanisms when used master keys that the attacker does not know and therefore both encryption keys cannot be generated and decryption [15].

The algorithm [19], can force the exit of a node compromised, by isolating it from the system when generates damage to the network, but its effectiveness it depends on the resources of the node. Some schemes, although they are novel, possess great computational complexity [22] or compromise chip size and increase node power consumption, decreasing its life time [23] The mechanisms that have heterogeneous networks, enjoy the advantage over systems homogeneous, the possibility of downloading the security to nodes that have greater resources processing and storage, achieving ease the functioning of common nodes and in general of the network.

Within the open topics for future work, the following aspects are found:

Improve the ability to add and remove nodes in the network without compromising system security. Reduce energy consumption, decrease header or overhead of messages generated by the different algorithms. Check the effectiveness of mechanisms in various networks and topologies. Improve policies to renew passwords that allow to reduce the time of operation.

IV. SIMULATION TOOLS

In most cases the devices used for the implementation of sensor networks wireless are characterized by being small, autonomous, very numerous and with important energy limitations. All these factors cause the analytical studies to be carried out to be very complex and experimental studies very expensive. Therefore, we see the need that exists by researchers and developers of carry out previous simulations [1] before the physical implementation of these networks.

Preliminary simulations are essential before the implementation of the WSN's, especially if this entails new protocols and functionalities network. This fact has caused a boom in simulation tools available. Without However, obtaining reliable results and representative through simulations is not a simple task.

V. CONCLUSION

With this work, an approach to the Wireless Sensor Networks (WSN) topic, that find a multitude of applications in the current society and in them converge a good number of information technologies and communications. Safety is deepened as one of the most important study topics in the networks of wireless sensors, due to the inability to use conventional mechanisms against attacks, since the sensors have resources limited processing and storage. To obtain a good degree of security in the WSN, it is necessary to jointly execute the authentication mechanisms, key management and network intrusion detection.

It is a field that is growing and evolving and where there is ample material, both for the research, such as for product development and applications. How future work will be studied more about optimization, design, deployment, distributed solutions and security in networks wireless sensors, and perform tests experiments of a model in a tool simulation.

REFERENCES

[1] Corral I. & Ana Belén. (2005). Design and implementation of a simulation environment for sensor networks wireless [Engineering from Telecommunication]. *Polytechnic University of Cartagena*.
[2] RAAP. (2020). *Wireless sensor networks*.
[3] Gomez M., Francisco. (2021). *Sensor networks wireless*.
[4] Schaeffer Elisa. (2015). *A look at the basics of optimization of sensor networks*.
[5] Franco B., Carlos. (2021). *Trends: Wireless sensor networks*.
[6] *TOSSIM*. Available at: http://www.tinyos.net/.
[7] http://www.cs.berkeley.edu/.
[8] Ruiz M., Pedro. (2020). *Introduction to sensor networks*. Available at: http://ants.dif.um.es/rm/.
[9] *Zigbee Alliance*. Available on: http://www.zigbee.org/.
[10] Vinagre D. & Juan José. (2007). Routing theory in wireless ad hoc networks. *Doctoral Thesis, Carlos III University of Madrid*.
[11] I. Mironov. (2005). Hash functions: Theory, attacks, and applications. *Microsoft Research, Silicon Valley Campus*.
[12] L. Lamport. (1981). Password authentication with insecure communication. *Commun. ACM, 24*(11).
[13] S. Emre Taşçı, E. Bayramoğlu, & A. Levi. (2008). Simple and flexible random key predistribution schemes for wireless sensor networks using deployment knowledge. In: *International Conference on Information Security and Assurance*.
[14] W. Du, J. Deng, YS Han, S. Chen, & PK Varshney. (2004). A key management scheme for wireless sensor networks using deployment knowledge. *IEEE Infocom*.
[15] Y. Ho Kim, H. Lee, & D. Hoon Lee. (2007). A secure and efficient key management scheme for wireless sensor networks. In: *Security and Privacy in Communications Networks and the Workshops, Secure Comm 2007. Third International Conference*, pp. 17-21.
[16] J. Young Chun, Y. Ho Kim, J. Lim, & D. Hoon Lee. (2007). Location-aware random pair-wise keys scheme for wireless sensor networks. In: *Third International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing*.
[17] J. Luo, P. Papadimitratos, & JP. Hubaux. (2008). GossiCrypt: Wireless sensor network data confidentiality against parasitic adversaries. In: *5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*.
[18] X. Yi, M. Faulkner, & E. Okamoto. (2008). Securing wireless sensor networks. In: *Third International Conference on Availability, Reliability and Security*.
[19] MIT open Course Aware, Chapter 7: Introduction to finite fields. *Electrical Engineering and Science Computing*.
[20] A. Shamir. (1979 Nov). How to share a secret. *Communications of the ACM, 22*(11), 656-715.
[21] A. Hamid, M. Mahbub Alam, & C. Seon Hong. (2007 Feb). Developing a security protocol based on LCG and orthogonal matrices for wireless sensor networks. *The 9th International Conference on Advanced Communication Technology*.
[22] DE Knuth. (1985). Deciphering a linear congruential encryption. *IEEE Transactions on Information Theory, IT-X*(1), 49-52.

