Wireless Sensor Network: Application, Service Attacks, and Security Schemes

Rupam Sharma[1], Nidhi Tripathi[2]
[1 & 2]Department of Computer Science, Gwalior Institute of Technical Studies, Gwalior

Abstract

Wireless Sensor network is an emerging technology and have great potential to be employed in critical situations like battlefield and commercial applications. In recent scenario, security is most crucial issue in almost every network including wireless sensor network. There are some crucial security issues and many attacks that need to be look around. In this paper, we comprise and discuss emerging issues of security threats in wireless sensor network.

Keywords

Wireless Sensor network, Application, Service attacks, Security Schemes.

1. Introduction

Wireless Sensor networks (WSN) are highly distributed networks of tiny, wireless nodes-lightweight, deployed in large numbers to monitor the environment or system by the measurement of physical parameters as previously discussed [1]. Basically WSNs are developed on the basis of need and their application. These are generally designed for real time analysis of low level data in hostile environments and they are well suited to a substantial amount of monitoring and surveillance applications. Wireless sensor networks have broad list of their applications [1]. Hence the security is an important and crucial issue now-a-days.

In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. The applications of sensor networks are endless, limited only by the human imagination [2, 3]. There is need to investigate the security attacks of WSN that are more concern to routine aspects of common human. Therefore this article provides comprehensive overview with recent update on various service attacks and security measures of wireless sensor networks.

2. Applications of WSN

Wireless Sensor Networks (WSN) has off late, found applications in wide-ranging areas (Fig. 1). Therefore, we discuss here WSN applications related to some prominent areas related to useful tools in military, medical, environmental and different industries [2, 3, 4]. These applications have major concern about need and safety of individual.

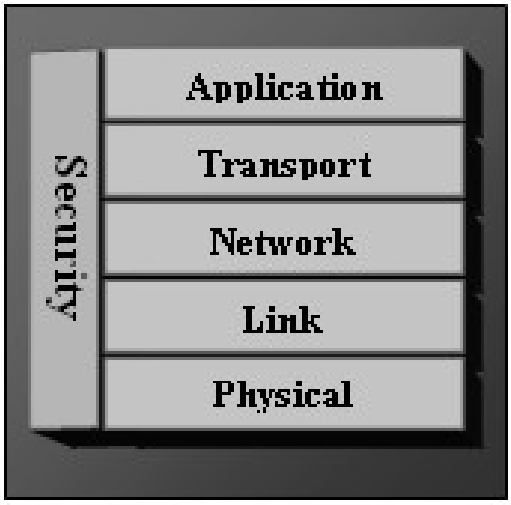

Fig 1 Security in wireless sensor networks

2.1. The military applications

Sensor nodes include battlefield surveillance and monitoring, guiding systems of intelligent missiles and detection of attack by weapons of mass destruction.

2.2. The medical application

Sensors can be extremely useful in patient diagnosis and monitoring. Patients can wear small sensor devices that monitor their physiological data such as heart rate or blood pressure.

2.3. Environmental monitoring

It includes traffic, habitat, Wild fire etc.

2.4. Industrial applications

It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc.

2.5. Monitoring application in infrastructure protection

It includes power grids monitoring, water distribution monitoring etc.

2.6. Other applications

Sensors will soon find their way into a host of commercial applications at home and in industries. Smart sensor nodes can be built into appliances at home, such as ovens, refrigerators, and vacuum cleaners, which enable them to interact with each other and be remote – controlled.

3. Securing Attacks in WSN

First of all Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically safe.

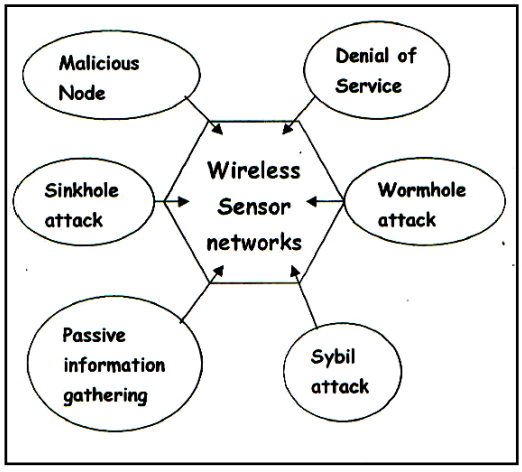

Fig 2 Security attacks on wireless sensor networks

Many sensors network routing protocols are quite simple and massages are recorded in form of data. The data obtained by the sensing nodes needs to be kept confidential and it has to be authentic. In the absence of security a false or malicious node could intercept private information, or could send false messages to nodes in the network. Major attacks of WSN are showing in the figure 2 i.e. Denial of Service (DOS), Wormhole attack, Sinkhole attack, Sybil attack, Passive information gathering, Node capturing, Malicious node and Hello flood attack.

3.1. Denial of Service (DoS)

This type of attack results into making unavailable the resources to their intended users. As an example node 'A' sends request to node 'B' for communication and node 'B' sends acknowledge to node 'A' but 'A' keeps on sending request to 'B' continuously. As a result 'B' is not able to communicate with any other nodes and thus becomes unavailable to all of them.

Denial of service attack may also occur at physical layer by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and unfairness in use of networks. In network layer, it occurs by way of neglecting and the greediness of packets resulting into path failure.

In transport layer, DOS attack occurs due to flooding and de-synchronization. Most of denial of service attacks may be prevented by powerful authentication and identification mechanisms.

3.2. The wormhole attack

One node in the network (sender) sends a message to another node in the network (receiver node) [4].Then the receiving node attempts to send the message to its neighbors. The neighboring nodes think the message was sent from the sender node (which is usually out of range), so they attempt to send the message to the originating node, but it never arrives since it is too far away. Wormhole attack is a significant threat to wireless sensor networks, because, this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover neighboring information. Wormhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

3.3. The Sybil attack

In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network. The incorrect information can be a variety of things, including position of nodes, signal strengths, making up nodes that do not exist. Authentication

and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but he should only be able to do so using the identities of the nodes he has compromised. Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor networks.

3.4. Sinkhole attacks

In a sinkhole attack, the adversary's aim is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive with high capability resources like high processing power and high bandwidth to surrounding nodes by which it always creates shortest path with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example, a laptop class adversary has a strong power radio transmitter that allows it to provide a high quality route by transmitting with enough power to reach a wide area of the network [5].

3.5. Passive information gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them [6]. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques should be used.

3.6. Node capturing

A particular sensor might be captured, and information stored on it might be obtained by an adversary [4].

3.7. Malicious Node

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network [6]. Insertion of malicious node is one of the most dangerous attacks that can occur and could spread malicious code to all nodes which potentially destroy the whole network or even worse.

3.8. Hello flood attacks

The Hello flood attacks in wireless sensor network can be caused by a node which broadcasts a Hello packet with very high transmission power to sender or receiver. The nodes receiving the messages assume that the sender node is nearest to them and sends packets by this node [7]. By this attack congestion occurs in the network. Blocking techniques are used to prevent Hello Flood attacks.

4. Data Security Schemes for WSNs

Studies revealed how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's lifetime. It aim sat increasing energy efficiency for key management in wireless sensor networks and uses [2]. Wood et al. (2002) studies DoS attacks against different layers of sensor protocols tack [8]. JAM presents a mapping protocol which ejects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming.

In another study, the authors show that worm holes those are so far considered harmful for WSN could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks. Ye *et.al.* (2005) presents a Statistical En-route Filtering (SEF) mechanism to detect injected false data in sensor network and focus mainly on how to filter false data using collective secret and thus preventing any single compromised node from breaking the entire system [9]. SNEP & μTESLA are two secure building blocks for providing data confidentiality, data freshness and broad cast authentication. TinySecra (2004) proposes a link layer security mechanism for sensor networks, which uses an efficient symmetric key encryption protocol [10]. In another paper, a probabilistic secret sharing Protocol has been defined to defend Hello flood attacks. The scheme uses a bidirectional verification technique and also introduces multi-path multi-base station routing if bidirectional verification is not sufficient to defend the attack.

A holistic approach aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option.

We should be concentrating more on sensor node themselves, because nearly all attacks on WSN starts from compromising a node. Since physical tampering cannot be avoided. Care must be taken to prevent software based

tempering. There are enough chances that applications/ operating system running in sensor node are vulnerable to popular exploits such as buffer overflow. Here, the problem is with composing the components of the overall system. A secure system can be realized only by building security in to the system architecture and this requires:-

- Security analysis of the architecture.
- Security testing of the realized system for implementation bugs.
- Removal/scrutiny of "undocumented features" that can be potentially exploited to violate the system security.

5. Conclusion and Future Scope

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. In Industries, product of the WSN will not get acceptance unless there is a full proof security to the network. In this paper, we discussed crucial security attacks of WSN's. Importance of the data security schemes for WSN's and emphasized on holistic approach on data security schemes for most of WSN's. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required for these wireless sensor network. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas yet cryptography itself is not sufficient for defending the network against insiders and laptop-class attackers; thus designing the protocols carefully is required as well.

6. References

[1] Sharma, K. & Ghose, M.K., "Wireless Sensor networks: An overview on its security threats", IJCA A special issue on "Mobile Ad-hoc networks" MANETs, 2010.

[2] Jamal N. Al-Karaki & Ahmed E. Kamal, "Routing Techniques in Sensor Networks: A survey", IEEE communications, Volume 11, No. 6, Dec. 2004, pp. 6-28, 2004.

[3] Al-Sakib khan Pathan et.al)"Security in wireless sensor networks: Issues and challenges" in feb.20 22, 2006, ICACT2006, ISBN 89-5519-129-4 pp 1043-1048, 2006.

[4] M. Tubaishat, S. Madria, "Sensor Networks: An Overview ", IEEE Potentials, April/May 2003.

[5]] E. C. H. Ngai, J. Liu, and M. R. Lyu,"On the intruder detection for sinkhole attack in wireless sensor networks," in Proceedings of the IEEE International Conference on Communications (ICC '06), Istanbul,Turkey. 2006.

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermeasures," AdHoc Networks Journal, vol. 1, no. 2–3,pp. 293–315, September 2003.

[7] Adrian Perrig, John Stankovic, and David Wagner, "Security in wireless sensor networks", Commun.ACM,47(6):53-57, 2004.

[8] A.D. Wood and J.A. Stankovic, "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp. 54–62, 2002.

[9] Yee Wei Law Paul J. M. Havinga, "How to Secure a Wireless Sensor Network", ISSNIP; 2005, IEEE2005, pp 89-95, 2005.

[10] Chris Karlof, Naveen Sastry, David Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. *ACM SenSys 2004, November 3-5, 2004.*

Author's Profile

Rupam Sharma has received her Bachelor of Engineering degree in Information Technology from Institute of Professional studies, Gwalior in the year 2011. At present she is pursuing M.Tech. in Computer Science from Department of Computer Science, Gwalior Institute of Technical Studies, Gwalior. Her area of interest is Wireless Sensor Network and development of new security of WSNs.

Nidhi Tripathi has received M. Tech. in Computer Science. At present he is working as Head of Department, Department of Computer Science, Gwalior Institute of Technical Studies, Gwalior. Her area of interest is analysis of performance of Wireless Sensor Networks and development of innovative security for WSNs.