Scientific Journal of Faculty of Education, Misurata University-Libya, Vol. 2, No. 8, June. 2017

Published on Web 01/6/2017

المجلة العلمية لكلية التربية، جامعة مصراتة، ليبيا، المجلد الثاني ـ العدد الثامن، يونيو 2017م

Security Challenges of Wireless Sensor Networks

Mufida Elobeidi **&** Rahil Beka

Abstract:

Wireless Sensor Network (WSN) is a collection of wireless nodes forming a network without any fixed infrastructure or centralized authority. In WSN, the sensors are free to organize themselves into a network without requiring any fixed infrastructure like base stations. It is an attractive networking option for connecting large number of sensors spontaneously..

Security in WSN is essential even for basic network functions like routing which are carried out by the sensors themselves rather than specialized routers or nearby sinks. The intruder sensor or Sink in WSN can come from anywhere with more resources availability, along any direction, and target any communication channel in the network. Intrusion prevention techniques such as authentication and encryption are applicable in the wired and infrastructure based cellular network. In the case of infrastructure-free WSN, these techniques are not applicable. The dynamic nature of the WSN also means that trust between nodes in the network is essentially non-existent. Without trust, preventive measures are unproductive and measures that are strictly on a certain level of trust between nodes are susceptible to attacks themselves. There is a need for intrusion detection and response to provide a second line of defense. Intrusion detection is the process of detecting and responding to malicious activity that is aimed at attacking the network. In this paper we have explored general security threats in wireless sensor network and analyze possible security threats.

Keys:

Wireless sensor network ,Security concept in WSNs, Obstacles of security in WSNs, Security attacks in WSNs ,Protection of WSNs .

1. Introduction:

Wireless sensor network (WSN) differ in terms of data they collect. As sensors are able to monitor temperature, humidity, lighting level and difference of sounds. This variation produced a wide range of household, industrial and military applications. By these sensors we can detect the movements of the enemy in battleground, as well as monitor animal and plants in the environmental protectorates. Also, we were able to explore and locate the tornadoes which may result in avoiding natural disasters. Furthermore, the remote-control techniques that contribute in finding out

what referred to currently as "smart houses" and their role in the security applications which enable sensors to detect security breaches and threats.

The security is the top priority the WSNs applications should have. There is a main demand to introduce security as a key element in designing these networks in order to ensure the processes of safety, data confidentiality and privacy of individual. Expansion of scope of wide usage of sensors make them easy targets to security breaches such as bugging data transmitted via network or alter or forge them, that is why these networks should be effective and secure.

In this paper we have reviewed possible attacks on WSN in general as well as attacks on specific WSN data gathering protocols. Rest of the paper is organized as follows . Section 2 Security concept in WSNs . Section 3 Obstacles of security in WSNs. In section 4 Security attacks in WSNs. In section 5 Protection of WSNs. In section 6 Threats in sensor networks and finally section 7 Conclusion the paper.

2. Security concept in WSNs

In order to realize WSNs security by a physical protection of sensors and safeguard the communication between network components, as well as protect data. Security requirements may be summarized in the following points [(1)(2)(3)]:

1. Confidentiality of data: which means to conceal data from unauthorized persons?
2. Advanced confidentiality**:** means to prevent any node reading any message after leaving the network.
3. Referential confidentiality: means to prevent any new node reading the old message transmitted after its is joining the network.
4. Data reliability: which denotes the guarantee of receiving messages from a reliable source?
5. Authorizationanddeterminationofjurisdictions: means to permit the only nodes authorized to participate in network engagements.
6. Access control: to prevent unauthorized access to the network resources.
7. Data soundness: to ensure data safety, that it isn't susceptible to sabotage or alteration during transmission via network.
8. Data freshness: means to ensure that all data and messages are new, and old data is not transmitted.
9. Non-repudiation: where no node can deny transmitting messages.
10. Network continuity: to be solid in face of security breaches.

11. Velocity to surpass infringements: the ability to ensure the continuity of the network.

Security means applicable to WSNs can be classified according to the following categories:

1. Protective means: to prevent security breaches occur or make their occurrence difficulty.
2. Detective means: to detect security breaches whenever they occur.
3. Reactive means :shutdown the damaged portion of the network.

The security degree of the WSN differs according to main factors [(4)], to mention some :

1. The nature of the area where the sensors deployed.
2. Availability of control stations in the network.
3. The number of nodes the network formed of, their characteristics and movements.
4. The possibilities of some events to occur.
5. The protocols used in running the network.

3. Obstacles of security in WSNs

These limitations make realizing security of WSNs complicated and difficult.

3.1 Sensor boundaries

It is described as limited resources in terms of energy sources, speed of processing, storage capacity, communication channels, which creates discrepancy between decreasing resources consumption and giving rise to network security level.[(5)]

If the sensors are mobile then they become more complicated, that is, the breaches arise out of mobile sensors could be difficult to be discovered, besides; the increase of the numbers of sensors used in forming the network which have been distributed in a broad areas in a way that increases the opportunities of attacking the network, so; accordingly the security should be distributed instead of depending on a central security point.

3.2 Network boundaries

The network topology is always changing and that makes it an easy target to all types of breaches on contrary to wire network which have portals and firewalls to protect its boundaries.

3.3 Physical boundaries

They are arising from distributing the sensors in open environments which make them susceptible to sabotage, in addition to their lack of protective means due to expensive costs.

4. Security attacks in WSNs

4.1 Classification of security attacks

Security attacks that the WSNs exposed to are classified in many forms of attacks in terms of their activity to : silent attacks (Negative) and active ones.(6) Negative attacks don't produce any alteration on data, while active attacks alter, sabotage and change the data. On the part of security requirements of the network, they are Classified as secret attacks and data reliability(7), attacks classified into two types : the first type takes the security mechanisms used in the network as its goal, and second type targets the main mechanisms in the network as routing mechanisms.(8) There are attacks aim at different protocol layers in the network, sensible layer, data linking layer, network layer, transmission layer, and applications layer (9), and every layer of them is exposed to different security breaches which will be dealt with next.. There are attacks aim at different protocol layers in the network, sensible layer, data linking layer, network layer, transmission layer, and applications layer, and every layer of them is exposed to different security breaches which will be dealt with next.(10)

Any attacker of WSNs is classified according to motives, purpose of attack, knowledge and resources it owns. When we engage in securing the network we should bear in mind the following questions :

What are we trying to protect ? Are we seek to protect exchanging data and safeguard their confidentiality? Are pursue to maintain the network and continuity of its work when exposed to an attack? What abilities attacker has ? What is the strategy adopted in this attack? What are the consequences arise from such an attack?

Attacker is classified according to its objectives, as follows: (11)

1. Inquisitive : seeks to get acquainted with the transmitted data stored in the network.
2. Contaminant : tries to distract and misguide the network by means of feeding it false data.
3. Remover : seeks to prevent network from receiving some data.
4. Replacer : functions to replace the correct data by false one.

Attacker is classified the according to the way of disseminating data within the network. Attacker of the flat network can't completely control it by

merely controls the nodes, while in hierarchic networks the Attacker can control the network by just control the root node.[12]

4.2 Security attack forms

we focus on the most important forms of attacks the WSMs exposed to, as we begin by reviewing the attacks that aim at protocol layer then we move to attacks that target transmitted data , and finally; we refer to sensible attacks directed against nodes of the network. [13][14][15][16]

4.2.1 Attacks against sensible layer

4.2.1.1 Radio jamming

It is one of the methods by which the attacker makes the network inaccessible by means of sending high-energy signal. Radio jam can divided into the following types : [17]

1. Continuous jamming : which sabotages transmitted data packets.
2. Deceitful jamming : sends false data which appear as a legal part of the data movement within the network.
3. Arbitrary jamming : alternates between the two types of sleeping to save energy.
4. Reactive jamming : deliberately sends jamming signals where the attackerfeels the data movement in the network.

The attacker can used a jamming source of a high energy able to shutdown the network completely, if that is not so; the attacker is able to use a low-energy sources strategically distributed.

4.2.1.2 Sensible manipulation

In which the number of sensors is high and widely distributed, in addition to that; the sensors are not protected by anti-manipulation casing so that it is easy the attacker access to sensors and stealing information stored in them or replacing them with other sensors it can control them.

4.2.2 Attacks against data linking layer

4.2.2.1 Collision and Sources consumption

When two nodes tray to transmit simultaneously on the same frequency a collision occurs, and when data packets collided then the data they carried becomes susceptible to change and that makes the node re-transmits via the communication channel continuously which causes node to not use the channel. If transmission process is not detected and seized, energy resources in transmitting nodes and neighboring nodes are exposed to be consumed

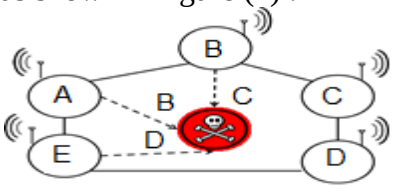
[13]. The attacker can cause collision by changing part of the data existing in the transmitted packets, and by that an error in re-transmission is resulted.

4.2.2.2 Interrogation

This attack transfers the shaking hand protocol used in achieving the communication between the nodes, as the attacker can consume the resources of the targeted nodes by transmitting data packets repeatedly, that makes the victim re-transmit the answer of receipt readiness to the extent that consumes its resources .[18]

4.2.2.3 Sybil attack

Here the attacker pretends to be more than one node in the network to affect the integrity of the data, and accordingly, be able to have access to storage of data distributor, routing mechanism, and mechanism of data aggregation and resources distribution [19], if the false identity combined with false sites then the attacker can appear in different places of the network and in different identities, as shown in figure (1) :



Figure(1) : Sybil attack.

4.2.3 Attacks against network layer

4.2.3.1Complex attack

Where attacker exploits routing algorithms to direct data movement to victim node in order to function as a complex that draws all transmitted messages in the network.

4.2.3.2 Wrong routing

malicious node which existing in the routing sends data packets in the wrong routes to prevent access to its legitimate receiver, the attacker can create routing circles within the network to change the lengths of the routings or to prevent packets access to data toward the correct node.[20]

4.2.3.3 Falsification Acknowledgement

Routing protocols require acknowledgement in order to ensure message access, attacker can eavesdropping to transmitted data packets, then falsifies

the acknowledgement of this packets, misleading the transmitted node that the legitimate receiver, who is actually out of service, has received them.

4.2.3.4 Wave attack:

By analyzing data movement within the network, the attacker can determine the special-responsibility nodes in the network as a cluster head or security keys manager in order to be able to control the network by means of launches radio jamming and blocks the service from this nodes.(21)

4.2.4 Attacks against transport layer

4.2.4.1 Flood attack

When the attacker repeats sending demands to some nodes, this attack occurs to supervise over their resources.

4.2.4.2 Desynchronization attack

Aims to disrupt communication existing in the network, as the attacker sends repeatedly fake messages to one of the communicators which makes nodes demand re-sending the message. If the attacker uses a suitable timing it can prevent communicating nodes from exchange the correct information in order to continue consumes their resources by demand re-sending the message.

4.2.5 Attacks against application layer

4.2.5.1 Confusion attack

This attack occurs when attacker immerses nodes with sensor stimulators which outsize the data transmitted from nodes to the terminal station, accordingly; wastes the node energy and consumes network band width. It can be restricted by modifying the sensors in order to respond when there are specified stimulators not merely to any random movement that may occur.

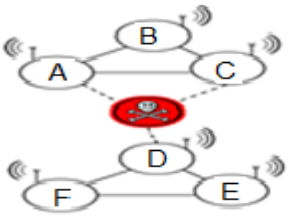
4.2.5.2 Hello flood attack

In routing protocols, nodes proves their existence by sending hello packets to the neighboring nodes, by that the attacker uses laptop or any other device with powerful aerial to send hello packets to all nodes in the network, misleading the node that the attacking device is a legitimate node belonging to the network and authorized to receive messages which results in wasting node energy and loss of data.

4.2.5.3 Sinkhole attack:

WSNs use multipoint routing, that means they suppose that all nodes participating in routing messages function to honestly pass messages without

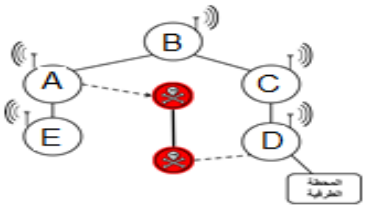
changing their route. Node becomes a victim of the attacker by believing itis one-step away to pass a message to it, accordingly; denies and neglects passing the message and forming a sinkhole that reveals the messages in a way allow some messages to pass while neglecting others, as shown in figure (2):



Figure(2) : Sinkhole attack

4.2.5.4 Wormhole attach

In this attack the adversary establishes a hypothetical tunnel for messages to pass along, this tunnel can be found by means of two nodes existent in two different sections in the network. The danger of the wormhole increases when the attacker is localized near the terminal station to mislead the network nodes it is too close and can receive all messages, as shown in figure (3) :



Figure(3) : wormhole attack

4.2.5.5 Overwhelming programming

Network programming systems allow nodes to be re-remote programmed. If this process is not secured, attacker can kidnap it to control network nodes.

4.2.6 Attacks against transmitted data

4.2.6.1 interruption

Here communication channel is unavailable which threatens continuity of network operation. It helps block the service.

4.2.6.2 Interception

Known as eavesdropping and silent surveillance, it aims at breaching the secrecy of messages exchanged between nodes by means of eavesdropping to controlling one node or its stored data. It is difficult to detect this type of

attack because it is targeted the data, it can be defeated by using cryptography mechanism.

4.2.6.3 Modification

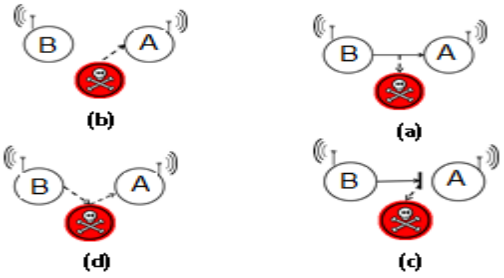
This attach compromises data integrity when the attacker have access to data to modify it creating jamming between nodes that exchanging data. attacker could alter sender and sent to data, or the message content itself or even erase some packets and spoil the message.

4.2.6.4 Fabrication

This attack aims at compromising the authenticity of data transmitted within the network, when the attacker feeds the network with fabricated data, accordingly; misleading network nodes, helping block the service when a node is immersed by flooding of fabricated packets.

4.2.6.5 Re-transmission

This attack affects the freshness of the data, when attacker re-sends old messages to mislead nodes with its freshness, as shown in figure (4):



Figure(4):attacks against transmitted data. (a) interception , (b)fabrication, (c) interruption, (d) modification .

4.2.7 Attacks against network nodes

4.2.7.1 Node capture

When WSNs deployed in open sites, which makes them susceptible to captured, and accordingly, the stored sensitive data to be stolen, so; capturing one node makes the whole network exposed to capture.[22]

4.2.7.2 False node

The attacker adds a false node to the network which subsequently feeds the network with false data, that may seduce its neighboring nodes to send messages.[23][24]

4.2.7.3 Node replication

The attacker replicates a node already replicated from one node existent in the network, as the replicated node bears identity of the victim node, and becomes able to falsify routing information within the network, and facilitate its access to secret information such as cryptography keys. There may be more than one copy with bears the same identity on contrary to Sybil attack where only one node appears in different identities.(25)

Non-tranquility

Aims at deprives node from tranquility, that leads to consume its energy resources up to death. That could happen by means of node that is immersed with a large number of messages or demands of intensive sensors tend to look as legitimate demands.

5. Protection of WSNs

In this part, we focus on some issues relevant to protecting and securing WSNs. We began by defining the general framework accordingly the security solutions function, and ended with reviewing principles of operation of some security systems in WSNs.

5.1 general frame to design security solutions

There are three main objectives in securing WSNs.(26)

1. Cryptography keys: which is more significance issue, though difficult in WSNs, due to the nature of random networks, intermitted communication, and nodes limitedness in terms of resources. Traditionally, managing keys done by an authenticated competent, but depends on only one competent compromises the network.
2. Secure routing: routing protocols used in WSNs are exposed to internal and external attacks. The challenge here is to find secure protocols under the topology of the dynamic network.
3. Prevention of denial of service: it is very difficult, that is the attacker can carry it out in all layers of network protocols. There is an emphasis on the importance of securing all network layers protocols to achieve a complete security for WSNs, as well as the importance of the cost of security mechanisms not to exceed the estimated cost of effects resultant of security breach.(27)

There are two ways to detect security breaches:

1. Central method: where a central node takes responsibility of detecting the breach, then decides the mechanisms to recover from such breach, and to ensure not to occur in the future.

2. Distributed method **:** all nodes contribute in detecting the breach. If there is any breach, they contact with the central node to take modifications needed on the topology of the network and routing information.

the negative aspects of the first method is that it increases the intensity of the data movement toward central node. The second method is suitable to networks that formed from small number of nodes. In case the number of nodes increased, the attacker can control the network without central node detects it.

Design of any security solution depends on the network nature, band and to what extent the adversary interested in attack it, besides; the cost of executing this security solution, particularly, consumption of nodes resources. Such consumption by security mechanisms unintentionally causes the services to be blocked in the network, that is known as security service block.[28] There are two types of energy costs accompanied execution of security mechanisms:

1. Fixed cost : one that is consumed when a potential breaches anticipated.
2. Variable costs : the energy needed to detect the breached nodes, and to ease the effect on the routing information within the network.

A summary of a set of research accomplishments in inventing means of securing WSNs, presented by.[29] pointed out some standards to be used in evaluating security solutions for WSNs:

1. Flexibility**:** security solution should guarantee continuation and protection of network, even after it is exposed to breach. Such solution should be able to be accommodated to any model of deploying sensors.
2. Effective energy usage**: i**n energy consumption, security solution should not cause any shutdown to the network.
3. Adaptation to shutdowns**:** any security solution has to provide security to the network even during shutdowns.

4Expansibility : security solution should be expandable without affecting security level.

5.Self-curing : if some sensors failed, the remaining ones should be re-arranged in order to maintain security level.

6. Warranty : means to ensure the information reached to users.

5.2 Review of security solutions

This section aims at furnishing the reader with the principles of security solutions designed especially to WSNs, particularly; cryptography, keys management, secure routing protocols, protection means against attacks and means of detecting sneaking.

5.2.1 Cryptography and keys management

Cryptography mechanisms designed for wire networks are not applicable to WSNs, because their application requires an increase in consuming of computer nodes abilities and their energy resources, as they may result in some delay in transmission or loss of data packets .[30] Also, it provides a security model its cryptography cost is proportionate to sensitivity of coded data, as it provides three security levels:

1. First level : designated to mobile code and uses the strongest level of cryptography.
2. Second level : uses less powerful cryptography for the sites of exchanged sensors.
3. Third level: it comes in lower level of cryptography used in data related to application.

Symmetric encryption mechanisms surpass the asymmetric ones (or what is known as general key-use encryption) in terms of speed of execution, and reduction of consumption of nodes limited resources, that makes the symmetric encryption an ideal choice for WSNs, though the big obstacles for the symmetric encryption is securing the distribution of the key between the communicating parties in the network.[31][32] As nodes in WSNs suffer from limited energy abilities, this protocol encounters with challenges which can be summarized as follows:

1. The pre-distribution of keys.
2. Selection of detection mechanism of neighboring nodes.
3. Change of key automatically.
4. And secure direct access from part-to-part, and the delay occurs during establishment of the keys.

Despite the challenges that face the key management in WSNs, many researchers succeed in providing protocols, classified, according to the network structure, to central protocols and distributed protocols, and according to the potentiality of sharing the keys between two nodes, to potential protocols and inevitable ones.[33]

In central protocols there what is called key distribution center, which undertakes distributing keys, and merely by selecting the number of key distribution center all the network falls and the attacker is captured., while the distributed protocols employ more than one entity to distribute and constitute keys that enhances its power to stand against any breach.

5.3 Secure routing

Many secure routing protocols of random wireless networks have been constituted, but they are not suitable for WSNs due to the accompanying computational intensity, besides; their inconformity with data movement in the WSNs.

That the security features should any routing protocol has, as follows : to check the identity, double-route confirmation, decentralization, multi-route transmission.(34) That this protocol should be able to isolate he unauthorized nodes during the detection process, protection route from any misleading, prevention exchanged messages to be breached during detection process, the ability of distinguishing false messages.(35)

There is a detailed analysis of a set of multi-route protocols in terms of security requirements. Researchers found out that authentication of data integrity in most chosen protocols is verified, and they ensure its ability to encounter any attacks such as Sybil attack. Researchers also emphasize the necessity of achieving balance between security level and consumed resources when selecting any protocol.(36)(37)

There is an evidence that helps the specialists in selecting the appropriate protocol in different applications of WSNs, particularly; in environment and houses monitoring, medical and military applications, each protocol designated to a number of characteristics, such as attacks it may exposed to, network topology, data deploy model, and consumed energy level.

5.4 Protection of denial of service

Protection means differ according to network layer the attack targeted.(38) In the sensible layer an attack can be launched by using radio jamming or by sabotaging node physically, and this can be defeated by mobile frequency technique which tends to change the frequencies used in the transmission by using random sequence agreed upon by the communicating parties, and nodes can protected by concealing and camouflaging them or by using a protective and anti-sabotage casing. In data link layer, attack can be carried out by data packets collision, interrogation, or re-sending packets. It is possible to prevent packets collision by adding error-correcting codes but that is expected to raise transmission cost and energy consumption. In order to prevent nodes to be put to interrogation or their resources consumed, we can put an end to rate of transmission demands to distinguish the surplus or by using multiple appositional transmission in time division to give each node a specified time period to transmit via it .

5.5 Infiltration detection

Systems of detecting infiltration contains an agent that analyzes the network in order to detect any abnormal behavior in the nodes, it works through three stages : data gathering stage, detecting stage and finally the reaction stage. The policies used in detecting infiltration is detection of malfunction or what is known as imprint detection, detecting of abnormality which compares node behavior with a standard behavior that is pre-determined, description-dependent detection which makes sure that the nodes function according to specified conditions.(39)

Detection systems can operate in a totally distributed methodology, totally central methodology or a combination between the methods. In the distributed system an agent is to be installed in each node to be able to monitor the neighboring nodes, and nodes can cooperate in determine the intruding node or stand independently in transmitting information to the terminal station in the network, while in central systems an agent is be installed in the terminal Station that operates in gathering specified data from nodes to use it in analyzing other nodes behavior in the network. Both systems can be combined in a way the agent to be installed in some nodes that engage in monitoring in addition to their normal activity.

It is worth mentioning that central systems do not consume a large amount of energy for they depend on the terminal station which has many resources, while the distributed systems raise its consumption of resources due to presence of an agent in each node.

6. Threats in sensor networks

6.1 Threat models

Through the research papers we studied and websites we reviewed which discuss WSNs, we reached out the following :

Threats in sensor networks can be classified as sensor-class (mote-class) attackers and laptop class attacker. Another classification can be made as external threats and internal threats. Mote class attackers may be sensors with similar capabilities as sensor network. These types of attackers can jam the radio link in its immediate vicinity. An attacker with laptop-class devices have greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna and hence they can affect much more than an attacker with only ordinary sensor nodes. A single laptop-class attacker might be able to eavesdrop on an entire network. External threats may cause passive eavesdropping on data transmissions, as well as can extend to injecting bogus data into the network to consume network resources and raise

Denial of Service (DoS) attack. Whereas inside attacker or internal threat is an authorized participant in the sensor network which has gone hostile. Insider attacks may be mounted by either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes and who then use one or more laptop-class devices to attack the network.[40][41][42]

Layering-based attacks and possible security approach[1]

Layer	**Attacks**	**Security Approach**
Physical Layer	Jamming and tampering	Use spread-spectrum techniques and MAC layer admission control mechanisms
Data Link Layer	jamming and collision	Use error Correcting codes and spread-spectrum techniques
Network Layer	Packet drop, bogus routing information and tunnel	Authentication
Transport Layer	injects false messages and energy drain attacks	Authentication
Application Layer	Attacks on reliability	Cryptographic Approach

POSSIBLE ATTACKS AGAINST WSN:[2]

Spoofed, altered,	Create routing loop, attract or repel network traffic,
or replayed routing information	extend or shorten source routes, generate false error messages etc
Selective	Either in-path or beneath path by deliberate jamming,
Forwarding	allows to control which information is forwarded. A malicious node act like a black hole and refuses to forward every packet it receives.
Sinkhole attacks	Attracting traffic to a specific node, e.g. to prepare selective forwarding
Sybil attacks	A single node presents multiple identities, allows to reduce the effectiveness of fault tolerant schemes such as distributed storage and multipath etc.
Wormhole attacks	Tunneling of messages over alternative low-latency links to confuse the routing protocol, creating sinkholes etc.
Hello floods	An attacker sends or replays a routing protocols hello packets with more energy

6.2 Problems Definition

There are several problems that can cause sensor attacks, however, the wormhole is the main concern in this proposal.

6.3Wormhole attack

In this attack an attacker could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. The simplest case of this attack is to have a malicious node

forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbors, leading to quick exhaustion of their energy resources. An attacker situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. Wormholes are effective even if routing information is authenticated or encrypted. , wormholes can be used to exploit routing race conditions. A routing race condition typically arises when a node takes some action based on the first instance of a message it receives and subsequently ignores later instances of that message. The goal of this attack is to undermine cryptography protection and to confuse the sensor's network protocols. We can prevent this by avoid routing race conditions. The solution requires clock synchronization and accurate location verification, which may limit its applicability to WSNs Figure (5).

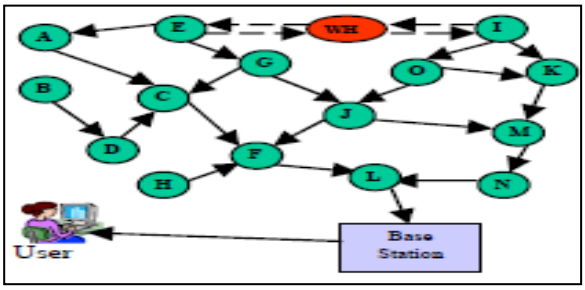


Figure (5) : demonstrates Wormhole attack where 'WH' is the attacker node which creates a tunnel between nodes 'E' and 'I'. These two

The following procedures should be followed in either to prevent any attacks and achieve high performance :

1. Traffic Analysis & Rate Monitoring to observe any possible attack attempts.
2. Data Aggregation
3. Thresholds on sensor nodes.
4. Traffic Rate control
5. Analysis Packets contents.
6. Wormhole attack detection by any simple algorithm During the wormhole attack, when one attacker receives packets at one point of the network, it forwards the packets through the wormhole link to the other attacker, which retransmits them at the other point of the network. We assume that the wormhole link is bidirectional and symmetrical so that the packets could be transmitted via either direction. Considering that if the length of the

wormhole link is less than R, both attackers are within each other's transmission range such that the packets transmitted by one attacker can be received and retransmitted by the other attacker, resulting in endless packet transmission loop. To exclude this exceptional case, we simply assume that the length of the wormhole link is larger than Figure (6).

Figure (6).**:** the wormhole link

7. Conclusion:

WSNs has made a way to many commercial, industrial and military applications, this noticeable wide spread led to attract more attention to provide secure protection to this networks. In this research we illustrated that security solution design of WSNs is not easy, particularly, under the random nature of WSNs which known with their security gaps, in addition to the limited resources. We presented in this paper the forms of attacks that threaten WSNs. So far there are many defensive methods to provide security against some attacks, but no complete security solution is yet available for WSNs. Hard work should be made to achieve balance between operation cost of security equipments, and operational cost of other functions of the network. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient Doubtless, there is an urgent need to develop security protocols and techniques to serve within the limited resources of the network without consuming them.

8. Recommendations:

In light of these findings, as we explained earlier that most of the attacks against security in wireless sensor networks are caused by the insertion of wrong information by the nodes which are agreed or compromised within the network .For defending the inclusion of these false reports by compromised nodes, a mean is required for detecting these false reports.

So it should create another base station same as the original base station keeping it in more far place from the attacker. This node should have the same characteristic as the original base station and known all nodes in the WSN. Then attacker will attack this station and the other base station will be safe.

First Step: Have a unique key which is known to all other nodes and the original station .

Second Step: codes between the nodes are sent continuously inside the domain and this code is sent to make the attacker thinking that this communication is real and he should go and attack the wormhole. Nodes should drop this traffic as soon as there is a congestion.

References:

1. Platon, E., &Sei, Y. (2008). Security software engineering in wireless sensor networks. Progress in Informatics, (5), 49. doi:10.2201/NiiPi.2008.5.6**.**
2. Saraogi, M. (n.d.). Security in wireless sensor networks, 1–12.
3. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials, 8(2), 2–23. doi:10.1109/COMST.2006.315852**.**
4. Nur, A., &Noman, M. (2008). A generic framework for defining security environments of Wireless Sensor Networks. 2008 International Conference on Electrical and Computer Engineering, 924–929. doi:10.1109/ICECE.2008.4769344**.**
5. Hu, F., & Sharma, N. K. (2005). Security considerations in ad hoc sensor networks. Ad Hoc Networks, 3(1), 69–89. doi:10.1016/j.adhoc.2003.09.009
6. Kavitha, T., &Sridharan, D. (2010). Security Vulnerabilities In Wireless Sensor Networks : A Survey, 5, 31–44.
7. Walters, J. P., & Liang, Z. (2006). Chapter 17 Wireless Sensor Network Security : A Survey, 1–50.
8. Pathan, a. S. K. (2006). Security in wireless sensor networks: issues and challenges. 2006 8th International Conference Advanced Communication Technology, 6 pp.–1048. doi:10.1109/ICACT.2006.206151**.**
9. Kavitha, T., &Sridharan, D. (2010).
10. Kavitha, T., &Sridharan, D. (2010).

11. Pietro, R. Di, Mancini, L. V, Soriente, C., Spognardi, A., &Tsudik, G. (n.d.). Networks, 1–12.
12. Nakayama, H., Ansari, N., Jamalipour, A., Nemoto, Y., & Kato, N. (2006). On Data Gathering and Security in Wireless Sensor Networks.
13. Kavitha, T., &Sridharan, D. (2010).
14. Pathan, a. S. K. (2006). Security in wireless sensor networks: issues and challenges.
15. Walters, J. P., & Liang, Z.
16. Wang, Y., Attebury, G., & Ramamurthy, B. (2006).
17. Kavitha, T., &Sridharan, D. (2010).
18. Kavitha, T., &Sridharan, D. (2010).
19. Pathan, a. S. K. (2006). Security in wireless sensor networks: issues and challenges.
20. Walters, J. P., & Liang, Z.
21. Kavitha, T., &Sridharan, D. (2010).
22. Wang, Y., Attebury, G., & Ramamurthy, B. (2006).
23. Padmavathi, G. (2009). A Survey of Attacks , Security Mechanisms and Challenges in Wireless Sensor Networks, 4(1), 1–9.
24. Wang, Y., Attebury, G., & Ramamurthy, B. (2006).
25. Padmavathi, G. (2009). A Survey of Attacks**.**
26. Kalsoom Shabana, Nigar Fida, Fazlullah Khan, Syed Roohullah Jan, Mujeeb Ur Rehman(2016) Security Issues And Attacks In Wireless Sensor Networks.
27. Kavitha, T., &Sridharan, D. (2010).
28. Nakayama, H., Ansari, N., Jamalipour, A., Nemoto, Y., & Kato, N. (2006).
29. Pathan, a. S. K. (2006). Security in wireless sensor networks: issues and challenges.
30. Pathan, a. S. K. (2006). Security in wireless sensor networks: issues and challenges.
31. Kavitha, T., &Sridharan, D. (2010).
32. Walters, J. P., & Liang, Z.
33. Walters, J. P., & Liang, Z.
34. Kavitha, T., &Sridharan, D. (2010).
35. Hu, F., & Sharma, N. K. (2005).
36. Modirkhazeni, A., Ithnin, N., & Ibrahim, O. (2010). Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey

Analysis. 2010 Second International Conference on Network Applications, Protocols and Services, 228–233. doi:10.1109/NETAPPS.2010.48.

37. Anwar R.W, Bakhtiari M, Anazida Abdullah A.H and Qureshi K.N(2017) Security Issues and Attacks in Wireless Sensor Network Faculty of Computing, University Teknologi Malaysia.
38. Hu, F., & Sharma, N. K. (2005).
39. Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., &Srivastava, M. B. (n.d.). On communication security in wireless ad-hoc sensor networks. Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 139–144. doi:10.1109/ENABL.2002.1030000.
40. Hu, F., & Sharma, N. K. (2005).
41. Kavitha, T., &Sridharan, D. (2010).
42. Anwar R.W, Bakhtiari M, Anazida Abdullah A.H and Qureshi K.N(2017).