Security Challenges in Wireless Sensor Network

[a] Navin Kumar Agrawal, [b] Dr. Arpit Jain, [c] Pramod Vishwakarma

a, b Asst Prof, *College of Computer Science and Information technology, Teerthankar Mahaveer University, Moradabad*

[a] garg.gla@gmail.com
[b] arpit.record@gmail.com

Abstract— **Wireless Sensor Networks are formed by exploiting a big amount of sensor nodes in a field for the surveillance of normally remote locations. A sensor node is made by many elements used to doing such operations like sensing, processing and transmitting data. Due to a few restrictions in security in Wireless sensor network security is a critical problem for users to use wireless sensor networks. The expansion of wireless sensor networks technology also incurs different types of security cheats for users. The first requirement of a user to use an application is that the application must be secured. Facilitating security to the remote sensor network is very competitive issue with make its functioning like this that it consumes less energy. The purpose of this paper is to elaborate the security based issues and problems faced by users in security of Wireless Sensor Network.**

Keywords— Wireless Sensor Network Security, Security issues in sensor Network.

I. INTRODUCTION

Wireless sensor network can be presented as a self-configured and self-pinning wireless network to consume physical or real world conditions such as voice, pressure, vibration, motion, temperature and to move the datagrams on the network to the destination or sink where the datagrams can be utilize or analyzed. A sink is a base station which performs like a VDU in computers i.e. like an interface between user and network. One can get the required data or information from the network by performing queries and get the result from the sink. Probably a Wireless sensor network have minimum 1 node while having hundreds of thousands of sensor nodes. The sensor nodes communicates to one another using radio signals within network. A wireless sensor node is endow with sensing and computing device, radio transceiver and power devices. The single node in a wireless sensor networks typically have limited processing speed, storage capacity and have low bandwidth to communicate with other nodes.

II. LIMITATIONS

The following part illustrated the restrictions in sensor networks which forms the structure of security agenda more difficult.

A. Node Limitations

A sensor node is of 4-9 MHz having 4KB of RAM, 128 KB flash and 916 MHZ of radio frequency. Combination of different sensor nodes is an increased limitation which restricts one security expositions.

B Network Limitation

Under node limitation, sensor networks gather all the restrictions of a node ad hoc network where they shortage physical under-pinning and they processed on unsecured wireless devices.

C. Physical Limitation

Sensor networks exploited in nature in real world (i.e. public or hostile) in some other devices makes them more sensitive to arrest. Physical security of node to make it more secure physically like tempered proof will affect the value.

III. CHARACTERISTICS

Sensor Networks are the future technology which will used in future in a very big amount. They are right now being exploited in churning monitoring, manufacturing and discharge assuming. Sensor nodes exploited in a huge amount in forethought geographical area to self-maintain into ad hoc wireless network to collect documents. A sensor node having a large number of exploited small, very less cost nodes that use without wire node-to-node network. They use multi-hop and group based roster algorithm based on finally used time (run time) network & discovery protocol. For the implementations of this paper we used Berkeley's Mica2Dot sensor node which is beneficial in form of figuring and communication resources.

VSECURITY IN SENSOR NETWORKS

Security in sensor networks is based on user that what should he needed to make protect. We illustrated 4 different security goals in sensor networks which are CIAA i.e. (Confidentiality, Integrity, Authentication, Availability).

ConfidentialityIt is the capability to restrict text or information from an unknown theft, where the text broadcast on sensor networks re-maintain

D. Integrity

It is the capability to prove that the text is nor theft by someone or not altered by anyone on the network.

E. Authentication

It is the ability to confirm the text is from which node, determining the reliability of text location.

F. Availability

It is used to observe that the node has the capability to use the capitals and to use resources and the netting is avail for the text to pass for another node.

A. Security classes

Pfleeger has shown four classes of preservation in computing system. We use these four malware classes in sensor networking. In computing systems the major components are hardware, software and data. In sensor network our purpose is to make safe to the network also, the bulge and the transmission between sensor bulge. The four classes of malware which exploit the compulsion of our preservation goals are shown below.

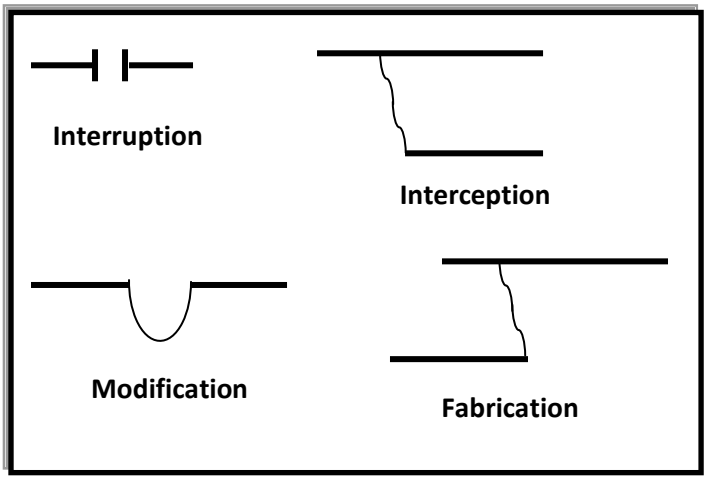

Fig. 1

In an Interruption, a transmission attachment in sensor network get break or may be terminated. Example of this type of malware are node abduction, text failure, adding some type of faulted code etc.

An interception defines the sensor network was being accommodation by ancompetitor where the hackers incomes unauthorized type of contact to sensor node or text. Suitable paradigm of this form of attack is bulge thefts.

Modification refers to unauthorized person cannot access the data but tampers with it, Suitable paradigm of this type of malware is modifying the datagrams have been transmitting causing a late time period of applicability thefts i.e. such as alluvion of networks with artificial or fraudulent data.

In Fabrication, an antagonist inputs wrong information or the collapsed information and play with the uprightness of data.

B. Attacks on Sensor Network

Building a base or structure of security threads in network, other part is for desirable security thefts in sensor network shown by:

a. False node: putting some malicious node by adding the wrong information or text, corrupted node can be commutations robust to decoy or hook these nodes restricts the other bulge to transfer information or text to it.
b. Message corruption: When format of data or part of data will made modify by the thefts it accommodate the text virtue.
c. Passive information gathering: Some thefts gather the data or information from network sensors if the data is not engrafted.
d. Node subversion: Thefts of nose may give its all information about its cryptographic keys it may accommodate the full sensor network.
e. Node malfunction: A malfunction node may provide wrong data that affects the virtue of sensor networks. Uniquely when the bulge is datagram gathering bulge. Paradigm is bunch node.
f. Node outage: Suppose when bunch of nodes stops its working what will happen? The whole sensor network properties could may be potent to ease the chattels of bulgeremoves by giving the second or other route.
g. More attacks: Chris Karloff el al has given some more precise thefts in sensor networks which are:

Sybil	An individual node shows its

attacks	multiple character, support to deflate the power of malware text or information tolerant programs i.e. sharing storage to different users and different routes for transferring data in bulges etc.
Sinkhole malwares	Captivate pressure of different bulge to an individual node. E.g. to make selective moving of data.

Fig. 2

C. Layering based Security Approach

1) Application Layer: Datagrams are gathered and maintained at this layer i.e. application layer, therefore it is our first priority to make sure the authenticity of datagrams. Wagner has given a resilient gathering program that is appropriate for bunch based network where a bunch skipper works as an gatherer in sensor network. While this type of approach is relevant if the gathering bulge is in hands with all the destination bulge and there is no disturbance in between the gatherer and destination bulge. In hierarchical bunching technique, the transmitting channel bounded by the gatherer and source station having very low amount of bandwidth because of the bunch skipper is an gatherer herself is a sensor bulge. To show the authority of an gatherer, bunch leader uses the cryptographic approach to be sure of the data grams reliability.

2) Network Layer: network layer performs the routing of text from bulge to bulge, bulge to bunch skipper, bunch skipper to bunch skipper, bunch skipper to source station and vice versa. Routing protocols in sensor network is of two types:

a. ID Protocol
b. Data Centric protocol

ID based protocol is that where data grams are routed to their final position based on the IDs specified in the datagrams and data centric protocol is that in which data grams having some attributes that shows that the data is of which type that has been provided.

3) *Data Link Layer:* It finds the error in the bulge and then detects it after that it does the correction if needed, it encoded the datagrams. Linking layer is protects or associated with jamming and DoS thefts. TinySec has described link layer encryption which is based on a key manage programmee. Somehow a theft have good energy power may perform an malware. Properties like LMAC have good jamming properties which are accommodate at Data Link Layer.

4) Physical Layer: It take cares of the exchange of information or text in between of sender and receiver however they may be nodes, data pace, signals quality, types of frequency always checked in Physical layer approach. Mainly FHSS (Frequency Hopping Spread Spectrum) is commonly used in sensor networks or bulges.

V. CONCLUSION

Wireless sensor networks is now very important for the upcoming future to every devices. In the unpresent of default preservation, exploit of sensor network is vulnerable to quality of thefts. Sensor nodes restriction and wireless transfer of data or thoughts or ideas or message become an individual security problem. Current research in sensor network security is commonly builded on a secured surrounding. There are different types of research problems remains unsolved before we can trust on sensor network. In this research I have mentioned thread individuals security problems occur in transferring data in wireless sensor network. On this study of wireless sensor network, I want to describe the need of a security framework to give countermeasure in front of malwares in wireless sensor networks.

REFERENCES

[1] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.
[3] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.
[4] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.
[5] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002.
[6] D. Wagner, Resilient aggregation in sensor networks, In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks. ACM Press, 2004, pp. 78-87.
[7] D. Ganesan, A. Cerpa, Y. Yu, and D. Estrin, Networking issues in wireless sensor networks, Journal of Parallel and Distributed Computing (JPDC), Special issue on Frontiers in Distributed Sensor Networks. Vol. 64, 2004.
[8] L.V. Hoesel and P. Havinga, A Lightweight Medium Access Protocol (LMAC) for wireless sensor networks: reducing preamble transmissions and transceiver state switches, in the proceedings of INSS, June 2004.
[9] C. karlof, N. Shastry and D. Wagner, TinySec: A link layer security architecture for wireless sensor networks, SenSys'04, November 3-5 2004, Baltimore, Maryland, USA
[10] H. Chan, A. Perrig, Security and privacy in sensor networks, IEEE Journal of Computing, Vol. 36, Issue 10, Oct. 2003, pp. 103-105
[11] F. Stajano, Security for Ubiquitous Computing, John Wiley and Sons, NY 2002, ISBN:0-470-84493-0
[12] E. Shi, and A. Perrig, Designing secure sensor networks, Journal of IEEE Wireless Communications, Vol. 11, Issue 6, Dec. 2004 pgs 38-43.