A survey on Wireless sensor Networks and its security attacks

R.Sheeba,*; A. AnishPremJani,*
*Assistant professor,Lord Jegannath college of Engineering and technology

Abstract -Wireless Sensor Network is a special type of network which finds its application in vast area. Though it is similar to ordinary network it is unique in its own way. Due to its efficiency and flexibility its application is increasing day by day. It is widely used in military applications, hospital, home applications, etc. Wireless Sensor Network senses or monitors various changes in the environment in which it is deployed. Since the wireless sensor network mainly finds its application in unattended areas it is vulnerable to several attacks. These attacks may be severe or may not be harmful.

Introduction

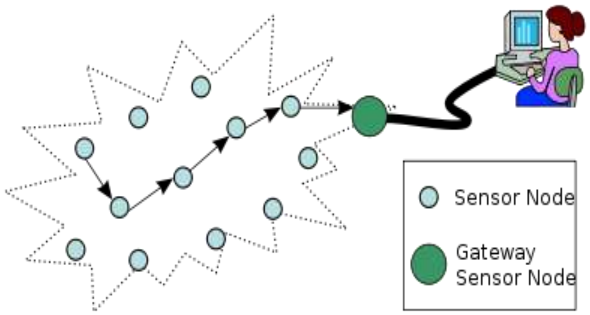
Advances in wireless and digital technologies and communication have lead to tremendous improvement in Wireless sensor networks. The improvements in various micro-electronics have lead to the development of low cost, low power networks. The wireless sensor network is improvement of our usual network.

The wireless sensor network consists of sensor nodes. The sensor node consists of a micro controller, external memory, transceiver, power source and sensors.The sensors available in the wireless sensor networks are spatially distributed to monitor and sense information or condition and co-operatively pass the data to a main location. The wireless sensor network finds its application in military applications, industry, home, industry,etc.

Working

The main functionof Wireless Sensor Network is to monitor and sense information and pass the sensed data or information through hoping or routing to a sink node in the network.The sensor nodes are usually scattered in the area. They do not follow any topology. The topology for the Wireless Sensor Network changes from one topology to another. Since, the sensor nodes are moving the topology goes on changing.

The following figure illustrates the working of Wireless Sensor Networks. Any change inthe working area of the network is sensed by the nearest sensor node.

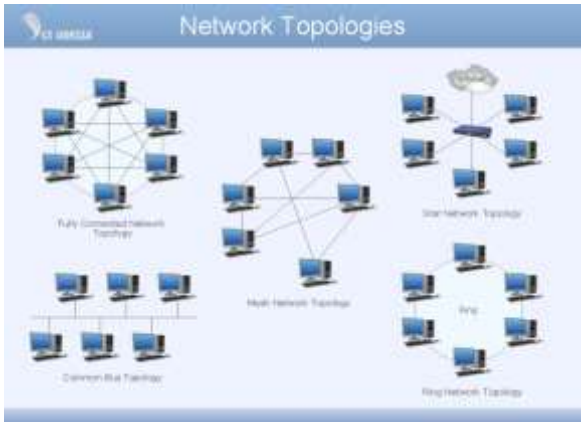


The sensed information is propogated from one sensor node to another until reaching the sink node. The sink node is one sensor node that is nearest to the final destination.The data or information is propogated using routing or hoping. The shortest path that is suitable to reach the sink node is usually selected for hoping or routing.

Topologies

To attain a good Quality of service(QOS) and Quantity of service, the best network topology should be selected. The selection of network topology also depends on the environment, economy and application that is to be applied. The basic network topologies

include mesh, star, ring, tree, bus.In fully connected network, all the nodes are connected to one another. This topology is completely incompatible for large scale sensor networks. Since, when a new node is to be added additional cable and other network problems arise.The following figure shows some of the basic network topologies.



In mesh topology, the nodes are regularly distributed and the communication is through the neighbour nodes. In this topology, group leaders are selected and if a group leader is disabled then another node takes that position automatically. In star topology all the nodes are connected to a single hub. If a communication to the central hub is lost then it affects only one link and the other links remain the same. In ring topology all the nodes are connected in a single direction. There is no group leader in this network. If a link is lost then the entire network is lost. A special form of ring topology is self healing ring topology.In bus topology all the nodes are connected through bus. The datas are received by reading the meassage header, where the destination address is specified. Here the data can be only retrieved and no retransmission is possible.

Constraints

Nodes in the Wireless Sensor Network are mainly resource contrainted. Some of the major constraints of Wireless Sensor Network are:

i. **Energy constraints**

Energy is consumed in Wireless Sensor Network for sensor transducer, communication and computation.

ii. Memory limitations

Sensor nodes are tiny devices. Hence, the memory and storage space is very small.The memory in Wireless Sensor Network is flash memory and RAM. Flash memory is used for storing application code and RAM memory is used to store intermediate results.

iii. Unreliable communication

Since there is no wired communication between nodes the chance for occurance of communication error is high. The communication error can be like packets may get damaged or packets may be corrupted or packets may collide and get damaged.

iv. High delay in communication

Due to routing and other hoping algorithms the communication between nodes may get delay.

v. Remote operation of WSN

Wireless Sensor Network finds its application mainly in rural areas where cannot interven easily. So, they are vulnerable to many security attacks. Though there are various methods and techniques followed in detecting and rectifying those attacks, they are very hard to be protected from those attacks.

Security

As already discussed, Wireless Sensor Network is vulnerable to several security attacks and hence protecting the wireless sensor network against such attacks is very essential. Some of the basic requirements in security is listed and explained below:

i. Data confidentiality

One of the main attack in wireless sensor network is that the confidential data is attacked to a greater extend than any other data.Hence, the confidential data should be protected from data attacks. Once an attacker gains access to the confidential datas in the network, then the chances for the attacker to control the network is very high. The network should not allow any other node than the recipient node to read the data that is being transferred. Even the secret key that is being transmitted should be encrypted and then transferred. Public information should also be handled carefully.

ii. Data integrity

The data that is being transmitted should not be altered by any intruder. Certain intruders try to alter the data if they cannot read or cause any other type of damage to the network.

iii. Availability

It is important to ensure that the data that is required should be always available in the network even when the network is under attack.

iv. Data freshness

It is always important to keep the data in the network fresh and upto date. The keys that are used for encryption should also be refreshed so that even if an adversary captures an already available key the network can operate without any failure.

v. Self healing

The nodes in a wireless sensor network should be self healing. This is a very challenging work. Since, the nodes are almost available in vast rural area where human intervention is low and high possibility of attacks are available. The process of making a sensor node as self healing is very challenging.

vi. Secure location

The sensor nodes should be located in the area where they are efficient and highly safe. There are various schemes available to locate the sensor nodes securely in the network. Both centralized and de – centralized methods can be followed.

vii. Authentication

The sensor nodes available in a wireless sensor node should be authentic. It is nothing but each sensor node should be ready to authenticate itself to other nodes available in the network. Also the nodes in the network should ensure that the intented node only has received the information.

Attacks

As we have already seen there are various requirements for the security. The various attacks which occur to the described requiements is explained below:

i. Attack against service integrity

In this attack the network is made to fail from its intended work or behaviour. Also the adversary can try and inject false or unwanted values into the network which may remain unknown to the sensor nodes or these attacks may cause damage to the network.

ii.Attack on availability

The attack on the availability of network resources and other required data can be referred as an attack on availability. This attack can be also referred as Denial of service(DOS) attack

iii. Attack on secrecy and authentication

Usual cryptography and other related algorithms and methods can be followed to protect secrecy and authentication.

i. Attack on availability

Though there are various methods available to prevent from these type of attacks none is favourable. Some of the types are given

i. Physical layer attacks

The security attack is on the physical layer which is responsible for frequency selection and other communication related things. The attacker can jam or tamper the communication.The jamming attack is that the adversary can cause a communication damage in the way in which the sensor nodes communicate. The attack can also be on the frequency in which the sensor usually communicate.The tampering attack refers to the attack in which the communication between the sensor nodes is completely blocked. This type of attacks affects the nodes severly.

ii.Data link layer attack

Link layer performs the function of multiplexing the data frames and blocks of data between various other nodes available. An attacker can attack this layer by causing frames or blocks to collide,thus causing retransmission of data. The attacker can also capture acknowledgement messages and messages which carry the encryption key,etc.

iii. Network layer attacks

Network layer is responsible for packet forwarding and routing data or information through intermediate nodes. Variable length data sequences are forwarded through this layer.There are various types of attacks available in this network layer. Some of them are explained. The very first and most common attack is the **spoofing attack**. In this attack, the attacker may alter or replay the information to create a disrupt in the traffic available in the network.Another type of network layer attack is **selective forwarding**. In this attack, the attacker may compromise a particular node and set its properties such that the node keeps on forwarding only to a particular node.

Another attack is **sinkhole attack**. In this attack a particular node resides as attractive to its neighbouring nodes and thus always the traffic flows through that particular node. Thus, causing a network traffic.

Sybil attack is another type of attack in which the sensor nodes have more than one identity in the network. This type of attack affects the network in various ways. Whatever may be the method that is to be followed by the network this type of attack affects the network. It works the same way for the networks.

Hello attackis another type of attack in which an adversary causes a mis communication. In this attack, an adversary who is very far away from the sensor node sends a hello message to the sensor node which is requesting for transmission. The sensor node after receiving the hello message thinks that the node is within the range and sends the data to be transmitted through the attacked node.

Worm hole attack is another type of attack in which the data available in one location is copied and transferred to another location.

iv. Attack in transport layer

Transport layer is responsible for efficient transport between various nodes in the network. One of the major type of attack an attacker cause to the transport layer is the flooding attack. In the flooding attack, the attacker keeps on sending request to a node so that the node becomes flooded with connection request and finally comes to a state so that it cannot receive any furtherlegitimate request.De-synchronization is another type of attack in which the attack disconnects an existing connection. The attacker may request for re-transmission again and again and finally causing energy loss in the network nodes.

ii. Attacks on secrecy and authentication

This attack is mainly on the secure and secret data available in the sensor nodes present in a network.

i. Node replication attack

In this attack, the adversary captures a particular node in the network then copies its identity and other security information and repeats the same node with the copied information into the network. With this attack the adversary can even capture an entire network.

ii. Attacks on privacy

Preserving privacy in Wireless Sensor Network is very challenging and difficult. Since all the data available in a sensor network is highly sensitive. Some of privacy problems that occur in a network is given

Eavesdropping attack is a very common attack. In this attack, the adversary tries to understand the information in the network.

Passivemonitoring is another form of privacy attack in network. In this attack, the adversary keeps monitoring the sensor nodes and tries to understand information available in the network.

Trafficanalysisis another attack on privacy in network. In this attack the adversary keeps on monitoring the traffic in the network and finds which the nodes to be attacked.

Masquerade is another type of attack in which the adversary covers up an good node and produces a compromised node and ask the network to transfer data through the compromised node and thus reads the data that is being shared through it.There are also various other types of attack possible and further to be identified in a Wireless Sensor Network. Thus the protection of Wireless Sensor Network from attacks is really very difficult and challenging.

References

[1] R. Jordan and C.A. Abdallah, "Wireless communications and networking: an overview," Report, Elect. and Comp. Eng. Dept., Univ. New Mexico, 2002.

[2] F.L. Lewis " Wireless Sensor Networks" Smart Environments: Technologies, Protocols, and applications , New York, 2004.

[3] Ian F. Akyildiz, Weilian Su, YogeshSankarasubramaniam, and ErdalCayirci, Georgoa Institute of Technology.

[4] Chee-Yee Chong, Member, IEEE And Srikanta P. Kumar, Senior Member, IEEE "Sensor Networks: Evolution, Opportunities, and Challenges"

[5] P. Gupta and P. R.Kumar, "The capacity of wireless networks," IEEE Trans. Inform. Theory, vol. 46, pp. 388–404, Mar. 2000.

[6] B. Deb, S. Bhatnagar, and B. Nath, "A topology discovery algorithm for sensor networks with applications to network management," Dept. Comput. Sci., Rutgers Univ., Tech. Rep. DCS-TR-441, 2001.

[7] "Distributed tracking in distributed sensor networks," presented at the Amer. Control Conf., Seattle, WA, 1986.

[8] ArchanaBharathidasan, Vijay AnandSaiPonduru "Sensor Networks: An Overview".

[9] Simulation Environment," UCLA Computer Science Department Technical Report 990027, May 1999.

[10] D. Braginsky and D. Estrin, "Rumor Routing Algorithm For Sensor Networks," Under submission to International Conference on Distributed Computing Systems (ICDCS-22), November 2001.

[11] M. Brain and T. Harris, "How GPS receivers work," http://www.howstuffworks.com/gps1.htm.

[12] N. Bulusu, J. Heidemann and D. Estrin, "GPS-less Low Cost Outdoor Localization For Very Small Devices," IEEE Personal Communications, Special Issue on "Smart Spaces and Environments", Vol. 7, No.5, pp. 28-34, October 2000.

[13] N. Bulusu, J. Heidemann and D. Estrin, "Adaptive Beacon Placement," Proceedings of the Twenty FirstInternational Conference on Distributed Computing Systems (ICDCS-21), Phoenix, Arizona, April, 2001.

[14] N. Bulusu, J. Heidemann, V. Bychkovskiy and D. Estrin, "Density-adaptive beacon placementalgorithms for localization in ad hoc wireless networks," UCLA Computer Science Department TechnicalReport UCLA-CS-TR-010013, July 2001.

[15] N. Bulusu, D. Estrin, L. Girod and J. Heidemann, "Scalable Coordination for wireless sensor networks:Self-Configuring Localization Systems," In Proceedings of the Sixth International Symposium onCommunication Theory and Applications (ISCTA 2001), Ambleside, Lake District,UK, July 2001

[16] N. Bulusu, V. Bychkovskiy, D. Estrin and J. Heidemann, "Scalable, Ad Hoc Deployable, RF-BasedLocalization", In Proceedings of the Grace Hopper Celebration of Women

in Computing Conference 2002,Vancouver, British Columbia, Canada, October 2002.

[17] D. E. Culler, J. Hill, P. Buonadonna, R. Szewczyk, and A. Woo, "A Network-Centric Approach toEmbedded Software for Tiny Devices," EMSOFT 2001:First International Workshop on EmbeddedSoftware, Oct. 2001.

[18] L. Doherty, "Algorithms for Position and Data Recovery in Wireless Sensor Networks," EECS MastersReport,UC Berkeley, May 2000.

[19] D. Estrin, R. Govindan, J. Heidemann and S. Kumar, "Next Century Challenges: Scalable Coordinationin Sensor Networks," In Proceedings of the Fifth Annual International Conference on Mobile Computingand Networks (MobiCOM '99), August 1999, Seattle, Washington.

[20] D. Estrin, L. Girod, G. Pottie, M. Srivastava, "Instrumenting the world with wireless sensor networks,"In Proceedings of the International Conference on Acoustics, Speech and Signal Processing (ICASSP 2001),Salt Lake City, Utah, May 2001.

[21] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, "Highly-Resilient, Energy-Efficient MultipathRouting in Wireless Sensor Networks," ACM Mobile Computing and Communications Review, Vol. 5, No.4, October 2001.

[22] W. Ye, J. Heidemann and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless SensorNetworks," In Proceedings of the 21st International Annual Joint Conference of the IEEE Computer andCommunications Societies (INFOCOM 2002), New York, NY, USA, June, 2002.

[23] Y.J.Zhao, R. Govindan, and D. Estrin, "Residual energy scan for monitoring sensor networks ,"Wireless Communications and Networking Conference, 2002 (WCNC2002), 2002 IEEE , Volume: 1 , Mar.17-21, 2002 Page(s): 356 –362.