University of Thi-Qar Journal Vol.12 No.3 SEP 2017
Web Site: https://jutq.utq.edu.iq/index.php/main
Email: journal@jutq.utq.edu.iq

A Survey on Security Challenges in Wireless Sensor Networks

Rana Hameed Hussain1
1 Dep. of Computer Science, Faculty Science Computers and Mathematic, Thi-Qar University
Rana_hameed2003@yahoo.com

Abstract

Wireless Sensor Networks(WSN) have seen widespread, so it became an important part in our daily lives. It has many characteristics distinguish it from other types of networks, Such networks help us know more about our environment, this could lead us towards a better and easier life. Wireless sensor networks is one of the best candidates among other networks. It's features are by sensing tasks from small scale, centralized and expensive to large scale, distributed and low-cost by using small battery to power sensors with wireless links. Because of the special nature of these networks emerged a number of security holes contribute to facilitate the penetration, which makes it imperative to reconsider the security aspects of these networks. This paper aims to show the security challenges in the wireless sensors networks and means to face it through the most prominent research achievements in this field.

Keywords: wireless sensor network ,security ,black hole ,node, attack

1. Introduction

Wireless sensor networks are different in terms by the data they collect, sensors able to collect data of the temperature, humidity percentages, the movements of vehicles, lighting levels, degrees of atmospheric pressure, and level sounds. This diversity in the abilities of sensors have led to the emergence of a large segment of the applications include home applications,

industrial applications, as well as the military applications, so sensors can use to explore and control the movements of the enemy on the battlefield, monitor the animals and plants in environmental reserves, in addition to its role in the discovery of fire and determine cyclones sites, helping to avoid natural disasters. On the other hand, wireless sensor networks play a critical role in medical applications that rely on sensors to monitor patient vital signs. Wireless sensor networks are also used in security applications that enable sensors to detect intrusions and security threats.

2. The Need to the Security

Security is the most important priorities provided in wireless sensors networks applications, there is a fundamental requirement for insertion the security as a key element in the design of wireless sensor networks , to ensure the safety of operations, confidentiality of sensitive data, and the privacy of persons in the network. The sensors was distributed in large-scale environments that may be sometimes forceful battles area, for example makes wireless sensor networks easy victim to various forms of security attacks tapping on the data transmitted through the network or feed the network with false data. All the wireless sensor networks applications require being effective, safe and able to adapt to network failures.

Achievement the security in wireless sensor networks by provide physical protection for the sensors, protection of communications between network components, finally data protection [Sangeeta and Mohammad ,2014]. It can summarized security requirements [Suhail Ahmad,2015] [Platon & sei,2008] [Kavitha and Sridharan ,2010] for wireless sensor networks in the following points :

1. **Confidentiality of data:** means hide the data from unauthorized persons to look at it.
2. **Advanced security:** means prevent any node of reading any message after leaving network.
3. **Backward security:** means prevent any new node to read any old message quoted by the join node of the network.
4. **Data authenticity:** include ensuring the receipt of messages from reliable **sources.**
5. **Authorization:** allow only authorized nodes to join in the work of the network.
6. **Access control:** prevents unauthorized access to network resources.
7. **Data integrity:** it makes sure the data intact and has not been vandalized or altered during transmission through the network.
8. **Data freshness:** all data and messages exchanged must be modern and prevent re-write old data.
9. **Degradation of security service :** means the network's ability to change the degree of security based on the change in the resources available network.

[Mohammad and et al. 2015] classified security means that applicable to wireless sensor networks to :

1. **Preventive measures :** it prevents security breaches from happening or to make it at least a difficult task.
2. **Revealing measures :** it will enable the network to detect intrusions when they occur and to differentiate between them and the failures of unintended.
3. **Interactive measures:** which may vary from a freeze on all jobs of the network to avoid future danger for more complex mechanisms

also to disable the affected part of the network with the rest of the parts work continuous.

The degree of security available in different wireless sensor network based on the key factors [Eric and Yuichi,2008], including:

1. The nature of the region, which sensors have been published in.
2. Availability of monitoring stations in the network.
3. The number of constituent nodes of the network, their characteristics, and their movements.
4. Possibility of attacks.
5. Protocols that used in network management.
6. Programmatic security requirements for the application that use the network.

3. Constraints of Security in Wireless Sensor Networks

In this part of the research restrictions that make achieving security in wireless sensor networks is complex and elusive.[Idrees and et al,2013] [Chen and et al. 2009] [Kavitha and Sridharan,2010]

1. **Constraints of sensors:** which are characterized by limited resources with respect to energy resources, processing speed, storage capacity and communication channels, which creates a conflict between reducing resource consumption and raise the level of security in the network. Also, this is a quick failure and tamper-resistant sensors. The complex is more than whether the sensors are subject to movement and move from site to another intrusions, that arise from a moving contract be difficult discovery. In addition to the high number of sensors used in the network and that is deployed in large areas and

harsh environments increase the chances of exploitation of network security loopholes and there is no need for distributed security management rather than depending on configuration a central security point.

2. **Constraints of Network:** geographic network is constantly changing, making it easy victim for the breakthroughs that can come about from all directions Unlike wired networks where the gates and firewalls to protect its borders are available. The addition or delete the nodes in continuous manner it is creates an unfixed routing structure, in addition to the adoption of wireless sensor networks to wireless communications that suffer from many security gaps.
3. **Physical Constraints:** which is arise from the deployment of sensors in an open and harsh environments, making it vulnerable to damage and captivity in addition to, the sensors don't have any protection and resistance the sabotage because of the industrial cost is high.

4. Classification Of Security Attacks

Wireless sensor networks are exposed to various forms of security attacks can be classified in multiple aspects. Attacks are classified in terms of its activity to: the passive attacks and active attacks, [David., and Herve,.2010] [Kavitha and Sridharan,2010] passive attacks which are viewing data only, without directing damage or alteration while active Attacks which are to damage , modify data and exploitation of the communication process. According to the security requirements network attacks can classified [Chih-Chun and et al. 2008] to data confidentiality, data authenticity attacks, continuous attacks on the network, and hidden attacks are targeting the integrity of network services. [Marcos and et al ,2010] are classified attacks into two types, the first type targets the security

mechanisms that used in the network, the second type is aimed basic routing mechanisms in the network. [Rudramurthy and Aparna. 2015] [Kavitha and Sridharan ,2010] are classified attacks according to the aggressor capabilities to attacks using sensors that belong to the network or devices emulated it in ability, the attacks using more powerful devices like mobile and computer. On the other hand are classified attacks, according to access point to the external attacks outgoing from objects outside the network, and issued an internal attacks outgoing from nodes belong to the network. There are also attacks targeting different protocol layers in the network: physical layer, data link layer, the network layer, transport layer, and the layer application [Rudramurthy and Aparna. 2015] [Kavitha and Sridharan ,2010].

Any aggressor on wireless sensor networks is classified based on: motivation , purpose of the attack, as well as the knowledge and resources they have. When you go to the secure wireless sensor networks, we think about the answer to the following questions [Padmavath iand Shanmugapriya.2009]: What we seek to protect it? Do you seek to protect data exchanged and maintain confidentiality? Do we seek to ensure the survival of the network and the continuity of the work when exposed to attack what? What is the capacity owned by the aggressor? What is the strategy followed in the attack? And What are the consequences of the attack?

[Di Pietro and et al. 2009] classified according to the aggressor objectives: **curious attacker** - which seeks to see the transmitted and stored data in the network, the **polluter attacker** - which seeks to confuse and mislead the network by feeding false data, **Remover attacker** - which aims to prevent the network sink from receiving some data, **replacer** - which works to replace the correct data with fake data. The damage that causes by

security attacks vary from network to another depending on the method of deployment and compilation of data used within the network [Chun and et al 0.2008], aggressor on flat networks will not be able to control the whole network when he control on part of it, but in the hierarchical networks the aggressor maybe have the ability to controls the whole network once if he control on the root node, which confirms different security means with the different network type.

4.1 Type Of Security Attacks

In this part of the paper we highlight on the most important attacks suffered by wireless sensor networks. Where we begin the review of the targeted attacks to the protocol layers [Kavitha and Sridharan ,2010] [Kahina CHELLI,2015], then move on to the attacks that target data transmitted [Sangeeta and Mohammad ,2014] [Rudramurthy and Aparna. 2015] [Kavitha and Sridharan ,2010], finally we include the physical attacks against the network [Chen and et al,2009] [Kahina CHELLI. 2015] [Khushboo and,Vaishali,2015].

4.1.1 Attacks Targeted The Physical Layer

1. **Jamming**

Jamming is classified as a form of denial of service, aims through the aggressor to disable the network by transmitting a high-power signal. Jamming can be divided into types [Kavitha and Sridharan ,2010]: the **continuous Jamming:** who works on the corrupting transmitted data packets **, deceptive jamming**: which sends false data appear as legal part of transmitted data within the network, **random jamming**: which toggles between the cases of sleep and jamming to save energy, **reactive jamming**:

who is trying to send jamming signals when he feels the movement of data in the network. Aggressor may be used High-energy jamming source able to disable the whole network. If this not available, the aggressor allows uses less energy sources distributed strategically.

2. The physical manipulation

which it is easy for several reasons: the high number of sensors in large area and wide spread if it ,in addition to the lack of protection of the sensors encapsulates the anti-manipulation. When the aggressor was able to access the sensors can steal sensitive information stored on them, or to replace it with other sensors can controlled it easily . Unlike other attacks that can avoid the resulting impact, the physical manipulation produces a lasting impact cannot get rid of it.

4.1.2 Data Link Layer Attacks

1. Collisions and resource exhaustion

Collisions occur when trying two nodes transmit at the same time, on the same frequency, and when they collide the data will change, this will push the node to re-transmit data through the channel of communication in continuous manner which deprives the rest of nodes from send. if not found control on retransmission operations and stopped it, this will depleted the energy resources in the sender nodes and the neighbor nodes. This type of attack used to block network services indirectly manner if there is a situation of injustice at use resources of network [David, and Herve. 2009], the aggressor can be cause a collision by changing part of the data in the transmitted packets and so there is an error calls for retransmission. It also the collision happen when the malicious node have contrary condition from

protocol in terms of sending at any time, and malicious node may claim as legitimate node, thus acquires the powers of the transmission.

2. Interrogation

This attack exploits the handshake protocol used to achieve communication between nodes, where the aggressor unable to exhaust the resources of target node by sending a request packet transmission frequently, this will prompt the victim node to re-send a reply to the extent that consumes resources [Kavitha and Sridharan ,2010].

3. Sybil Attack

Here the aggressor will impersonate the identity of more than one node in the network which affects the reliability and validity of the data, through falsification of identity the aggressor will able to penetrate the distributor storage of data, routing mechanism used in the network, the data collection mechanism, and the distribution of resources . If false identities merged with fake sites can become the aggressor to appear in different locations of network with different identities [Sangeeta and Mohammad,2014] Which increases the probability of selecting Sybil node as part of a legitimate routing path. A set of counterfeit nodes may work to write negative reinforcements challenging the validity of the total data sent by the contract [Idrees and et al ,2013] Figure 1 shows the Sybil node that arrogate identity more than nodes.

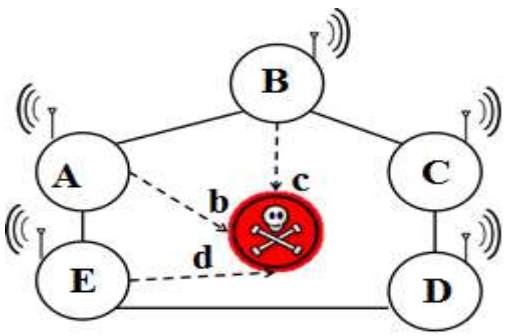

Figure1:Sybil attack

4.1.3 The Network Layer Attacks

1. Sinkhole attack

The attacker exploit routing algorithms to route the movement of data to the victim node , which work as sink node to dread away all the messages transmitted through the network. this sink - which could cut the road between the nodes and the terminal in the network-may be used to achieve the black hole or worm hole attack.

2. Hello Flood Attack

According to several of the routing protocols nodes announces its presence by sending Hello packets to its neighboring nodes, also the aggressor may proceed to use laptop - or any other device that has an antenna for sending hello packages to all nodes in the network, which deludes this node. The aggressor device legitimacy knots belong to the authorized to receive messages ,network which leads to a waste of energy node and data loss.

3. Black-Hole Attack

Wireless sensor networks using Multi-Hop routing, which means all nodes participate in message routing works to pass messages faithfully, without change its path, contract fall victim to the aggressor when he convinces it that he is just one leap to pass messages to him , upon receipt of the messages may refuse to pass some messages and neglected constituting black hole disappear inside , pass messages selectively allowed the passage of some of them and others are neglected . in Figure show 2 malicious node acts as a black hole, which mediates between clusters network [Marcos and et al ,2010]

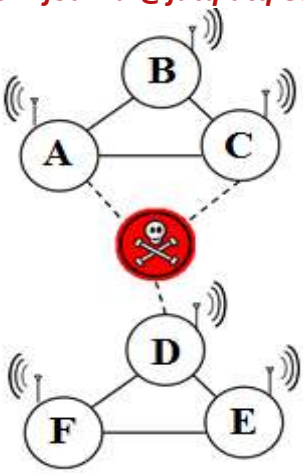

figure2: Black hole attack

4. Wormhole Attack

In this attack, the attacker creates a default tunnel pass through messages, it can be found in the tunnel by holding two nodes find in different parts of the network, increasingly dangerous hole worm when positioned aggressor in the vicinity of the base station to the illusion of nodes in the network, after that the jump one allowing him to receive all messages as shown in Figure 3 show wormhole attracts where node message without going through the contract legitimacy.

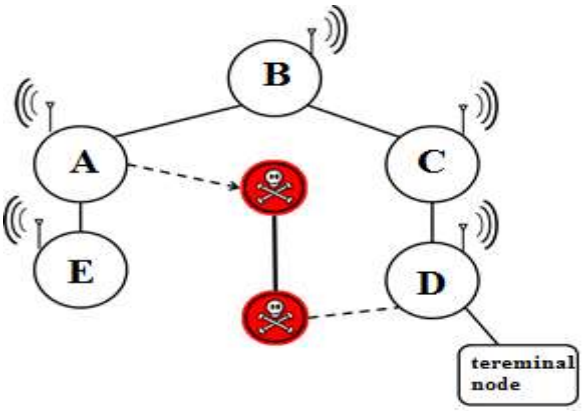

Figure 3 :worm attacks

5. False routing Attack

A malicious node is operates in the routing of data packets to send it in the wrong path to prevent their access to legitimate future. The aggressor can change the routing information as well as to create direct links in the network, also change the path lengths. Or to attract the direction of data packets to a specific node or spared them [Chun and et al,2008]

6. Acknowledgement Spoofing Attack

Wireless sensor networks require routing protocols used to approve the delivery to make sure that messages arrive. May the aggressor eavesdropping on packets of data transmitted then acknowledgement spoofing of these packages which deludes sender nodes that legitimate receiver to it, which may be out of service in the truth , then you will make sure that the aggressor will used this gap to give incorrect information on the status of the nodes in the network.

7. Homing Attack

Through data traffic in the network analysis can determine the aggressor with special responsibilities in the network contract like cluster head and keys or security manager, to be able to control the network by launching jamming and denial of service attacks on these nodes. [Kavitha and Sridharan ,2010]

4.1.4 The Transport Layer Attacks

1. Flood attack

In this attack the aggressor is repeating send connection requests to the node to exhaust the resources. It can be protected from this attack to put limited an number of connection requests sent from each node.

2. De-synchronization Attack

Which aims to disrupt the existing communications network, where the aggressor repeating send fake messages to one or both ends of the connection, pushing the node to request retransmission. If aggressor used suitable time, he can prevent the connected node to the exchange any correct information to continue to exhaust resources to correct transmission request.

4.1.5 Application Layer Attacks

3. **Overwhelm Attack**

It is occur when the aggressor is immersing the nodes by using Stimuli to the sensors which inflates the size of the node data sent to the base station. This type of attack is designed to waste energy the nodes and network bandwidth consumption. It can be minimized the effects by adjusting the sensor so that it works when there is a specific stimuli, like sensing the movement of vehicles to any random movement occurs around.

4. Deluge Reprogram Nodes

The network programming systems allow reprogramming of the nodes remotely, if this process is not secure, the attacker can does the process to control the nodes which consisting of the network.

4.1.6 Data Transmitted Attacks

In wireless sensor networks, sensors send to the base station reports of the changes that occur in the monitored parameters, these reports may be exposed to a range of attacks remind them below.

5. Interrupt

In this type of attack the communication channel will become not available. This will threatening the network to work continuity which help to achieve denial of service.

6. Interception

This attack aims , are eavesdropping or passive monitoring to penetrate the secret exchange of messages between the nodes through eavesdropping on or through control on node within the network, and data stored within it. It is difficult to discover this type of attacks because it does not make any modification to the data, but it is possible to reduce the incidence through the use of appropriate encryption mechanisms[Suhail.2015].

7. Modification

This attack threatens the validity and integrity of the data when the aggressor able to access and modify data, which creates interference between the nodes that exchange data. Aggressor may change the data sender, recipient, message content itself, or wipe some packages which spoil the message.

8. Fabrication

This attack targeted the reliability of data transmitted within the network when the aggressor feeding network with data made by him. The main purpose of this attack is to mislead the constituent nodes of the network. It is possible will help to achieve denial of service when the nodes inundated by flood of fabric packets.

9. Replay

This attack affects the novelty of the data when aggressor replay old messages to illusion the node is new. This gap is found in networks that do not use time aware protocols.

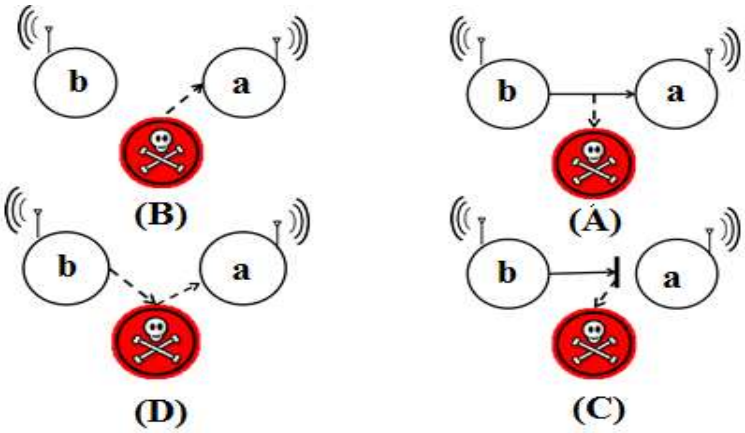

Figure4: Data Transmitted Attacks[(A) Interception (B) Fabrication (C) Interrupt (D) Modification

4.1.7 Physical Attacks Against The Network Nodes

1. Node Capture

Usually wireless sensor networks deploy in an open sites which makes them exposed to capture. Once node was captured, the aggressor can steal sensitive information stored on it, destroy them, or re-programmed. The capture one node will present the whole network to the risk. [Suhail.2015] [Davi., and Herve,2010]

2. Fake Node

The aggressor can add fake node to the network to run feeding it wrong with data, it may be able to a leads up its neighboring nodes to send their data to it. This attack consider the most serious attacks because counterfeit node

can publish malicious codes to other nodes in the network [Padmavathi and Shanmugapriya ,2009] [Davi., and Herve,2010]

3. Copy Node

The aggressor will adding a copy of node from the existing nodes in the network ,so that copy node carry the identity of the victim node, which becomes capable of falsifying routing information within the network, as well as to enable them to have access to confidential information and encryption keys, when put the copy node in strategic locations, aggressor can control different bands in network with potential for network separation [Marcos and et al ,2010] [Suhail.2015] there could be more than one copy in the same identity unlike Sybil attack which one node appear with different identities.

4. Sleep Deprivation Attack

This attack is aimed at depriving the node from the sleeping mode, leading to the exhaustion of energy resources even die. that may occur by immersing the node with a large number of messages, or request implementation dense calculations appear as if they were legitimate requests [Sangeeta and Mohammad,2014] [Idrees and et al ,2013].

5. Protection Of Wireless Sensors Networks

In this part of the research focus on some of issues related to the protection and secure wireless sensor networks, this part begins with definition of the general framework of all most security solutions, and ends with an offer to the principles work of some security systems in wireless sensor networks.

5.1 The General Framework For Design Security Solutions

[Eric and Yuichi, 2008] indicates to three main objectives in the field of secure wireless sensor networks:

(1) **management of cryptographic keys** - a critical issue, but consider a difficult task in wireless sensor networks due to the nature of random networks, broken connection, and limited resources of nodes. Traditionally, the keys are managed by reliable contributors, but the use of a single contributors in wireless sensor networks is a serious matter because it broke the contributors drop the whole network.

(2) **secure routing** - routing protocols that used in wireless sensor networks exposed to a lot of internal and external attacks, the challenge lies in finding secure protocols under dynamic geographic network, the node is heavily not immune, in addition to the capabilities of the sensors, with limited energy.

(3) **prevent denial of service attacks** - It is extremely difficult because of the ability of the penetrator to implemented the attacks in all network protocol layers. [Kavitha and Sridharan ,2010] confirms the need to secure all network protocol layers to achieve an integrated security for wireless sensors networks that the security mechanisms to be adaptable to the nature of distributed networking and dynamic composition. Also it emphasizes on importance the cost of the estimated security mechanisms not exceed the effects resulting from the security breach. While [Padmavathi, and Shanmugapriya,2009] heading to clarify two methods for the detection of security breaches:

1. **centralization approach** - which is the central node responsible for detection of penetration and then determine the necessary

mechanisms to recover this penetration and prevent it is happening in the future.

2. **distribution approach** - where all nodes shared in the discovery of the hacking, if it was happen the central node will connecting with other nodes in order to make the necessary adjustments on the network geographic and routing information. The disadvantages of the first approach it will causes an increase in the density of data traffic towards the central node, the second approach is suitable for networks that consisting of a small number of nodes, if the number of nodes was increased, the hacker can take control of the network without feeling the central node.

So design any security solution based on the nature of the network ,the target of the network and the degree of attention of the aggressors to penetrating the network [Di Pietro and et al,2009]. In addition to the cost of the implementation of this security solution, especially regard to the consumption the resources of the nodes. Where the consumption the resources of the nodes by security mechanisms. It may lead to unintended a state of denial of service in the network which is known to block the security service[Chen and et al,2009].

[Kahina CHELLI, 2015] differentiate between two types of associated energy costs for the implementation of security mechanisms:

1. **fixed costs** – it is the energy consumed in anticipation of possible breakthroughs and **variable costs** - it is the energy necessary to explore the hacker nodes and then reduction The effect on the routing information in the network. [Eric and Yuichi,.2008] summarizes range of research achievements in innovation means to secure wireless sensor networks and

mentions [Kavitha and Sridharan ,2010] some metrics that can be used in the evaluation of security solutions for wireless sensors networks:

2. **Flexibility** - an security solution should make the continuity the work of the network and protect it, even after exposure to penetrate, as it should be able to adapt to any model for the deployment of sensors.

3. **efficiently** - the security solution must not causes energy consumption the network and stopping it.

4. **Fault Tolerance** - on any security solution must continue to provide security for the network, even a crash was occur.

5. **Scalability**- the security solution should be capable of expansion without affecting the level of security

6. **Self-healing** – if the failure occur at some nodes in the network it should rearrange remaining nodes to maintain the level of security.

7. **Assurance**- means to ensure the dissemination of information to its users.

5.2 Review Of Security Solutions

This part of the research aims to provide to reader the principles of the work of security solutions that specifically designed for the wireless sensors networks like encryption and key management, secure routing protocols, the means of security service denial of service attacks, and finally the means of intrusion detection.

5.2.1 Encryption And Key Management

The encryption mechanisms that designed for wired networks are not applicable in wireless sensor networks because of the application of these mechanisms requires increase in the computational capabilities of the node, increase the consumption of energy resources and it may increase the incidence of delay in the transmission or loss of data packets [Eric and Yuichi,.2009]. [Healy and et al. 2007] suggests encryption mechanism to reduce costs by exploiting the resource available to most of the sensors the encryption unit in chip Chipcon CC2420 . On other hand [Rudramurthy, Aparna and,2015] study of energy consumption in the implementation the operations of encryption programming and they are grade practical principles to encryption in wireless sensors networks effectively. Also [Chen and et al, 2009] offers security model in which the cost of encryption appropriate with the sensitivity encrypted data and offers three security levels:

1. **First Level** - Custom for mobile code which is more data sensitivity in the network and uses most powerful encryption levels.
2. **Second Level** - that uses encryption less powerful to the location of sensors that exchanged.
3. **Third Level** - It is the lowest levels of encryption used for data special application.

It is agreed that the encryption mechanism used in the wireless sensor networks must be restrictions with the components of the network nodes, code size must be appropriate for necessary operation, the size of data that resulting from the use, the time it takes in implementation its and the level of energy they consume. The researchers [Pietro and et al. 2009],[Chen and et al. 2009] [Suhail Ahmad,2015],[[Kavitha and Sridharan ,2010] reviewed

proposal encryption mechanisms that can be apply in the wireless sensors networks. they concluded that mechanisms of symmetric cryptography exceeding the mechanisms of asymmetric cryptography it is known public key cryptography. Which is characterized by speed of implementation and reduction of the level limited resources consumption of the nodes this makes symmetric cryptography ideal choice for wireless sensor networks. However, the biggest obstacles of the symmetric cryptography was the insurance mechanisms of distribution keys process among the nodes in the network.

Application the encryption in wireless sensor networks raises some important questions regarding the management of cryptographic keys. The keys management protocols is one of more important issues in field of security wireless sensors, which requires management the keys between nodes in a secure manner and reliable. While the nodes in wireless sensor networks suffer from limited capacities, so these protocols facing challenges can be summarized in the elements the following: Key pre-distribution which may be difficult to implement due to the limited size of the memory in the sensor, Choose mechanism discovery the adjacent nodes that must be strong to prevent the hacker from exploiting the discovery of secret keys, change the key automatically which will not be easy to achieve because of the difficulty expected time needed to discover the key and the difficulty of determining the length of the period, which represents the key expires, pressing the hacking nodes which may be exploited by the aggressor to discover the key, in addition to securing direct access from node to node and the delay associated with the operations of creation the keys [Suhail Ahmad ,2015] .

In spite of the challenges facing the key management in wireless sensor networks enable many researchers to provide protocols [Khushboo and,Vaishali. 2015] classified it according to the structure of the network to

centralized protocols. and distributed protocols. According to the probability of sharing the key between two nodes to the probabilistic protocols and inevitability protocols. In centralized protocols there are something called Key Distribution Center, which is responsible to issuance and distribution of keys. The weakness of this type it can be exploited by aggressors to penetrate the network ,when hacking the Key Distribution Center the whole network fall into the hands of the aggressor. By contrast, we find that distributed protocols employs more than destination for distribution and establishment of keys. which enhances its strength in the face of penetration so we find that most of the methodology used distributed protocols. Protocol is classified as an imperative if ensures the existence of a common keys between any two intermediate nodes in the network , on the contrary probabilistic protocol that does not guarantee it.

[Chun and et al,.2009] the researchers focused on review a set of keys pre-distribution protocols as most appropriate for heterogeneous wireless sensor networks, which are the most common. And researchers offer a detailed assessment of a wide range of protocols belonging to nine different categories, to conduct the evaluation the researchers mention standards to measure the effectiveness and flexibility of the protocol summarized by: the size of memory that is consumed to store the keys, the number of processor cycles that needed for issuance the keys, the amount of data exchanged between the nodes through the process of issuance of the keys, the size of the energy consumed in the issuance of keys, ensure the correlation of nodes through availability of sharing keys among themselves, not to rely on prior knowledge of the node sites in the network, the ability to work in a wide range and easily add new nodes to the network.

There are several types of keys used in wireless sensor networks [Marcos and et al,2010] include : **Comprehensive keys**- where all network nodes share the same key that used to encrypt and decrypt all messages exchanged. **Pair wise key of nodes** - that is supposed if the node number **(x)** of neighboring nodes, so it must store (**x)** of different keys to communicate with its neighbors. **Pair wise key of groups** –it is used inside the cluster nodes shared key to communication between clusters using capital marital keys, **individual keys** - where allocated to each node private key, known only to the sink of network. We can say that marital keys stronger than the Comprehensive keys because of the fail happen the penetrate was at limited part of the network. On the contrary the Comprehensive keys may cause the failure the whole network.

5.2.2 Secure Routing

Many secure routing protocols was created for random wireless networks but they are not suitable for wireless sensor networks, because of its associated computing density and the lack of compatibility with the data traffic in wireless sensor networks [Khushboo and Vaishali, 2015]. [Kavitha and Sridharan ,2010] refers to security features that must be provide in secure routing protocols: identity verification, bi-directional confirmation, restrict on network topology, the adoption of decentralization and multi-path transmission. [Khushboo and Vaishali, 2015] adds that the protocol should be able to isolate unauthorized nodes during route discovery procedure, maintaining the confidentiality of network topology, protecting path from misinformation, prevent penetration messages exchanged during route discovery procedure, and the ability to discover fake routing messages.

It can be classified as secure routing protocols to : **flat-based routing protocols**– It gives the nodes equal roles in the routing process, **hierarchical routing protocols** - it gives nodes different roles in the process of routing process, **geographic routing protocols** - The direct data depending on the nodes location in the network. it is noted that most of the protocols serve static networks without any consideration to the possibility of nodes movement [Suhail Ahmad,2015] .

[Martins and et al, .2010] It provides detailed analysis of a set of multi-path protocols in terms of security requirements achieved through used it, in addition to identifying key management protocols and authentication mechanisms which used. Researchers have found that it is achieved authentication and integrity of data in most of the selected protocols which confirms their ability to deal with attacks such as Sybil attack and other attacks. Other researchers also refers to the need to achieve a balance between the level of security and resources consumed when choosing any protocol.

Also [Chen and et al,2009] offers professional guide assist to choose the appropriate protocol for different applications for wireless sensor networks, in precisely monitoring environment and home monitoring, medical and military applications, office applications, and monitoring production. Each protocol identifies a number of characteristics, for example, attacks that might be exposed to, a network topology, the deployment of the data model, and the level of energy consumed.

5.2.3. Protection from Denial of Service attacks

The means of protection varies depending on the network layer that will attacked. [Kahina CHELLI ,2015] [Marcos and et al ,2010] in physical

layer can be implemented using radio jamming attack or damage node physically, in the data link layer can be implemented through the collision of data packets, interrogation, and resend packets, while in the network layer can be implemented through denial service by invention routing protocol, homing attack, and flooding of hello packet. In the transport layer aggressor may be able to denial the service through immersion sensors. The following the means of protection possible in these layers.

1. **Physical layer**

It can be avoid the radio jamming by using variable frequency technology which depended on change the frequencies, it using a random sequence agreed by the parties of the network in the transmission. As well as the effective strategies determine jamming scale in the network and overdone in transmissions. it can be prevent the nodes sabotage during hide the node , disguise their appearance or use of protective packaging and anti-sabotage.

2. **Data link layer**

You can prevent collision of packets by adding error correction codes to the end of packet, but it is expected this will lead to increased transmission cost and raise the level of energy consumption. To prevent the interrogation node and the exhaustion of resources, it can put limited rate of send requests or identify the surplus or use time division multiplexing transmission to give each node a specific period of time can transmit through it.

3. **Network layer**

Routing protocols is the gap that begin from it the denial of service attacks. It can be prevented by employing mechanisms to verification of the

identities and locations nodes, By using system control to track route of the node packages in adjacent nodes to ensure they arrive.

5.2.4 Intrusion Detection

Intrusion detection systems contain an agent works as network analysis to detect any abnormal behavior of issue coming from any nodes, it works in three stages [Chun and et al ,2008] : aggregation data network phase, discovery phase which operates according to certain policy, finally reaction phase which the agent released a security warning. The policies that used in the intrusion detection : The discovery of misuse or what is known as **signature-based detection** that are looking for specific patterns indicate to existence a penetration, **anomaly-based detection** which is works on compared the behavior of nodes with pre-determined standard behavior, **specification-based detection** that ensure the functioning of the nodes in accordance with specific conditions [Sangeeta and Mohammad,2015] .

Intrusion detection systems can operate completely in distributed methodology, centralized methodology, or be combined between two methodologies [Chun and et al ,2008]. In distributed systems are installed agent in each node to be able to control its neighboring nodes and nodes may cooperate with each other in determining the alien node or take each node sends its information to the base station of the network, while in the central systems is the agent installation in the base station which operating aggregate specific data from the nodes used it in the analysis of the behavior of the network nodes, we can combination between distributed and centralized systems so that the agent installed in some of the nodes, which holds the monitoring process in addition to the normal work.

It is worth mentioning that the central systems do not consume energy because it dependence on the base station, which is characterized by an richness of resources, but they require special guidance collects data from nodes to analyze the behavior of protocols, as we find that the distributed systems increase the consumption of resources because of the presence of an agent in each node, and embedded systems mediating between the central and distributed to avoid the need for special routing protocols in addition to the reduction of the level of consumption of nodes resources.

6. Conclusion

Wireless sensor networks found their way into many commercial applications, industrial, and military. led to increased interest in providing security protection for these networks. We have explained in this research to design security solutions for wireless sensor networks is not easy, especially because of the random nature of this networks, wireless communications that known in weaknesses security, as well as limited resources.

We were offered in this paper types of attacks that threaten the security of wireless sensor networks, so far has been the development of defensive means specializes in providing some protection from these attacks, without an integrated security solution that protects wireless sensor networks from all threats faced available. When considering the security aspects in wireless sensor networks must work to achieve a balance between the cost of operation of security mechanisms and the cost of operation of network functions. There is no doubt that there is an urgent need for the development of protocols and security technologies operate within the limited resources of the network without exhausts it.

7. References:

1- Sangeeta Vhatkar; Mohammad Atique, "Design Issues and Challenges in Hierarchical Routing Protocols for Wireless Sensor Networks", Computational Science and Computational Intelligence (CSCI), International Conference on (Volume:1).**2014**.

2- Eric Platon and Yuichi Sei. "Security software engineering in wireless sensor networks**"** . *Progress in Informatics*, 5:49--64, Mar. **2008**

3- Mohammad Hossain, Umme Muslima, Humayra Islam, "Security Analysis of Wireless Sensor Network" ,A Literature Review, Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2 Issue 1, January - **2015**

4- T.Kavitha, D.Sridharan, *"*Security Vulnerabilities In Wireless Sensor Networks: A Survey*",* Journal of Information Assurance and Security, Vol. 5, **2010**

5- Khushboo Gupta,Vaishali Sikka, "Analysis Of Security Threats In Wireless Sensor Network", International Journal of Computer Applications (0975 – 8887) Volume 112 – No 4, February **2015**.

6- Rudramurthy V C, Dr. R Aparna, "Security Issues and Challenges in Wireless Sensor Networks: A Survey." International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 10, October **2015**

7- Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou*,"* Sensor Network Security: A Survey**"**, IEEE Communications Surveys & Tutorials, Vol. 11, No. 2, Second Quarter **2009**

8- Idrees S. Kocher, Chee-Onn Chow, Hiroshi Ishii, and Tanveer A. Zia: "Threat Models and Security Issues in Wireless Sensor Networks".

International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October **2013**

9- Suhail Ahmad Shah," Security Issues and Challenges in Wireless Sensor Networks (An Overview)", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 7, July **2015**

10- Roberto Di Pietro, Luigi V. Mancini, Claudio Soriente, Angelo Spognardi, and Gene Tsudik, "Data Security in Unattended Wireless Sensor Networks**"**, IEEE Transactions On Computers, Vol. 58, No. 11, November **2009**

11- David Martins., and Herve Guyennet ,"Wireless Sensor Network Attacks and Security Mechanisms : A Short Survey**"**. 13th International Conference on Network Based Information Systems, **2010**

12- G. Padmavathi, D. Shanmugapriya: "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" , International Journal of Computer Science and information security", Vol.4, pp.117-125, August **2009**

13- Chih-Chun Chang, Sead Muftic, David J. Nagel, "Security in Operational Wireless Sensor Networks", Consumer Communications and Networking Conference (CCNC), **2008**

14- Marcos A. Simplício Jr, Paulo S. L. M. Barreto, Cintia B. Margi, Tereza Cristina M. B. Carvalho**.** "A survey on key management mechanisms for distributed Wireless Sensor Networks". Computer Networks, **2010**: 2591~2612

15- Kahina CHELLI, " Security Issues in Wireless Sensor Networks: Attacks and Countermeasures," Proceedings of the World Congress

on Engineering 2015 Vol I WCE 2015, July 1 - 3, **2015**, London, U.K.

التحديات الأمنية في شبكات المتحسسات اللاسلكية

م.م رنا حميد حسين [1]

[1] كلية علوم الحاسوب والرياضيات\جامعة ذي قار

الخلاصة:

شهدت شبكات الحساسات اللاسلكية انتشاراً واسعاً حتى أصبحت تشكل جزءاً مهماً في حياتنا اليومية. و من المعلوم أن لشبكات الحساسات اللاسلكية خصائصها التي تميزها عن غيرها من النظم الحاسوبية، و من هذه الطبيعة الخاصة انبثق عدد من الثغرات الأمنية تساهم في تسهيل اختراق شبكات الحساسات اللاسلكية مما يحتم إعادة النظر في النواحي الأمنية لهذه الشبكات. يهدف هذا البحث إلى عرض التحديات الأمنية في شبكات الحساسات اللاسلكية و وسائل مواجهتها و ذلك من خلال استطلاع أبرز الإنجازات البحثية في هذا المجال.