A Survey on Security issues in Wireless Sensor Network

[1] T.Nagaraju [2] S.Asif [3].M.Janga Reddy

1Assistant Professor, Dept of CSE, CMRIT Kandlakoya(v), Hyderabad, India

2Assistant Professor, Dept of CSE, CMRIT Kandlakoya(v), Hyderabad, India

3. Professor, Dept of CSE, CMRIT Kandlakoya(v), Hyderabad, India

Abstract- This paper Explains a brief layout on WSN (remote sensor compose) organize building besides it shows a point by point exchange on various security objective related to sensor center points in WSN framework, for instance, Data protection, Data genuineness, Accessibility, Authentication, Data freshness, Time Synchronization et cetera. Amounts of hazardous attacks that can happen in a WSN framework are shown in this paper for which game plans can be arranged remembering the ultimate objective to improve the organizations of such frameworks. Such harmful strikes are according to the accompanying: Spoofed, balanced, or replayed information, Selective sending, Sinkhole ambush, Sybil Attack, HELLO surge strike, Wormholes Attack.

Key words: Wireless sensor arranges, Attacks, Security issues, Sinkhole ambush.

INTRODUCTION

"A sensor system is an arrangement of monstrous quantities of little, cheap, self fueled gadgets that can detect, process, and speak with different gadgets with the end goal of get-together nearby data to settle on worldwide choices about a physical situation" [1]. The sensors hubs are utilized for observing distinctive situations as a part of the helpful way and process the information for examining. The two parts of remote sensor arrange conglomeration and base station, total gather the data from that point adjacent sensors, coordinate them and send to the base station for preparing. These sensor hubs comprises of some real parts detecting, preparing after that correspondence [2]

The qualities of WSNs are remote medium, low power utilization, minimal effort and low information rate. Different attributes of WSN are huge quantities of sensors, synergistic flag handling, effectively conveyed, self-configurable and self-sort out, and framework less.

Wireless sensor network architecture:

Sensor Nodes: Sensors nodes are the heart of the network. They are in-charge of collecting data and routing this information back to a sink.

Gateway/Sink: A gateway enable to the communication between the sensor nodes (Field devices).The gateway are also called access points.

Task manager: A task manager is managing the operation, administration, security, and maintenance of all sensor nodes in a network.

Security manager: the security manager is responsible for the security of nodes in a network and management of keys. [4]. For example see Fig.1.

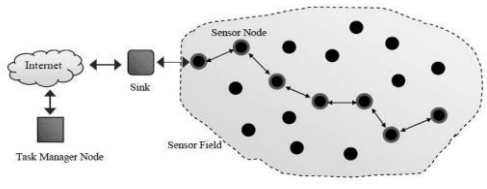

Fig. 1: Architecture of WSN

The rest of the paper is composed as takes after. In segment 2, exhibit the security necessities in WSNs. Area 3; introduce the past work done Section 4, conceivable assault in remote sensor system is examined. Segment 5, exhibit the conclusion.

II.Goals

Security Goals in WSNs: The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The most important security requirements in WSN are listed below:

2.1 Data confidentiality: It means restricting data access to authorized personnel. The data should not be leaked across adjacent sensor networks. It ensures that a given message cannot be understood by anyone other than the desired recipient.

2.2 Data integrity: Data integrity ensures that the receiver receives unaltered data in transit by any unauthorized personnel.

2.3 Availability: It ensures that the desired network services are available even in the presence of denial of service attacks.

2.4 Authentication: It ensures that the communication from one node to another node is genuine, i.e., a malicious node cannot masquerade as a trusted network node.

2.5 Data freshness: Data freshness ensures that the recent data is available without any replay of old messages by unauthorized personnel**.**

2.6 Self-organization: Nodes should be flexible enough to be self-organizing (autonomous) and self-healing (failure tolerant).

2.7 Robustness and survivability: Sensor network should be robust against the various attacks and if an attack succeeds, the impact should be minimized.

2.8 Time Synchronization: These protocols should not be manipulated to produce incorrect data.[5]

Constraints in wireless sensor network: [5]

Resource constraints: Sensor nodes have low computational capability in its limited resources, wireless communication bandwidth are limited, small memory etc.

Small message size: In sensor network are message size is small as compared to existing networks. There is no use of segmentation in many applications in wireless sensor network.

Sensor location and redundancy of data: In a sensor network are position of nodes is very important since data collection is normally based on location. Also there are use a common phenomenon to collect data, so these data are high probability then this data has some redundancy.

Cryptography: [7] Cryptography simply aims at making data not understandable to an unauthorized adversary which has the goal of data interpretation.

Plain Text The plain text is the actual message that has to be send to the other end.

Cipher Text: Cipher text is the original message is transformed into non readable message before the transmission of actual message.

Encryption: A process of converting Plain Text into Cipher Text is called as Encryption.

Decryption: It is a process of converting Cipher Text into Plain Text.

It consists of two categories.

1. Asymmetric Cryptography
2. Symmetric Cryptography.

Symmetric Cryptography:
Symmetric key cryptography mechanism use a single shared key between the two communicating host which is used both for encryption and decryption.

Asymmetric Cryptography: Asymmetric key cryptography also known as public key cryptography, which uses public-private pair key for encryption and decryption

III.PREVIOUS WORK DONE

Raja waseem anwar et al. "Security Issues and Attacks in Wireless Sensor Network" This paper dissected security issues and physical assaults. The most physical assaults irritate the remote sensor organize security objectives like secrecy, respectability, validness and accessibility.

Vikas kumar et al. "Remote Sensor Networks: Security Issues, Challenges and Arrangements" This paper displays the assaults and their order in remote sensor systems. Likewise it exhibits a brief review of security component and difficulties of remote sensor arrange.

Sahabul Alam et al. "Examination of Security Threats in Wireless Sensor Network" This paper gives the Security plans and the danger assaults in remote sensor arrange. Security plans like: Cryptography, Steganography and Physical layer Secure Access. Danger assaults like: Collisions, Tampering, Jamming, Unfairness, and Flooding and so on. They likewise propose an answer for the assaults in remote sensor arrange. One conceivable arrangement is the utilization of cryptography methods.

Ritu Sharma et al. "Investigation of Security Protocols in Wireless Sensor Network" gives imperatives, security objectives, risk models and run of the mill assaults on sensor systems and their guarded procedures or countermeasures significant to the sensor systems, including security techniques. Security objectives in WSN :(Availability, Authorization,Authentication, Confidentiality etc).They likewise propose an answer for security in remote sensor system and gives the outline of different security conventions.
Yih-Chun Hu et al. "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks" ARIADNE is an on-request secure specially appointed steering convention in light of DSR. It depends on exceedingly productive symmetric cryptography. It gives indicate point validation of a steering message utilizing a message confirmation code (MAC) and a mutual key between the two gatherings. It adapts to assaults performed by vindictive hubs that change and manufacture directing data with assaults utilizing pantomime.

Abhishek Pandey et al. "A Survey on Wireless detector Networks Security" offers the superimposed style of remote detector prepare. These square measure the distinctive layer square measure various capacities. The target of Network layer is to get best method for effective steering instrument .In this layer square measure used filter convention to spare the vitality utilization (force of sensor) to boost the lifetime of sensors. Filter offers cluster primarily based transmission. The target of use layer is guilty of data gathering, administration and handling of the knowledge through the appliance programming for obtaining dependable results. during this layer square measureused SPINS (security convention in detector organize) convention square measure offers info confirmation.

Jyoti Attri et al. "Concentrate on cryptographic procedures in PC arrange

security" give the review of cryptography systems like Symmetric and lopsided key. In

symmetric key cryptography, single key is utilized for encryption and decoding process i.e. utilizing same key information can be scrambled and unscrambled .Symmetric key are quick as contrast with lopsided key. Symmetric key is more adequate for security in remote sensor arrange.

IV. POSSIBLE ATTACKS IN WIRELESS SENSOR NETWORK ROUTING

4.1 Spoofed, adjusted, or replayed data

The most immediate and best method for assaulting any steering convention is to focus on the data being traded between the hubs. By caricaturing, changing or replaying directing data, enemies can accomplish various intentions like making steering circles, augmenting or shortening steering ways, drawing in or repulsing system activity, expanding end-to-end inactivity, parceling the system, creating false blunder messages, and so forth.

4.2 Selective sending

A legitimate hub would dependably reliably forward the got messages to its goal. Nonetheless, a noxious hub would decline to forward specific messages and basically drop them, guaranteeing that the message doesn't achieve the proposed goal. This is called particular sending assault. A basic type of this assault is that the pernicious hub would go about as a dark gap i.e. drops each message parcel that touches base to it. However, such hubs have the hazard that the neighboring hubs would consider them as dead hubs and would look for another course. In this way, enemies adjust a more inconspicuous frame i.e. wisely forward just certain messages. Consequently, the danger of getting got is minimized. Specific sending assaults are more powerful when the assailant unequivocally incorporates itself in the steering way of the information. Different methods for actualizing specific sending is by sticking or bringing on crash on the transmitting data.

4.3 Sinkhole assault

In sinkhole assault, a bargained hub is made to look extremely appealing to the encompassing hubs concerning the directing calculation. (For instance, foe can publicize a top notch steering way and thus redirect the way through it.) Hence a figurative sinkhole is made with the enemy at the inside. Also, now since the directing way is redirected through this foe hub, serious harms should be possible by it. Sinkhole is an extremely viable method for actualizing particular sending. Parodying, modifying or replaying the steering data should likewise be possible by the foe. The motivation behind why sensor systems are exceptionally powerless to sinkhole assault is on the grounds that all message bundles being transmitted have a solitary extreme goal, the base station. A traded off hub just needs to give a solitary top notch course to the base station and subsequently, affecting extreme harms.

4.4 Sybil Attack

In Sybil assault, a solitary hub introduces various characters to alternate hubs in the system. Courses accepted to go through various hubs would really be going through a similar enemy hub and consequently accordingly risking a perpetual circle.

Sybil stack posture huge dangers to area based steering convention. Conventions which require trade of area data would be unfavorably influenced as enemy hubs, utilizing Sybil assault, would trade different arrangements of directions, as opposed to a solitary arrangement of directions and

consequently can be in more than one place at a time.[6]

4.5 HELLO surge assault numerous conventions require broadcasting HELLO parcels by the sensor hubs to declare it to the neighbors, along these lines cautioning them that it's inside their transmission run. Yet, an enemy could surge false HELLO bundles. Consequently, the hubs would consider it to be inside the range while the enemy might be arranged a long way from it. In such situations, hubs would be pointlessly transmitting message and thus depleting its vitality. Conventions which rely on trade of area data between the hubs are probably going to be focuses of such assault.

4.6 Wormholes Attack

In wormhole assault, a foe burrows messages got in one a player in the system over a low idleness connect and replays them in an alternate way. Wormhole assault ordinarily includes two far off vindictive hubs, deluding others to downplay the separation between them by handing-off parcels along an external channel, which is accessible just to the assailant. An assailant arranged near the base-station may totally upset the directing by making an all around put wormhole. This assault is probably going to be utilized as a part of mix with listening stealthily or specific sending. Recognizing Wormhole assault is troublesome when utilized alongside Sybil assault. Wormholes can be insightfully used to make sinkholes

V.CONCLUSION

This paper presented a detailed picture about various security issues related to WSN networks. Also a brief introduction to cryptographic technique is made to enhance the security of wireless sensor network.

REFERENCES

1. Olariu S. et al., "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University.
2. *Raja Waseem Anwar, et al., "*Security Issues and Attacks in Wireless Sensor Network*",* World Applied Sciences Journal 30 (10): 1224-1227, 2014,ISSN 1818-4952
3. Vikash Kumar1. et al., " Wireless Sensor Networks: Security Issues, Challenges and Solutions",
   International Journal of Information & Computation Technology,ISSN 0974-2239 Volume 4, Number 8 (2014)
4. Yogesh Chaba. et al., "Analysis of Security Protocols in Wireless Sensor Network", Int. J. Advanced
   Networking and Applications 707 Volume: 02, Issue: 03, Pages: 707-713 (2010)
5. Sushma1.et al., "Security Threats in Wireless Sensor Networks'', IJCSMS International Journal of
   Computer Science & Management Studies, Vol. 11, Issue 01, May 2011 ISSN (Online): 2231 – 5268
6. Jyoti Attri.et al., "Study on cryptographic techniques in computer network security'', Asian J.of Adv.
   Basic sci.: 2(3) , 98-102 ISSN (online):2347-4114
7. Sujesh P. Lal.et al., "Security Issues in Wireless Sensor Networks – An Overview'', Sujesh P. Lal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) 2015, 920-924
8. Jaydip Sen., "A Survey on Wireless Sensor Network Security'', International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2, August 2009
9. Abhishek Pandey. et al., "A Survey on Wireless Sensor Networks Security", International Journal of computer Application (0975-8887) Volume 3-No.2,June 2010
10. Wendi Rabiner Heinzelman.et al., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", International Conference on System Sciences, January 4-7, 2000, Maui, Hawaii.
11. David B. Johnson et al., "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", Wireless Networks 11, 21–38, 2005

Mr. T.Nagaraju, received M.Tech(IT) from JNTU-H B.Tech.[CSE] from JNTU-H. Working as assistant Professor in CMRIT, CSE department. His research interest is Cloud computing.

Mr. S.Asif, received B.Tech(CSE) from JNTUH, M.Tech(DCN) from VTU Belgaum. Asst Professor CMRIT CSE Department His Research interest is Network Security.

Dr.M Janga Reddy Principal CMRIT Hyderabad, His Research Interest is Network Security.