ASSESSMENT OF THE CHALLENGESAND SECURITY IN WIRELESS SENSOR NETWORKS

Hesam Ghasemi

Department of computer Islamic Azad University, Ayatollah Amoli branch Amol, Iran

Email:www.hesam.ghasemi3@gmail.com

Abstract-Today, There are growing interest to use communication services; accessible for advanced reasearch which caused creating wireless sensor networks. Network security is a major challenge. Network security is so challenging task. Considering to limited resources of sensor nodes; creating security in wireless sensor network is harder rather than other traditional networks. Considering hostile nature location; wireless media and limited nature of resources in small sensor in this networks accompany with security challenges lager than traditional networks. Due to natre of location without supervision and limitation of internal resources; the security of wireless network is a challenging task. On the other hand; due to limitation of resources; the security thechniques of typical computer network in "WSN" can't be performed. However; wireless sensor networks suffer from a lot of limitations like poer limitation; Processing capabilities; unattended operation and etc. Also, It can be expected the threat and attacks in all layers of the network protocl. The wireless sensor networks have benn determined with severity of computational limitations and temporary energy resources of operating environment. In this essay, the security challenges and kinds of attacks in the sensor networks will be evaluated, due to meet challenges, The requiered strategies are suggested.

***Keywords*: wireless sensor networks, security, security challenges, limitation of network resources**

I. INTRODUCTION

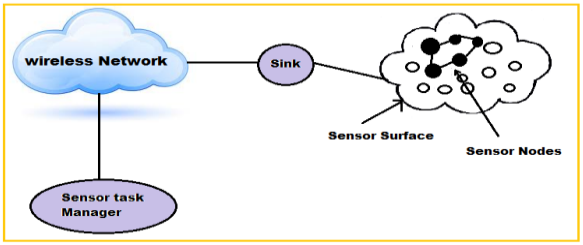
In the Present, The wireless sensor networks (WSN) are the main part of supporting various technologies [1]. WSN is a great dynamic research are a including data managing , distributed algorithms , programming models, hardware, design network system and security and social factors[2]. wireless sensor network as a modern technology is under pressure progressing recent technology in micro-electromechanical systems technology (MEMS), wireless connections and digital electronics.

There is a low-cost and small sensor which organize smart self-multi functional devices, are equipped with

ISSN 2519-0814

the battery, radio, microcontroller and sensor[2,3,4]. Each network whether the Internet or noc wireless network are vulnerable to destructive activities.

Destructive attacks in ((WSN)) are much more rather than the temporary network, because of WSN formed of the node with limited resources. while it may be the aggressor attacks with powerful resources such long-range wireless networking capability. Thus, security in ((WSN)) is so important, because of limitation resources, the security techniques can be performed[5].



Fg. 1. Designing wireless sensor network

This report is about collecting data, supervision environment and prediction system. the error measurement in the construction of building, car, airplane and the whole range of intelligent networks are the different applications of the sensor network.

The most wireless applications such traditional network require security.

Standard encryption methods are used in WSN for move security it is not useful to use typical methods in WSN cause of limitation resources in the sensor. there fore with out security techniques adverse results will happen actually the wireless networks require global attention which causes of low-cost and potential solution face with different challenges in the word wide[6]. many of used factors of wireless sensor network including the self-organized self-restoration dynamic topology network contrast with impaired nodes mobility the located node performance without supervision resistance the lack of nodes congruence scalability at the time of location and after location. the main challenges for network design are resources such as limited memory capacity the calculation ability energy source and communication bandwidth[7,8].

In the following, the main challenges in sensor networks and security requirements of receiver wireless network are suggested.

In Chapter 3 the threats and attacks in Wireless sensor network will be suggested. In chapter 4 the basic security plans in wireless sensor networks will be surveyed. Finally, bin the last chapter the results will be studied.

II. THE MAIN CHALLENGES IN WIRELESS SENSOR NETWORKS

The wireless sensor network has limitations in resistance limitation of extreme resources which following sensor nodes and unreliable connection in wireless sensor network is the challenges in wireless sensor network is the basic effort in sensor network security.

A. The limited resources

Because of limitation of hardware source the wireless sensor network will have challenges in each sensor. the embedded devices with limited sources are responsible for distribution and temporary complex network protocol.

So that energy capacity the basic limitation of energy creating the collection of related issues about designing.

B. Unreliable connections

While wireless media distribute in nature innately it may be that packages damage because of channel mistakes and conflicts or reduce the node density in the network . the aggressor can attack with denial of services (dos) without effort . the hub router network density and processing nodes can lead to more delay

ISSN 2519-0814

in the network, as a result, it is difficult to coordinate between sensor nodes.

C. *Protection operation*

The sensor creates close interaction with physical environment process fuse which has new information for the suggestion to users. This little node that often are openly used in large scale and even war zones. The Potential Issues Are Related To Destruction Of Random Nodes In Physical Record. Getting The Secure Data In Different Environment Of Physical Wireless Sensor Are Related To Final User.

D. *Security Class*

Attack To Wireless network can be as pause tracking making and correction. tracking attacks to secrecy. illegal access needs to sensor nodes or saved data which the sensor network put in danger with an enemy . due to get related information the enemy tries to give in correct data and show himself reliable.

III. THREATS AND ATTACKS IN WIRELESS SENSOR NETWORKS

The wireless sensor network exposed with different security threats. because of self-distributed traits, the limited calculative resource in energy and power are so limited. this limitation creates a large – range for aggressors. the kinds of attacks following:

A. *goal oriented attacks*

1) *Inactive attacks*

These attacks are done against secrecy data an aggressor has divided sensitive data for traffic monitoring. inactive attacks including traffic analytics monitor communication decoding poor traffic and obtaining authentication information.inactive tracking of network operation can lead to predicting future actions by the aggressor. such attacks can lead to disclosing information or files without satisfaction by the aggressor.

2) *Active attacks*

The other aggressor is inactive in the active attacks but they can effective in the active attacks but they can effectively control the networks. some of the kind of attacks following: denial service attacks (dos) modified data black hole distribution pit trick ness flooding densetrample wormhole construction flooding subversion node selective transport incorrect node.

B. *Player – oriented attacks*

There are two kinds attacks that named External and internal attacks.

1) *External attacks*

It my be that the external attacks being sane of inactive eaves dropping that can spread the denial attacks by injecting bogus data to network resources.

2) *Internal attacks*

The aggressor can hurt to network in secret because they can obtain authentication information licensed. they are a part of legitimate nodes and access to information . it is not expected the easy attack pattern. the aggressor can do the different attacks following: changing wrong routing eaves dropping drop setup package that is the last trick because it is hard to recognize for that it deduces by the aggressor or as result of collision or noise.The attacks cause the suppression of information which don't allow them reducing the performance of there are kind of drop package attacks such as black hole gray hole which are a serious threat for application programs such as military supervision system battlefield supervision and other vital substructure[14].

C. *Larger – oriented attacks*

The wireless receiver network is organized as a layer form this layer–oriented architecture cause the network become vulnerable to kinds of attacks.

ISSN 2519-0814

1) Physical layer attack

Physical attacks in wireless sensor networks are in the form of getting node form radio channel densely. physical attacks in the wireless receiver network are too hard. physical attacks protect the software attack because of the lack of physical control to particular nodes. Density is a crucial attack in physical layer that its purpose is interference in typical operation. It may be that an aggressor delivers radio signals to a wireless channel. an aggressor can deliver effective signals with high energy to prevent wireless media and prevent sensor to denial service attacks in this layer[7].

2) The linked layer attacks

The capacity of linked layer protocol is for coordination the close node to get linked to the higher layer. the deliberate attack can break pre–defined protocol behavior in linked layer. for example, it may be that the aggressors facing with heckling in an induction package cause redelivery or stopping or surveying the massage due to the derivation information of related patterns. this can be performed when theMessage can encoding and cant decoding. even it can leads to misuse the ((MAC)) in dependant layer priority patterns.

3) Network layer attack

The wireless receiver network layer is exposed with kinds of dos attacks that play the main role in proper disturbance of goal direction information and as a result considered as A proper operation of ad – hoc network. Pit attacks try to endanger the proper traffic into nodes creates a figurative pit against the center enemy. if an aggressor is a node it is enough to preserve it to get from the proper network. destructive nodes or attacks can deliver the proper message and leave them in the direction[17]. there are some faking changing or distribution the routing information that considered as direct attacks against a routing protocol that it is possible to put the information between nodes. it is possible an aggressor be the faking changing or distribution the routing information due to the disturbance in traffic network[15].

4) Transfer layer attacks

It is possible that an aggressor doesn't obtain the new connection in needful resources by the deformed connection or don’t reach to the highest degree. the aggressor produces the limitation of resources for the legal node.

5) Attacks of application layer

We can name different kinds of attacks in this layer as suppressdisjunction imperfection of data sand wreak codes. codes in suppress attack an aggressor may suppress nodes of the network and cause net transfer amass of traffic into a basic stand. this attack causes consuming of nets band width and disembarks of nodes energy foundmental[5].

IV. SCHEME OF SECURITY IN THE WIRELESS SENSOR NETWORK

A challenge for using each useful scheme of security in wireless receiver network is the extent of the sensor so perks memory and the type of tasks expected of the sensor and also communication capacity is limited. for secured transfer of different kinds of data in sensor network we use some Encryptionical techniques symmetric and asymmetric key that the security of a symmetric Encryption depends on mathematic and algorithm problem, as a result, a lot of energy consumed in the symmetric key of code that used for repeating simple operating in Encryption. usually, ways for achieving secured goals are introduced as follow:

A. Symmetric Encryption in wireless sensor networks

this idea used for loading esoteric data in sensor nodes before lodgment of them in the network . this esoteric data may have hidden keys or support data that help to sensor nodes to fined real hidden key. a secured node can communicate by usingthese keys. The main problem of this solution is that imperial of a key can lead to the collusion of the whole network. for

ISSN 2519-0814

conquering to this limitation some researcher present sum of two by two key instead of one unique key[12].

In general existing symmetric Encryption for the reciver wireless network has focused an benefit from pitch key, after pitching network although they cause dynamism management of key by refreshing a key. indication when amount of sensor nodes increase symmetric iconography in implementation software. since they are in commerce between flexibility and operation and natural environment in which sensor nodes exist cause damage of that toward different attacks . in Encryption an exoteric key with thousands and millions multiplication is involved and tums it to a research branch in adaptation and optimization of advanced Encryptionical systems for smaller systems such as sensor devices. a lot of traces with concentrating on an adaptation of light weight and asymmetric Encryption of algorithm.

B. Asymmetric Encryption in wireless sensor networks

Encryption considered as an exoteric key that is so difficult for using in wireless sensor networks. for achieving to the security of WSN these condition required:

1) Surreptitious (esoteric)

Security of data in the process oftransfer from the anode to the other or deprivation of illegal access in another way of saving secret data. illegal access to sensitive data sand over hearing repressed by encoding. these nodes should hide their secret data from showing. for example in software strengths, lots of sensitive data between nodes can transfer through a development channel for security between receiver and receptor. finding the path from these sensitive data can occur by passing through lots of nodes before achieving to the final point. it is necessary of Encryption of huge transferring by coding general sensor for saving from attacks of traffic analysis.

2) Completeness

Integration includes confirming data or readability of transfer that is irreversible. integration of security makes dispensation or reformation. all of the data make by validation code and MAC machines.

MAC is the receiver of satisfaction and confirmation message. security is wearing a disguise against of attacks[7].

3) Authenticity

Wireless sensor network in nature is like dispensation communication so in attack instead of changing contents of text we can add useless packages in main packages and allows legal messages come and stop receiving messages from the illegal resource. a digital signature is one way to confirm the identity of anode[9].

4) Updating data

In Encryption of common key after a period of time they guaranty that change newly received data. this warranty that there are no attacks in which receiving a unit of data and send them again[8]. we can achieve to this security by a time tag with this message. comparison the time of receiver node and time recognition of receiving updating data is 0(zero).

5) Access

Communication and calculation potential in sensor nodes is limited. so calculation shows its ability increasing usage of energy but if there is no further energy there will be more access of data. the separable idea of the anode can effect on accessibility of a network. an aggressor can use energy or source of attacks.

Such as DOS or setup nodes compromise attack sensor nodes can use their energy in on the intelligent way with timely sleep mood that is a fixed mood for along time and a saving energy for a time when you need a longer time for usual calculation.

6) Self – organization

It is better that the sensor nodes have the self – recovery or self – organization abilities to adjust with

ISSN 2519-0814

environmental changing [9]. so they can break a single node are needed for sensor flexible nodes which can be transferred to unusual situations.

7) Coordination

It is neck to coordinate when are formed the connection between two nodes. it may be that a sensor radio is out of energy reserving situation. Therefore, the synchronization group urgent need for sensor networks in common diagnostic software.

8) The secure localization

The different attacks are done by finding the correct node location in the network.The search for the wasting package and layer protocol data can be performed by designed opponent so it is necessary the secure node situation. the sensor nodes should be in an accurate direction in the proper network which each node can to find the other nodes in wireless sensor network and determine the error location[10].

V. CONCLUSION

The wireless sensor network progress in the most application program of the critical mission, so it is necessary to vital security. However, the wireless sensor networks suffer from kinds limitation such as limitedenergy, processingcapabilities, saving capacity, unreliable connections unattended operation and etc. there are a lot of ways to create security that the main is encryption.

It is so important that the selection of encryption method suggest the proper security services in wireless sensor networks. the encryption is considered as a general key for sensor nodes with too heavy limited resources.

However, the studies are shown that it is passible the encryption is the general key for network sensor by using algorithm selection related parameter optimization and low power technique. these encryption patterns are deleted the problems of symmetric methods that lead to more operation. Diffie – Hellman and RSA are appropriate for sensor nodes based on elliptic curve encryption The results have shown that it is possible the reaching to excellent result by smaller try because reduce the calculation time and saved – delivered data. Specifically, the asymmetric methods by encryption of general key are the elliptic curve encryption for needed security purposes in wireless sensor networks.

The challenges attacks and security of wireless sensor networks have been surveyed in this essay due to suggest a general view and the results have been shown.

REFERENCES

[1] Abhishek Jain, Kamal Kant, and M. R. Tripathy*,"Security Solutions for Wireless Sensor Networks",* Second International Conference on Advanced Computing & Communication Technologies, 2012.

[2] Daniel E. Burgner, Luay A, "Wahsheh *"Security of Wireless Sensor Networks",* Eighth International Conference on Information Technology: New Generations, 2011.

[3] Kalpana Sharma. M K Ghose*, "Wireless Sensor Networks: An Overview on its Security Threats"*, IJCA Special Issue on Mobile Ad-hoc Networks 2010.

[4] David Martins, and Herve Guyennet, *"Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey",* 2010 IEEE.

[5] Anitha S.Sastry, Shazia Sulthana and Dr.S Vagdevi, *"Security Threats in Wireless Sensor Networks in Each Layer",* International Journal of Advanced Networking and Applications, Vol. 04 Issue 04, pp. 1657-1661, 2013.

[6]. Shahnaz Saleem1, Sana Ullah2, Hyeong Seon Yoo1*"On the Security Issues in Wireless Body Area Networks"* International Journal of Digital Content Technology and its Applications Volume 3, Number 3, September 2009.

ISSN 2519-0814

[7]. Prabhudutta mohanty, Sangram Panigrahi,Nityananda sarma and siddhartha sankar satapathy *"Security issues in wireless sensor network data gathering protocols: a survey"* Journal of Theoretical and Applied Information Technology.

[8] S. P. Prabhudutta Mohanty, Nityananda Sarma, Siddhartha Sankar Satapathy, *"SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS: A SURVEY.,"* Journal of Theoretical & Applied Information Technology, vol. 13, pp. 14-27, 2010.

[9] M. Pooja , Dr. Yudhvir Singh, *"Security Issues and Sybil Attack in Wireless Sensor Networks,"* International Journal of P2P Network Trends and Technology, vol. 3, 2013.

[10] A. Jain, K. Kant, and M. R. Tripathy, *"Security Solutions for Wireless Sensor Networks,"* presented at the Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, 2012.

[11] M. Y. Malik, *"An Outline of Security in Wireless Sensor Networks:Threats,Countermeasures and Implementations,"* CoRR, vol. abs/1301.3022, 2013.

[12] M. R. K. Amin Reza Sedghi, *"Data Security via Public-Key Cryptography in Wireless Sensor Network,"* International Journal on Cybernetics & Informatics (IJCI) vol. 2, 2013.

[13] A. Singla and R. Sachdeva, *"Review on Security Issues and Attacks in Wireless Sensor Networks,"* International Journal, vol. 3, 2013.

[15] Q. I. Sarhana, *"Security Attacks and Countermeasures for Wireless Sensor Networks:* Survey," International Journal of Current Engineering and Technology, vol. 3, 2013.

[16] M. K. Jain, *"Wireless sensor networks: Security issues and challenges,"* International Journal of Computer and Information Technology, vol. 2, pp. 62-67, 2011

[17] Chris Karlof and David Wagner, *"Secure routing in wireless sensor networks: attacks and countermeasures,"* Ad Hoc Networks Journal, Vol.1, Issue 2-3, pp. 293-315, 2003.

ISSN 2519-0814