A Security and Privacy Threats in Emerging Wireless Sensor Networks-Survey

P. Shobana
Research Scholar
Department of Computer Science
PSG College of Arts and Science

Dr. R. Shanmugavadivu
Assistant Professor
Department of Computer Science
PSG College of Arts and Science

Abstract-A sensor network is composed of large number of sensor nodes that are randomly deployed or very close to one another.wireless sensor networks are the distributed sensor to monitor which helps to pass their data through network to main location.In this paper we intend to discuss about the security and privacy in sensor network.this would helps to know how to protect from attacks to wireless sensor networks.we will review the some of security potentials, analyze the each attacks and overview the some protecting techniques performance and efficiency will done.

Keywords: Unwanted Wireless Sensor Network, Radio Frequency Identification,attacks.

1. INTRODUCTION:

A sensor network is designed to to perform a set of a high-level information processing tasks such as detection,tracking or classification.Measures of performance for these tasks are well defined, including detection of false alarms or misses,classification errors security attacks and track quality.one may have seen “sensors” on many occasions.Wireless sensor Networks targets tiny sensors that have RF(Radio frequency)communication capabilities.WSN sensor includes an analog sensing chip to sense environmental parameters(such as temperature and light), a micro-controller to execute local data processing(such as video compression) and networking operations(such as performing a routing protocol with neighbor sensor) and radio transceiver to send/receive sensed data through a wireless medium.the entire sensor can powered by batteries or other power sources(such as solar energy) with a lifetime of several months to a few years.WSNs employ the medium access control (MAC)protocol to coordinate the signal transmissions over the shared wireless radio channel.Otherwise,multiple nodes may try to access the transmission medium simultaneously,which leads to signal collision,

Data loss,re-transmission,wastage of energy,delay in data transmission.In this security can be lossed because of signal attenuation refers to the loss of energy as transmitted signals travels from source node to destination node through air.The edges of the obstacles can result in multiple signals divided from the original transmitted signal, rough surfaces of the obstacles can cause scattering due to multiple signal reflections.

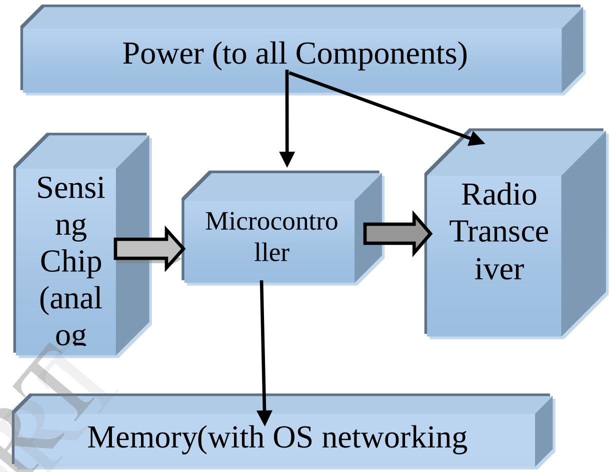


Figure1.1 lists only the most important components of a WSN sensor.There could be other circuit parts depending on practical application requirements.for instance,we may plant a GPS receiver in a sensor to keep track of accurate positions to absorb solar energy.

2. NEED FOR SECURITY

In wireless sensor network security is the vital role of the system.security is the actor and the main goal of the system like protecting confidentiality,integrity, and availability of the communication and computation.Sensor networks have a certain severe resource constraints due to their lack of data, storage and power.wireless sensor networks are vulnerable security attacks as medium to transmission of data is broadcasting.sometimes systems that are in physically can be captured or destroyed.

3.TAXONOMY OF WSN ATTACKS:

Attacks on sensor networks can be classified in to general categories on the classification standards as follows.

Mote-Class/laptop-class attacker:A mote-class attacker typically does not have enough resources to deploy strong attacks.but it can attack low-energy sensors.A laptop-class attacker has access to powerful equipment allows the adversary to launch much more powerful attacks.

Insider/outsider attackers:An outsider attacker has no special access to the sensor network, it does not know the WSN keys.But it can use passive eavesdropping to obtain data.An insider attacker is more difficult to prevent, because it has access to the encryption keys or other codes used by the network.A compromised node, an otherwise legitimate part of the network.

Passive/active attackers:A passive attacker compromises the privacy and confidentiality requirement by passively listening to the network data.However, an active attacker could damage the function of the network by actively attacking the WSN.for example,the attacker may inject faulty data into the network by pretending to a legitimate.

4. REQUIREMENTS OF SECURITY:

Wireless sensor networks that can be works with some important goals that to achieve it and protect from the hackers.some times the hackers can hack and destroy the whole system which is physical system.requirements of the security are in the following categories that are

- Data Confidentiality:Sensor networks should not leak any sensitive data to any unauthorized neighboring nodes.
- Data Integrity:The sensitive data should not erased or changes by adversary.
- Data Freshness:The sensitive data received by the nodes should be recent and should not be old message re-player.
- Availability:the data that should be used with limitation of the data access of the system.

5. ATTACKS ON SENSOR NETWORK ROUTING :

In the ideal world, a secure routing protocol should guaranty the integrity, authentication and availability of messages in the Presence of arbitrary power.Receiver can receive all the messages and able to verify the integrity all messages as well as the identity of the sender .Sensor network routing protocols are very simple.Most of the network layer attacks against sensor networks fall into one of the following categories that are :

- Spoofed, altered or replayed routing information
- Sybil Attack
- Sinkhole Attack
- Wormholes
- HELLO flood Attacks
- ACK spoofing

Spoofed, altered or replayed routing information:

In this all the data transmissions can be controlled by routing protocols.The establishment of a routing path is through the relevant sensors.The most of the direct attacks against the routing information exchanged between the nodes.An attacker can spoof,alter,or repel the network traffics generate false error ,partition of network, and increase end-end latency.

Sybil Attack:

In a Sybil attack, a single sensor presents multiple instances to other nodes in the network.Attacks can be significantly reduce the effectiveness of fault-tolerant schemes,such as distributed storage, dispersity and multipath routing schemes.In the WSN routing schemes ,Sybil attack can seriously damage geographic routing protocols because geographic routing uses a location-aware scheme and the Sybil attack, an attacker can appear in multiplaces simultaneously.If every pair of neighboring nodes uses a “unique key ” to initialize frequency hopping or spread Spectrum communication ,it may difficult to launch in next attack.

Sink hole Attack:

A sinkhole attack attracts the nearby traffic through an adversary node that could be an outsider attacker or a native compromised attacker.Thus this with some similarities to balckhole attack.By attracting data to its side, it has many opportunities to tamper with application data.In the black hole makes the incoming data “disappear”in which that sink holes can discard the such data but it may keep processing.but it is very difficult to detect it than the black hole.

Wormholes:

The Wormhole attack is the one of the toughest threats in WSN$_{s.}$In this attack, an adversary tunnels the messages received in one part of the network over a low latency link and replays them in a different part.a wormhole can actually can create a sinkhole which provides a high-quality route to the base station ,all the traffic in the surrounding area will be drawn through attractive path,because it is very close to base station.

HELLO flood Attack

In many WSN routing protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors.A transmitter can convince all the nodes within a network that it is their neighbor who uses with HELLO flood attack could trick their every nodes that it was their neighbor node.An attackers can does not need to have the capability of constructing legitimate traffic to use the HELLO flood attack.

ACK spoofing:

Acknowledgment spoofing is to achieve route establishment reliability,some routing algorithm rely on explicit or implicit the data link layer algorithm.The ACK attackers could be an convincing a neighboring node that a dead node is alive, or claiming a weak signals as a strong one.An ACK attack can cause a significant loss of data in networks that determine paths using data link reliability.

6.General security issues :

Wireless networks are inherently more vulnerable than their wired counterparts.notable factors contributing to security problem include the following:

- Channel:

Wireless usually involve broadcast communication,which makes eavesdropping and jamming easier.

- Mobility:

If a wireless device is affiliated with a person, tracking the device reveals that person’s location. Thus privacy become a important concern

- Resources:

End host usually battery powers devices which limits computation, size of RAM and secondary storage.which open the door of denial of service attacks at battery depletion.

- Accessibility:

Some devices are generally left unattended and are places in remote locations which increases more chance for physical attacks

7. Secuirty Issues:

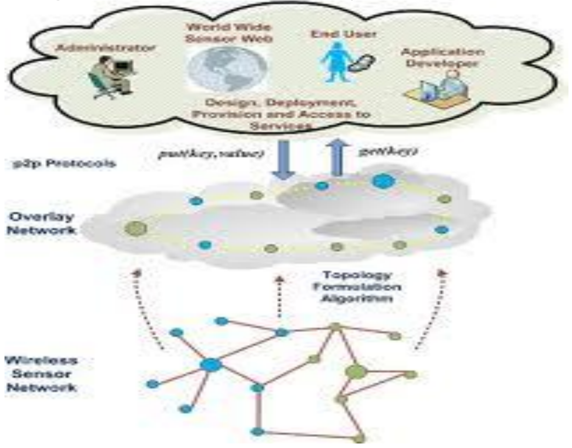
To resolve the problem of limited life of span of battery in wireless sensor network which weak the the technology development.limited battery can spoil the whole process and checking of battery and power consumption in military services is not possible.Another problem is Constant presence of sink that might not be helpful for medical , battle field and and disasters. For these drawbacks to resolve the above issues,two new wireless sensor network introduced

- Unattended WSN(UWSN)

- Radio frequency Identification(RFID)

7.1 Unattended WSN (UWSN):

Unattended WSN operate without continuous presence of a sink.Instead sensor-collected data is harvested by an itinerant sink that visits the network intermittently, with a certain upper bound on the interval between successive visits.because sensors cannot communicate with the sink at will,they must accumulate that and wait for sink.In figure 2 we can see how that unwanted can be removed and protect from it .The unattended nature of the network might be promoted by some design requirements to avoid any central point of failure.



7.1.1. Security issues in UWSN:

- Data Protection at individual sensor-The main challenge is to protect the data on individual sensor from the attacker to attained this encryption is used. So that even if the decrypt the data.this is attained by periodically updating secret keys through one way function.

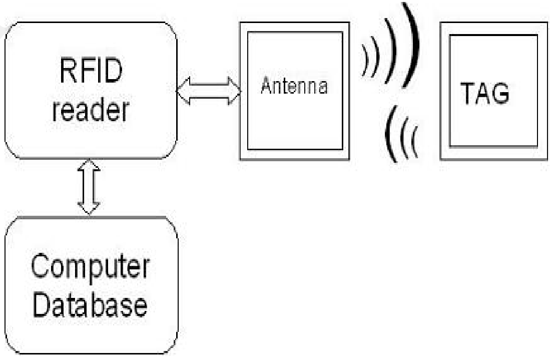
- Data survival-To achieve data survival sensor plays a hide and seek game by moving all its data around the network. This ultimately a losing game unless encryption is used.

- Secrecy-The attackers aims to learns sensor secrets in order to decrypt in data.The proposed system allow sensor to recover from the compromise by providing and obtaining help from sensors.

- Authentication-Data obtain by each sensor is authenticated by sink.so that it can identify that data is modified by any attacker.The proposed technique involves sensors to co-sign the data of their neighboring nodes. So that if any one of the co-signer is not compromised,sink can verify integrity and authenticity.

7.2. RFID$_s$

A micro chip in a label used to transmit data when the label is exposed to radio waves.Radio Frequency Identification that uses radio-frequency waves to transfer data between reader and movable items to identify, categorize, track.RFID is fast, reliable, and does not require physical sight or contact between reader/scanner and the tagged item.The RFID can come in two varieties: a transport-only tag which only allows one-way communication to the transceiver and are often referred to “passive” tags and “active” tags which allow information to read as well as written to the tags which is shown below in the figure 3 how the transmission is processing.



7.2.1 Security Issues in RFID:

The RFID security is only relevant if the information stored on tags is considered valuable.difficulties have been reported in RFID are tag collisions,tag detuning and tag failure with each of these issues causing potential security risks in the is of RFID.The main security concerns with RFID are The tempering of RFID devices;the cloning of RFID devices;and the cryptographic to protect RFID devices.

- Cloning RFID devices-RFID cloning is much simpler than traditional forms of identity theft which require more information and before the identity is used.RFID transport cards which store amounts on the itself rather than in a centralized database.

- Cryptographic Functions-The most determinal security issue with RFID is the type of encryption mechanism in place within the RFID system and tags.In this information can be hide by cryptographic mechanism and it can be stored and retrieval to centralized system..

8. PRIVACY OF WSNS:

8.1 Privacy of sensed data:

In wireless sensor network the sensed information stays within the sensor network and its accessible only by trusted parties is an essential step toward achieving privacy.for example a sensor network might anonmize data by reporting only aggregate temperature over a wide area or appropriate location of sensed individual.a system stored the sensed data in an anonmized database, remaining details that can be adversary might find useful.another approach is to process in the sensor network in a distributed manner so that single node can observe the query against potential system abuse by compromised malicious networks.

8.2Preserving a source location:

Wireless Sensor Network can be preserving a source location privacy under external,global,passive attacks in the privacy community.this can be categorize into two types that are

- Proxy-based Filtering scheme.
- Tree-based Filtering scheme

Proxy-based Filtering scheme:

In this sensors are selected as a proxies to collect and filtered the dummy message from surrounding sensors.This can be reduces the communication cast of the system by dropping many dummy message before they reach the base station.

- Tree-based Filtering scheme:

In this filtering scheme it is organised by into tree hierarchy proxies closer to the base station filter traffic from proxies and farther away. The message overhead is reduced.

9. SECURING DCS SYSTEM:

Data centric sensor can be secured under the Control of Internal, Local,active attacks.Data Centric Sensor network the information of data are saved inside the sensor network and sensor data in contrast to sensor nodes are named based on attribute.$_{p}$DCS includes very efficient key management schemes for revoking a compromised node once its compromise has been detected. This prevents an attacker from knowing the future storage location for particular events.

10. Conclusion:

In this paper, we have shown the different ways of attacks,security and privacy issues of Sensor Networks to protect from attacks, which will helps to increase security in wireless sensor Network.This could be helps to know the frequency detector and jammer could make a normal data communication to achieve the anti-jamming Communication.All disciplines can be related each other to generate some challeging issues to protect it.This would helps to protect from end-to end activity in the data link layer which can pass information to sensor which can deliver it using the proper encryption and decryption techniques.

Author Profile:

P.Shobana received MCA Degree in Computer Application from Anna University,Coimbatore, India.Presently she is doing her research in Information Security under the guidance of Dr.R.Shanmugavadivu at PSG College of Arts & Sciences,Coimbatore, India in Dept.of Computer Science and pursuing her M.Phil. Her research interests include Artificial Intelligence, Electroencephalography and Wireless Body Sensor Networks

Dr.R.Shanmugavadivu received M.Sc,M.Phil Degree in Computer Application from Bharathiar University,Coimbatore ,India.Finally she finished Doctorate of Ph.d in the domain of Data Mining from Bharathiar University, Coimbatore ,India.She is working as Assistant Professor in Department of Information Technology at PSG College of Arts and science,Coimbatore.She presented many research papers in National& International Conferences & journals.Her research interests include,Sensor Networks,Data mining and Networking.

REFERENCES:

1. Akyildiz, F., Su, W., Sankarasubramaniam, Y. & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine*, Vol 40, No 8, pp. 102-114, August 2002.
2. Araujo, A., Blesa, J., Romero, E., & Villanueva, D. (2012). Security in cognitive wireless sensor networks: Challenges and open problems. *EURASIP Journal on Wireless Communications and Networking*, p. 48, 2012.
3. Fei Hu, Xiaojun Cao."Wireless Sensor Networks :Principles and Practice", 1st Edition(2013),Auerbach Publication
4. Feng Zhao, leonidas Guibas,"Wireless Sensor Networks:An Information Processing Approach",Elsevier Publication.
5. Chan, H, Perrig, A., and Song, D., "Random key predistribution schemes for sensor networks", In IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213
6. Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.
7. Kargl, F., Lawrence E., Fischer M., and Lim Y. Y., Security, privacy and legal issues in pervasive ehealth monitoring systems. 7th International Conference on Mobile Business icmb, pp. 296–304, 2008.
8. Ng,H.S.,Sim,M.L. And Tan, C. M., Security issues of wireless sensor networks in healthcare applications. *BT Technol. J.* 24(2):138–144, 2006.CrossRef
9. Yong, W., Attebury, G., and Ramamurthy, B., A survey of security issues in wireless sensor networks. *IEEE Commun. Surv. Tutor.* 8(2):2–23, 2006. Second Quarter.CrossRef
10. Zia, T., and Zomaya, A., Security issues in wireless sensor networks. In Proceedings of International Conference on Systems and Networks Communications, 2006. ICSNC '06, vol., no., pp.40–40, Oct. 2006.
11. Y.C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.
12. Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi and John Pinkston. In Security for Sensor Networks.
13. Chris Karlof David Wagner. "In Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures"
14. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, K. Jones. On Providing Anonymity in Wireless Sensor Networks. In Proceedings of the Tenth International Conference on Parallel and Distributed Systems (ICPADS'04).
15. Chris Karlof, Naveen Sastry, David Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. ACM SenSys 2004, November 3-5, 2004.