Volume 2, No. 1, Jan-Feb 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Empirical study on security attacks in Wireless Sensor Network

Vasanthi.V
Ph.D Research Scholar, Department of Computer Science,
Karpagam University
Coimbatore,India
vasarthika@gmail.com

M.Hemalatha*
Head, Dept of Software Systems,
Karpagam University,
Coimbatore,India
hema.bioinf@gmail.com

Abstract: Since, wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks are interacted with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. Various security risks are involved in the operation of WSN counter measures, and existing solutions are reviewed. There is currently enormous research potential in the field of WSN security. Thus, it familiar with the current research in this field will benefit researchers greatly. With this in mind, we survey the topics in wireless sensor network security, and present the obstacles and the requirements in the sensor security, classify them in many of the current attacks, mechanisms and challenges and finally list their corresponding defensive measures.

Keywords: wireless sensor network, Protocols, Security, Attacks, security goals, challenges.

I. INTRODUCTION

Since, sensor networks are application dependent Wireless sensor networks have become a growing area of research and development due to the tremendous number of applications that can greatly benefit from such systems and has lead to the development of tiny, cheap, disposable and self contained battery powered computers, known as sensor nodes or "motes", which can accept input from an attached sensor, process this input data and transmit the results wirelessly to the transit network. It is well suited to a substantial amount of monitoring and surveillance applications. The wireless sensor network applications such as military command, industrial quality control, observation of critical infrastructures, smart buildings, healthcare. Major of the sensor network are deployed in hostile environments with active intelligent opposition [9]. The security problem is a crucial issue. This problem is due to the wireless nature of the sensor networks and constrained nature of resources on the wireless sensor nodes, which means that security architectures used for traditional wireless networks are not viable. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a very dangerous environment where they are not physically protected. In this paper we discuss some of the applications of WSN, Security goals, Classification of Security Attacks, Security
Mechanisms and Challenges in Wireless Sensor Networks.

II. APPLICATIONS OF WSN

Wireless Sensor Networks (WSN) has applications in wide-ranging areas. In this section we list some of the applications in WSN[2].

[a] Military command: Applications of sensor nodes include battlefield surveillance and monitoring, guiding systems of intelligent missiles and detection of attack by weapons of mass destruction

[b] Industrial quality control: It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc.

[c] Observation of critical infrastructures: It includes power grids monitoring, water distribution monitoring etc.

[d] Smart buildings: Sensors can also be used in large buildings or factories monitoring climate changes. Thermostats and temperature sensor nodes are deployed the areas around the building. In this additionally, sensors could be used to monitor vibration that could damage the structure of a building.

[e] Healthcare: Sensors can be used in biomedical applications to improve the quality of the provided care. Sensors are implanted in human body to monitor medical problems like cancer and help patients maintain their health.

III. SECURITY GOALS

Wireless sensor networks are vulnerable to many attacks because of broadcast nature of transmission medium, resource limitation on sensor nodes and uncontrolled environments where they are left unattended. Similar to other communication systems [2][9], WSN have general security goals represented in figz

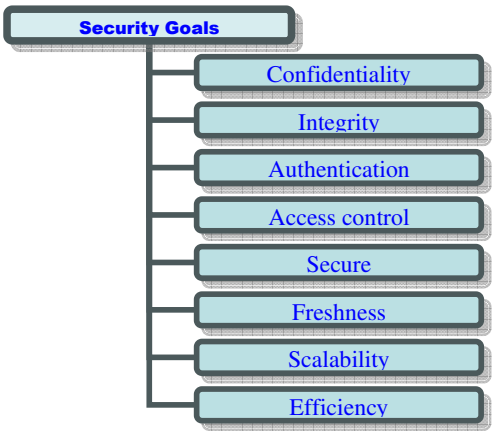

Figure 1: **Common security goals**

Confidentiality: protecting secret information from unauthorized entities.

Integrity: ensuring message has not been altered by malicious nodes.

Data Origin Authentication: authenticating the source of message.

Entity Authentication: authenticating the user/node/base-station is indeed the entity whom it claims to be.

Access control: system which enables an authority to control access to areas and resources in privileged entities.In addition, WSNs have following specific security objects:

Forward secrecy: preventing a node from decrypting any future secret messages after it leaves the network.

Backward secrecy: preventing a joining node from decrypting any previously transmitted secret message

Survivability: providing a certain level of service in the presence of failures and/or attacks

Freshness: ensuring that the data is recent and no adversary can replay old messages

Scalability: supporting a great number of nodes

Efficiency: process, storing and communication limitations on sensor nodes are must be Consider.

IV. CLASSIFICATIONS OF SECURITY ATTACKS

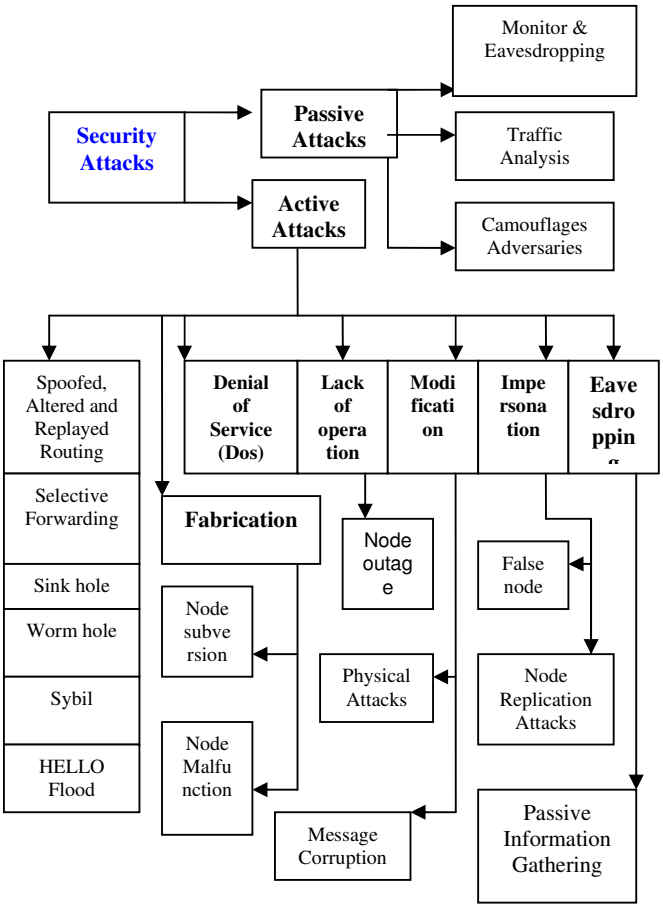

Figure 2**. Classification of security attacks**

Passive Attacks: Passive attacks are in the nature of eavesdropping on, or monitoring of transmissions. The motive of the attacker is to obtain information that is being transmitted. Two types of passive attacks
[a] Release of message contents
[b] Traffic analysis.

Monitor and Eavesdropping*:* This is the most commonly attacked attacker to privacy. By listening to the data, the adversary could easily discover the communication contents. Network traffic is susceptible to monitoring and eavesdropping [11]. This should be no cause for concern given a robust security protocol, but monitoring could lead to attacks similar to those previously described. It could also lead to wormhole attacks.

Traffic Analysis: This is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed when the messages are encrypted. Traffic analysis attacks are forged, where the base station is determinable by observation that the majority of packets are being routed to one node. If an adversary can compromises the base station then it can render the network useless.

Camouflage Adversaries*:* One can insert their node in the sensor network. Then these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

Active Attacks: Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into these categories:

[a] Routing Attacks in Sensor Networks
[b] Denial of Service Attacks
[c] Node Subversion
[d] Node Malfunction
[e] Node Outage
[f] Physical Attacks
[g] Message Corruption
[h] False node

Routing Attacks in Sensor Networks:

Spoofed, altered and replayed routing Information: An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information [12]**.**

Selective Forwarding: A node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node, such as the sinkhole attack or acknowledgement spoofing. The attack can be used to make a denial of service attack targeted to a particular node. If all packets are dropped, then the attack is called a "black hole".

Sybil attack: Authentication is must for prevention against this attack.[1]

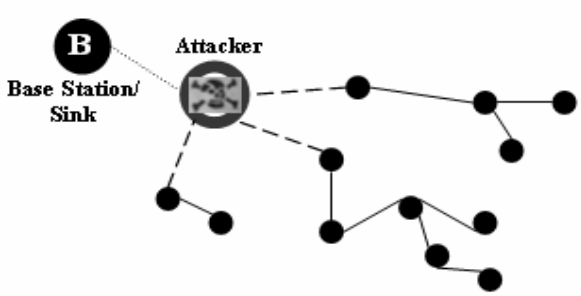

Figure 4. Sybil attack

Sinkhole attack & Wormhole attack: It occurs on the route between sensor and base station. Regular monitoring and flexible route selections are needed. wormholes use channels that are invisible to the network and the advertised routes of sinkholes are extremely hard to verify.

HELLO flood attacks: In a HELLO flood attack a malicious node can send, record or replay HELLO-messages with high transmission power. It creates an illusion of being a neighbor to many nodes in the networks and can confuse the network routing badly. Such attacks can easily be avoided by verify bi-directionality of a link before taking action based on the information received over that link.

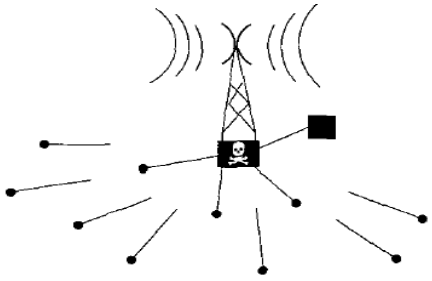

Figure 5.HELLO flood attack

Denial of Service (DoS) Attacks:

It occurs by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a networks capability to provide a service [11].

In wireless sensor networks, several types of DoS attacks in different layers are as follows.

[a] Physical layer - jamming and tampering,
[b] Link layer - collision, exhaustion, unfairness.
[c] Network layer - neglect and greed, homing, misdirection, black holes.
[d] Transport layer -this attack could be performed by malicious flooding and de synchronization

Node Subversion: Capture of a node that reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured and information are stored on it might be obtained by an adversary.

Node Malfunction: A node in a WSN may malfunction and generate inaccurate or false data. The node serves as an intermediary, forwarding data on behalf of other nodes it may drop or garble packets in transit. Detecting and culling these nodes from the WSN becomes an issue.

Node Outage: If a node serves as an intermediary or collection and aggregation point, what happens if the node stops functioning? The protocols employed by the WSN need to be robust enough

Mitigate the effects of outages by providing alternate routes.

Physical Attacks: Sensor networks operate in hostile outdoor environments. In these environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks. Physical attacks destroy sensors permanently, so loss is irreversible. At any time, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

Message Corruption: Attacks against the integrity of a message occur when an intruder inserts themselves between the source and destination and modify the contents of a message.

False Node: An intruder might "add" a node to a system and feed false data or block the passage of true data.

V. SECURITY MECHANISM

Security is sometimes viewed as a standalone component of a system's architecture, where security is provided for every module [11]. This separation is, however, usually a flawed approach to network security. To achieve a secure system, security must be integrated into every component that can be designed without security can become a point of attack. Consequently, security must be in every aspect of system design. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high-level and low-level.

Low-Level Security Mechanism

Low-level security primitives for securing sensor networks includes,

[a] Key establishment and trust setup
[b] Secrecy and authentication
[c] Privacy
[d] Robustness to communication denial of service
[e] Secure routing

Key establishment and trust setup: When setting up a sensor network, the first requirements is to establish cryptographic keys for later use. As we know sensor devices have limited computational power, making public-key cryptography [12] primitives too expensive in terms of system overhead. Key-establishment techniques need to scale to networks with thousands and more number of nodes. The simplest solution for key establishment is a sharing key. It could be possible for the attacker to compromise a single node that would reveal the secret key and thus allow decryption of all network traffic. To overcome this problem is to use a single shared key to establish a set of link keys, one per pair of communicating nodes, and then erase the network wide key after setting up the session keys.

Secrecy and authentication: Cryptography is the standard defense [14] measures that provide the protection against eavesdropping, injection, and modification of packets. For achieving a high degree of security we use end-to–end cryptography in point-to-point communication but it requires that keys be set up among all end points and be incompatible with passive participation and local broadcast.

Privacy: Sensor networks have thrust privacy concerns to the forefront. The most obvious risk is that ubiquitous sensor technology might allow ill intentioned individuals to deploy secret surveillance networks for spying on unaware victims. Therefore, an additional system requirement is that guidelines regarding fair information practices are built into, the networks, in an attempt to protect privacy rights.

Robustness to communication denial of service:
In WSN, the intention of the attacker is to disrupt the network traffic by broadcasting a high-energy signal. If the transmission is powerful, then the entire system's communication could be jammed. One standard defense against jamming employs spread-spectrum communication. The networked nature of sensor networks allows new, automated defenses against denial of service.

Secure routing: One major challenge to secure routing in WSNs is that it is very easy for a single node to disrupt the entire routing protocol by simply disrupting the route discovery process. Papadimitratos and Haas propose a secure route discovery protocol that guarantees, subject to several conditions, that correct topological information will be obtained [17].

High-Level Security Mechanism
High-level security primitives for securing sensor networks includes,

[a] Secure Group Management
[b] Intrusion detection
[c] Secure Data Aggregation

Secure Group Management: Since sensor nodes are required to group themselves in order to fulfill a particular task, it is necessary that the group members communicate securing between each other, despite, the fact that global security may also be in use. In other words, the processing of the raw data consists of dividing the network into small groups and analyzing the data aggregated, by the group leaders. So the group leader has to authenticate the data it is receiving from other nodes in the group. so it requires group key management.

Intrusion detection: Typically a wireless sensor network uses cryptography to secure itself against unauthorized external nodes gaining entry into the network. But cryptography can only protect the network against the external nodes and does little to thwart malicious node that already possess one or more keys. An Intrusion Detection System (IDS) monitors a host or network for suspicious activity patterns outside normal and expected behavior. Brutch and Ko have surveyed the challenges in intrusion detection and have proposed watchdog, control messages, neighborhood watch and anomaly detection as Possible solutions to dynamic source routing attacks. Since it is not possible for every nod e to have a full powered IDS agent due to resource limitations, the basic problem in this area is how to distribute the intrusion detection agents and their tasks in the network.

Secure Data Aggregation: Data aggregation (or "fusion") is necessary in sensor networks to reduce the amount of data transmitted to the base station. This is possible because a sensor network is data centric [].It could be possible for attacker to control over an aggregating node, injecting the false reports or ignore reports affecting the credibility of the generated data and hence the network as a whole. The main aim of this area is to use resilient functions, that will be able to discover and report forged reports through demonstrating the authenticity of the data somehow. Wagner established a technique in which the aggregator uses Merkle hash trees to create proof of its neighbor's data, which in turn is used to verify the purity of the collected data to the base station.

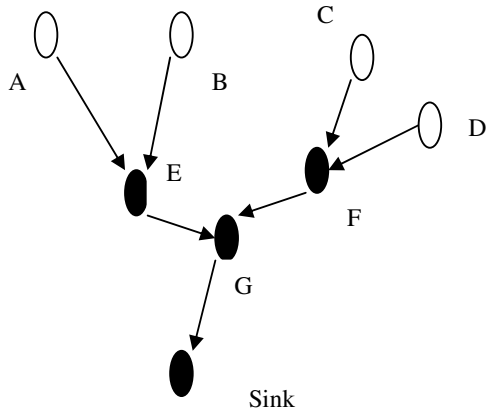

Figure 6: Data Aggregation

VI. CHALLENGES FACED IN SENSOR NETWORK

The WSNs has presenting many significant challenges in designing security schemes. A WSNs is a special network which has many constraint compared to a traditional computer network.

[a] Wireless Medium
[b] Ad-Hoc Deployment
[c] Hostile Environment
[d] Resource Scarcity
[e] Immense Scale
[f] Unreliable Communication
[g] Unattended Operation

Wireless Medium: In WSN, nodes are connected with each other, and the traffic pattern is toward the sink through the gateways, uses variable bands of frequency depending upon the nature and type of application, as for example, the WSN used for animal tracking or habitat monitoring uses 174 MHz, while most of the alarming sensor nodes use 434 MHz frequency band [8].

Ad-Hoc Deployment: This sensor networks means no structure can be statically defined. The network topology is always subjected to changes due to node failure, addition, or mobility [12]. Nodes may be deployed by airdrop, those nodes may failed or to be replaced the network must support self-configuration. Security schemes must be able to operate within this dynamic environment.

Hostile Environment: It is major challenging factor in which sensor nodes function. Motes face the possibility of destruction or captured by attackers. The nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, disassemble it, and extract from it valuable information (e.g. cryptographic keys such as secret key, private key, etc). The highly hostile environment represents a serious challenge to security researchers.

Resource Scarcity: The resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, Security, computational complexity, and memory like space allocation. There is no such trivial task. Energy is the most precious resource for sensor networks in security Resource. Communication is too expensive in terms of power. Security mechanisms must give special effort to be communication efficiently.

Immense Scale: The proposed scale of sensor networks which are posed a significant challenge for security mechanisms. Simply networking hundreds and thousands of nodes has proven to be a substantial task. While providing security to small to large networks here is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiently.

Unreliable Communication: The unreliable communication is another threat to sensor security. The security of the networks becomes relies heavily on a defined protocol, which in turn depends on communication.

[a] Unreliable Transfer
[b] Conflicts
[c] Latency

Unattended Operation: The function of particular sensor network depends on unattended nodes for long period of time. There are three main cautions to unattended sensor nodes [12]:

[a] Exposure to Physical Attacks
[b] Managed Remotely
[c] No Central Management Point

VII. CONCLUSION

All of the previously mentioned are Applications of WSNs, Security goals, Security Mechanisms and the attacks like Hello flood attack, wormhole attack, Sybil attack, sinkhole attack, serve one common purpose that is to compromise the integrity of the network they attack. In our paper we mainly focus on the security attacks and mechanisms in WSN. This paper summarizes the attacks and its classifications in WSNs and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The challenges of WSNs are briefly discussed above. This survey will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safety.

VIII. REFERENCES:

[1] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges**",** International conference on Advanced Computing Technologies**,** Page1043-1045, year 2006

[3] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328.

[4] D. C. Schleher, Electronic Warfare in the Information Age. Artech.

[5] D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile ad hoc and Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28, year 2005.

[6] D.Ganesan, R.Govindan, S.Shenker, and D.Estrin, "Highly resilient, energy efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review (MC2R), vol. 1, no. 2, 2002.

[7] F. Nait-Abdesselam, B. Bensaou, T. Taleb, "Detecting and avoiding wormhole attacks in wireless Ad hoc networks," IEEE Communication Magazine, Vol.46, Issue 4, pp. 127-133, April 2008.

[8] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004

[9] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year. 2002.

[10 John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006.

[11]Mohit Saxena, "Security In Wireless Sensor Networks - A Layer Based Classification", Cerias Tech Report 2007-04.

[12]S. Khan, K-k. Loo, T. Naeem, M.A. Khan, "Denial of service attacks and challenges in broadband wireless network," International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp.1-6, July 2008.

[13]Wang, B-T. and Schulzrinne, H., "An IP trace back mechanism for reflective DoS attacks", Canadian

Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904. ISSN : 0975-3397 1835

[14]Y.Wang, G.Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, year 2006.

[15]Y.Mun and C. Shin, "Secure routing in sensor networks: Security problem analysis and countermeasures," in International Conference on Computational Science and Its Applications - ICCSA 2005, May 9- 12 2005, vol. 3480 of Lecture Notes in Computer Science, (Singapore), pp. 459–467, Springer Verlag, Heidelberg, D-69121, Germany, 2005.

[16]Thomas Haenselmann (2006-04-05). Sensornetworks. GFDL Wireless Sensor Network textbook

AUTHOR

Dr. M. Hemalatha completed MCA MPhil., PhD in Computer Science and Currently working as a Asst Professor and Head, dept of software systems in Karpagam University. Ten years of Experience in teaching and published Twenty seven paper in International Journals and also presented seventy papers in various National conferences and one international conferences Area of research is Data mining, Software Engineering, bioinformatics, Neural Network. Also reviewer in several National and International journals

Vasanthi.V was born on 28th,Jan 1984. She received her Bachelor of Computer Application from Nirmala College for women in 2005 and Master degree in Computer science from Hindusthan college of Arts and Science in 2008. She completed her M.Phil from karpagam University in 2009. Currently pursuing Ph.D in computer science at Karpagam university under the guidance of Dr.M.Hemalatha Head, Dept of Software System, Karpagam university, Coimbatore. Area of Research is wireless sensor network.