An Overview on Protocol Stack Attacks in Wireless Sensor networks

Parvathy.K

Abstract— Wireless Sensor Network (WSN) is an emerging technology, comprising of distributed, autonomous tiny sensing devices named nodes. Wireless Sensor Networks are not single-handedly limited to military applications ,industrial and civilian application areas, industrial process monitoring and run, robot health monitoring, vibes and in flames monitoring, healthcare applications, home automation and traffic control. Nodes are deployed independently to monitor mammal or environmental conditions, such as temperature, hermetic, vibration, pressure, leisure seizure or pollutants parameters. Security is the major concern of a wireless sensor network .In this paper, a detailed classification of attacks in wireless sensor networks are discussed.

Index Terms—Wireless Sensor networks,Security Attacks,Protocol Attacks,OSI Model,Sensors,Confidentiality,Integrity and Authentication.

1 INTRODUCTION

The Wireless sensor network is most widely used in the various fields like medical applications, military applications, wildlife tracking, weather checking applications, traffic control applications. [7]WSNs are a particular type of ad hoc networks, comprised mainly of large number (hundred or thousand) deployed sensor nodes with limited resources and one or more base stations (BSs) or sink , typically serves as the access point for the user or as a gateway to another network. Nodes can collect and transmit (with wireless links) environmental data (temperature, pressure, humidity, noise levels, etc) in autonomous manner. The node in WSN plays two ways of methods : collecting the data and route the data returning to the base station.

Sensor nodes are used to detect enemy intrusion in battle field as well as they can be used to measure various environmental variables so in order to keep the information secret it is important to establish a secure communication between the sensor nodes.[3] The wireless sensor network consists of large number of tiny sensor nodes; each sensor node is equipped with integrated sensor, low battery powered and the main task of sensor node is sense, process the data and provide short range of communication. . sensor node consists of five components,: power unit (battery), memory, transmitter/receiver, embedded processor, and sensing unit.[2][5] Additional components can be implanted in a sensor node: location finding system: allow the node to find its position, a power generator: used for recharging battery node and prolong its lifetime, and a mobilizer: make nodes move .

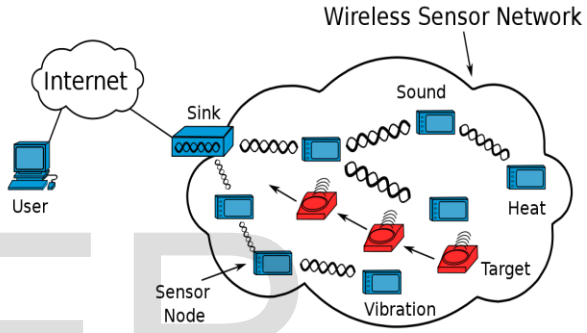

Fig.1 Wireless Sensor Networks

Sensing units are usually composed of two subunits: sensor and analogto- digital converter (ADC). When an event was produced (analog data) node sense analog signal observed convert it to digital signals by the ADC unit, and then treat it with the processing unit. A transceiver unit connects the node to the network. The number of sensor nodes in a sensor network can be several orders of magnitude on peak of the ad hoc network. Sensor nodes are densely deployed. Sensor nodes are prone to failures.[4]The topology of a sensor network changes every one
frequently.[9] Sensor nodes mainly use a puff communication paradigm, whereas most ad hoc networks are based visa--versa reduction-to narrowing communications. Sensor nodes are limited in expertise, computational capacities, and memory. Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.

2 SECURITY REQUIREMENTS OF WSN

Due to the lack of a wired communication medium, the limited resources of sensors, WSNs, deployed mostly in hostile environments with mission critical tasks, several security challenges are more complex than with other types of networks. security requirements for WSNs include the standard security metrics known as CIAA (Confidentiality, Integrity, Authentication and Availability) in addition to the security requirements specific to this type of network

- *Parvathy.K is currently working as Assistant Professor in Sri Ramakrishna Institute of Technology,Coimbatore,Tamilnadu, India,. E-mail: parvathy.cse@srit.org*

which aim to protect the information and resources from attacks and misbehaviour. In the following we illustrate the security properties and requirements we to establish a reliable communication in WSNs and to provide secure services. Confidentiality: This is the most important issue in network security which guards data from eavesdroppers. It ensures that a given message remains hidden and cannot be used by anyone other than the desired receiver. Integrity: Data integrity is needed to ensure the reliability of data parquets. Authentication: all applications require data authentication which ensures the reliability of the message by giving the ability of each communication host to identify its origin and to verify the other's identity to counter to packet injection or spoofing and to all malicious routing information. Availability: Availability affects several sides in the sensor network.

3. ATTACKS ON PROTOCOLSTACK IN WSN

3.1 OSI Model

The role of this model (Opening System Interconnect) consists in standardizing the communication between the participants so that various manufacturers can develop compatible products (software or hardware).

Each layer of the model communicates with an adjacent layer (that of the top or that of the lower part). Each layer uses the services of the sub-bases and provides some to that of higher level.

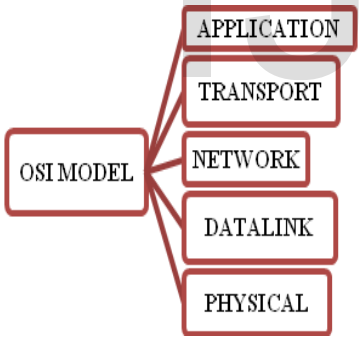

Fig.2 OSI Model

WSNs are vulnerable to various types of attacks. These attacks are of different mechanisms, techniques and goals which makes necessary to find and adopt a well-defined taxonomy in order to facilitate design and development of WSNs for researchers and protocol programmers.

3.2 ATTACKS IN PROTOCOL STACK

The protocol stack used by nodes in a wireless sensor network consists of the Physical Layer, Data Link Layer, Network Layer, Transport Layer, and Application. It ensures the energy efficiency in the network, manages the use of the wireless medium with the routing task and facilitates synchronization and cooperative efforts between sensor nodes. [8]Each level on the protocol stack takes on a set of tasks and guarantees a set of services. Therefore, it will be targeted by several attacks. Physical Layer: This layer ensures the data transmission services which encompass the selection of access channels, radiofrequency regulation and deflection, signal processing and data encryption to increase the communications reliability. [10]Data Link Layer: This layer is responsible of physical addressing, error detection and/or correction, data streams multiplexing, medium access and flow control as well as ensuring reliable point-to-point and point to- multipoint connections in the network. Network Layer: This layer is in charge of routing the data supplied by its upper layer. It is very important task encompasses packets routing and forwarding, addresses assignment and energy management.[9] Transport Layer: The transport layer ensures the management of end-to-end reliable delivery of packets connections and the establishment of end-to-end connection in addition to flow and congestion control. [11]Application Layer: This layer contains user applications which oversee the sensing tasks. It manipulates user data with a set of application protocols, and it is a target of attacks aiming at affecting the synchronization of communications and data confidentiality.

The physical layer[12] is the lowest layer in the protocol stack for WSN. The responsibilities of the Physical Layer are frequency selection, carrier frequency generation, signal detection, modulation, and encryption. Its main priority is energy minimization and secondary concerns are the same as those of other wireless networks.

The various types of attacks possible are jamming, tampering and Sybil. Most wireless communications use the RF spectrum as a broadcast medium. These messages can be easily intercepted by the intruders and modified or new messages created and injected into the network.[13] **Radio signals** can be **jammed** or **interfered**, which causes the message to be corrupted or lost. The most common types of attacks in in physical layer in WSN are jamming attacks. **Jamming** interrupts the network if a single frequency is used throughout. It also causes excessive energy consumption by addition of infected packets. Examples of jamming attacks include sinkhole and wormhole attack. [15] four different type of jamming attack that can be used by an attacker to stop the operation of a wireless network. How each model effects on the sending and receiving capability of a wireless node and its impressiveness was evaluated. [7][8]**Tampering** is another attack on physical layer. In this attack, nodes are vulnerable to tampering or physical harm. In case of a **Sybil attack**, a single node duplicates itself and presented in the multiple locations. [14]The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network [15].

The responsibilities of the Data Link Layer are the multiplexing of data streams, data frame detection, medium access and error control. [11]A wireless sensor network must have a specialized MAC

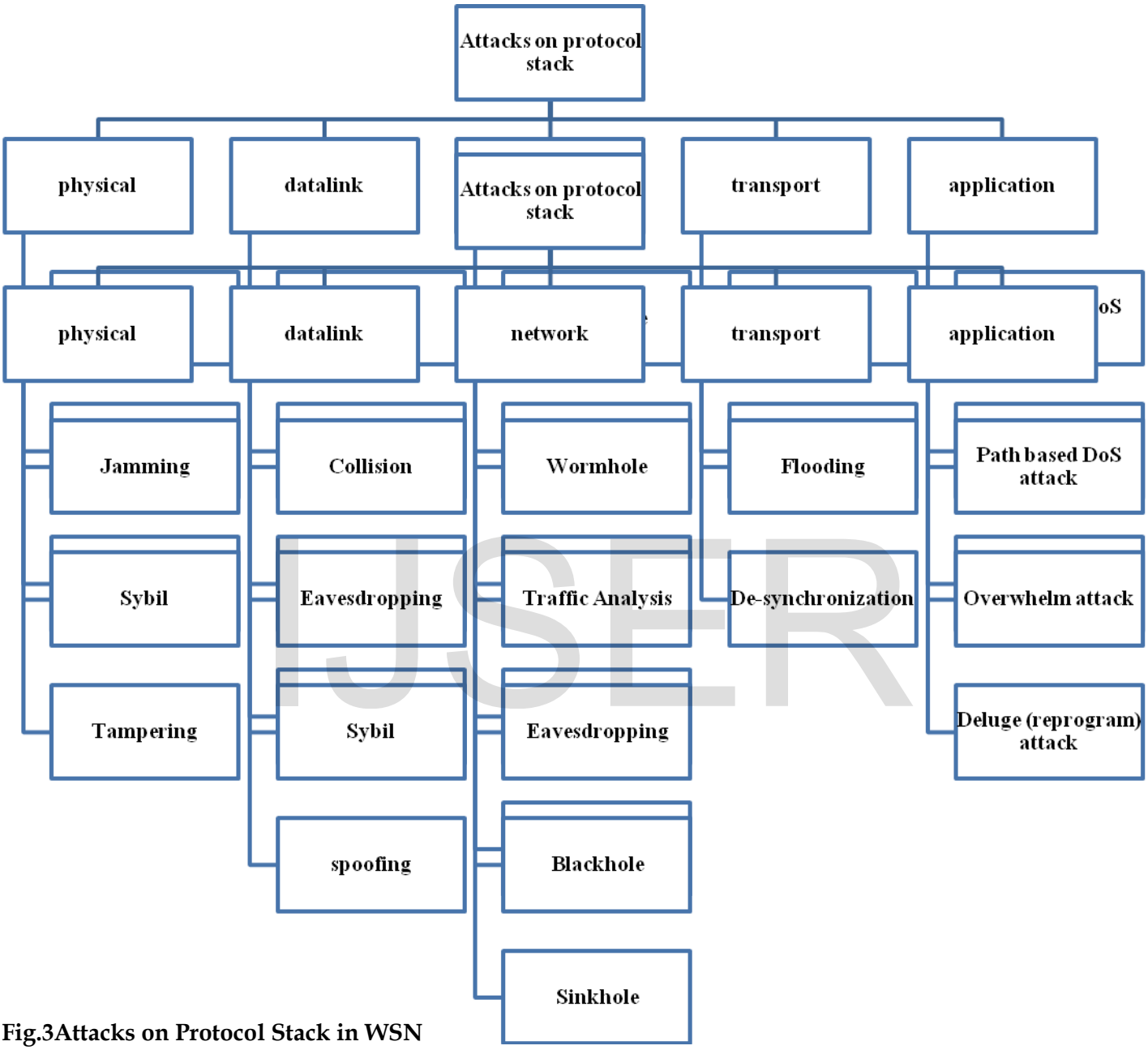

Fig.3Attacks on Protocol Stack in WSN

protocol to address the issues of power conservation and data-centric routing.

Some of the MAC protocols are sensor-MAC (SMAC), Etiquette Protocol, and CSMA for Sensor Networks. [14] Attacks can also be made on the link layer. The various types of the possible attacks here are eavesdropping, Sybil, spoofing, collision. An attacker may violate the communication protocol causing de-synchronization, and continuously send messages in an attempt to cause collisions. An attacker may consume easily a sensor node's power supply by forcing oversupply retransmissions and thus cause exhaustion of the battery power. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. [17] In case of Eavesdropping, the adversary (eavesdropper) aims to determine the aggregate data that is being output by the sensor network: it is attempting to see what the system is observing, e.g., to predict how the owner of the sensor network will react. [16] By spoofing routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc. The network layer [14] in a WSN must be designed with the following considerations in mind: power efficiency, WSNs are data-centric networks, and WSNs have attribute-based addressing and location awareness. The Link layer handles how two nodes talk to each other, the network layer is responsible for deciding which node to talk to. Network layer is susceptible to various attacks. These may include eavesdropping, DoS, Selective forwarding, Sybil, Traffic analysis, wormhole, sinkhole, hello flood, node capture, black hole, spoofing, acknowledgment spoofing, misdirection, internet smurf attack and homing.

Out of these attacks, eavesdropping, spoofing, Sybil and Traffic analysis have already been explained in the attacks on Data link layer section.[12] A **sinkhole attack** tries to lure almost all the traffic toward the compromised node, creating a metaphorical sinkhole with the adversary at the center. Also if an attacker captures a single node, it is sufficient for him to get hold of the entire network. Malicious or attacking nodes can however refuse to route certain messages and drop them. If they drop all the packets through them, then it is called a **Black Hole Attack**. In the **Wormhole Attacks**, an adversary can tunnel messages received in one part of the network over a low latency link and replay them in another part of the network. This is usually done with the coordination of two adversary nodes, where the nodes try to understate their distance from each other, by broadcasting packets along an out-of-bound channel available only to the attacker. **Spoofed, Altered, or Replayed Routing Information** is the most direct attack against a routing protocol in any network is to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network. These disruptions include the creation of routing loops, attracting or repelling network traffic from select nodes, extending and shortening source routes, generating fake error messages, partitioning the network, and increasing end-to-end latency. An attacking node can spoof the Acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes. The transport layer comes into play when the system needs to communicate with the outside world. Communication from the sink to the user is a problem because the Wireless Sensor Network is not based on global addressing and attribute-based naming is used to indicate the destinations of DATA packets. The Transport layer is also vulnerable to some attacks as Flooding attack and de-synchronization attack. [14]In case of **Flooding**, many connection requests are sent until the resources required by each connection are exhausted or reach a maximum limit. Eventually the node's resources are exhausted and render it useless. In the **de-synchronization attack**, the attacker repeatedly forges the messages to one or both end points which request transmission of missed frames. Hence, these messages are again transmitted and if the attacker maintains a proper timing, it can prevent the end points from exchanging any useful information. This is the topmost layer of the sensor network protocol stack. A Sensor Management Protocol, SMP, [14] at the application layer is used to make the hardware and software of lower layers transparent to the Sensor Network Management Applications. The system administrators and programmers with interact with the Sensor Network using SMP. Again the lack of global identification and infrastructure less nature of sensor networks must be taken into consideration.

Three types of attacks are common on this layer. These include: path based DoS, Overwhelm attack, Deluge or reprogram attack. [15]The **path based DoS attack** involves sending extra or replayed packets into the network on the leaf nodes. This occupies the resources of the entire network and starves the legitimate traffic. In **Overwhelm attack**, an attacker might attempt to overwhelm network nodes with sensor stimuli, causing the network to forward large volumes of traffic to a base station. This attack also consumes network bandwidth and drains node energy. [9]The third attack is **Deluge (reprogram) attack** where [13] Network programming system lets you remotely reprogram nodes in deployed networks.

4 Conclusion

This paper gives an overview of the general concept of wireless sensor networks and its attacks. WSNs play a major role in unattended areas, especially mission critical areas like Military, Health and in other civilian applications, In highly unattended areas, WSNs become vulnerable. Security is an important feature for deploying the sensors. This paper summarizes various security attacks and their countermeasures especially in protocol stack.

References

[1] "21 ideas for the 21st century," Business Week, pp. 78-167, Aug.39, 1999.

[2] H. Karl and A. Willig, "Protocols and Architectures for Wireless Sensor Networks", John Wiley and Sons Ltd, the Atrium, Southern Gate, Chichester, West Sussex, England, 2005.

[3] D. Culler, D. Estrin, and M. Srivastava, "Overview of Sensor Networks", *IEEE Computer*, August 2004.

[4] K. Martinez, J. K. Hart, and R. Ong, "Environmental sensor networks", *IEEE Computer Journal*, Vol. 37 (8), 50-56, August 2004.

[5] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk , and J. Anderson, "Wireless sensor networks for habitat monitoring", Proceedings of the 1st ACM International workshop on Wireless sensor networks and applications, Atlanta, Georgia, USA, 88-97, 2002.

[6] http://en.wikipedia.org/wiki/Sensor_Networks

[7] Akyildiz, I.F., W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, August, 102-114(2002).

[8] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh , "Overview of Security Issues in Wireless Sensor Networks" , 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, , © 2011 IEEE

[9] Dirk Westhoff, Joao Girao, Amardeo Sarma , "Security Solutions for Wireless Sensor Networks"

[10] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, "A Security, Privacy and Trust Architecture for Wireless Sensor Networks", 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia

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

[12]. Mike Horton and John Suh , A Vision for Wireless Sensor Networks , 2005 IEEE

[13]. Jaydip Sen , A Survey on Wireless Sensor Network Security, Vol. 1, No. 2, August 2009, International Journal of Communication Networks and Information Security (IJCNIS)

[14]. T.Kavitha, D.Sridharan Security Vulnerabilities In Wireless Sensor Networks: A Survey, Journal of Information Assurance and Security 5 (2010) 031-044

[15]. Norman Dziengel, Nicolai Schmittberger, Jochen Schiller, Mesut G• unes, Secure Communications for Event-Driven Wireless Sensor Networks, Department of Mathematics and Computer Science Freie Universit• at Berlin Takustr. 9, 14195 Berlin, German