ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks

Dr. Banta Singh Jangra, Vijeta Kumawat

Abstract*—WSN (Wireless Sensor networks) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring, environmental control, surveillance tasks, monitoring, tracking etc. All these severe constraints and demanding deployment environments of WSN make security for these systems more challenging than for conventional networks. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. In this paper starting with a brief overview of the sensor networks, a review is made of and how to provide the security on the wireless sensor networks. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks.

***Index Terms*— Wireless Sensor Network, Security Attacks, Defensive Mechanisms, Challenges, Holistic.**

I. INTRODUCTION

Wireless Sensor Network(WSN) are a most challenging and emerging technology for the research due to their low processing power and associated low energy. The sensor network is a group of self- organized, low priced sensor nodes and creates network in spontaneous manner. The WSN combines sensing, computation and communication in a single small device, called Sensor Node. It mainly contains battery, radio, microcontroller and power devices. The sensors in a node provides the facility to get the data like temperature, pressure, light, motion, sound etc and capable of doing data processing. The main goal of the applications is achieved by the cooperation of all sensor nodes in the network. There are many sensor network applications like security monitoring, environmental data collection, medical science, military, tracking etc. Security becomes extremely important factor when sensor networks are randomly deployed in a hostile environment.

Even through wireless sensor network is an advanced technology of network, it is extremely different from traditional wireless networks. This is, due to the unique characteristics of sensor nodes in WSN. So existing security mechanisms of traditional wireless networks are not directly applied in WSN. Sensor networks are closely interacting with physical environment. So sensor nodes are also deployed in all areas even physical accessible attacks and broadcasting sensed data in network. These reasons give a scope to new security mechanism rather than applying existing traditional security mechanisms in WSN. The traditional security mechanisms are authentication, symmetric key encryption & decryption and Public Key Infrastructure (PKI) cryptography [3], [2], [1]. The major challenge is to deploy the above encryption techniques or their counterparts in a sensor network which is characterized with constrained memory, power supply and processing capability [4]. In this paper, we discuss the most common security services for WSN. The paper is structured as follows. Section-II

II. SECURITY GOAL FOR SENSOR NETWORK

A sensor network is a special type of Ad hoc network. So it shares some common property as computer network. There are usually several security requirements to protect a network [5]. These requirements should be considered during design of a security protocol, including confidentiality, integrity, and authenticity. An effective security protocol should provide services to meet these requirements. The security requirements [9], [6], [7], [8], [5], [10] of a wireless sensor network can be classified as follows:

A. Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following: A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive. In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network. Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

B. Data Integrity

Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. The integrity of the network will be in trouble when:

- A malicious node present in the network injects false data.
- Unstable conditions due to wireless channel cause damage or loss of data. [11]

C. Data Authentication

Authentication ensures the reliability of the message by identifying its origin. An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

D. Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

E. Data Availability

Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate. However, failure of the base station or cluster leader's availability will eventually threaten the entire sensor network. Thus availability is of primary importance for maintaining an operational network.

III. COMMUNICATION PROTOCOL

Wireless sensor networks use layered architecture like wired network architecture. Characteristics and functions of their each layer are given below.

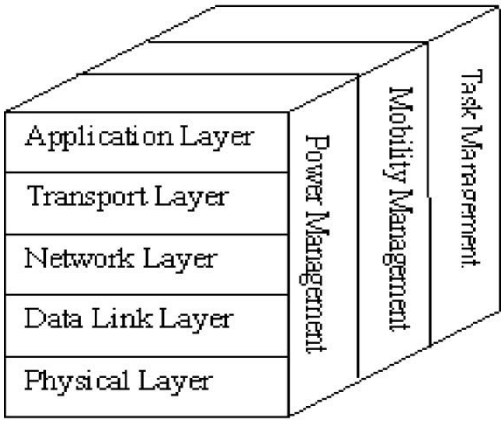

Fig 1: Layered Architecture of WSN

1) Physical Layer

The objective of physical layer is to increase the reliability by reducing path loss effect and shadowing. This layer is responsible for established connection, data rate, modulation, data encryption, signal detection, frequency generation and signal detection.

2) Data Link Layer

The objective of Data link layer is to insure interoperability amongst communication between nodes to nodes. This layer is responsible for error detection, multiplexing. Prevention of Collision of packets, repeated transmission etc.

3) Network Layer

The objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa. The LEACH and PEGASIS are the protocols which describe the techniques to save the energy consumption (power of sensor) so as to improve the life of sensors. LEACH gives cluster based transmission while PEGASIS is chain protocol [12, 13, and 14].

4) Transport Layer

The objective of Transport Layer is to establish communication for external networks i.e. sensor network connected to the internet. This is most challenging issue in wireless sensor networks.

5) Application Layer

The objective of Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results. SPINS (Security Protocols in sensor Networks) [15] provides data authentication, replay protection, semantic security and low overhead. SPIN has two secure building blocks SNEP and µTESLA. SNEP provides baseline security primitives: Data Confidentiality, two party data authentication and data freshness. µTESLA provides authentication broadcast for severely resource constrained environments. Localized Encryption and Authentication Protocol (LEAP) [16] is a key management protocol for sensor networks. It provides multiple keying mechanisms (Group Key, Cluster Key, and Pair wise Shared Key) in this regard. By data Aggregation we can optimize data, network's traffic load etc. Existing protocols described above are summarized in table 1 below in Appendix;

IV. SECURITY THREATS AND ATTACKS IN WSN

A. Security Threats

A threat is a circumstance or event with the potential to adversely impact a system through a security breach and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as risk. The categories of the threats could be (a) Passive Information Gathering, (b) Subversion of node or Insertion of a false node, (c) node malfunction, (d) node outage, (e) message corruption, (f) denial of service, or (g) traffic analysis. Threats in wireless sensor network can be classified into the following categories:

1. External versus internal attacks:

The external attacks are from nodes which do not belong to a WSN. An external attacker has no access to most cryptographic materials in sensor network. The internal

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. The inside attacker may have partial key material and the trust of other sensor nodes. Inside attacks are much harder to detect. External attacks may cause passive eavesdropping on data transmissions, as well as can extend to injecting bogus data into the network to consume network resources and raise Denial of Service (DoS) attack. Whereas inside attacker or internal threat is an authorized participant in the sensor network which has gone hostile. Insider attacks may be mounted by either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes and who then use one or more laptop-class devices to attack the network.

2.. Mote-class versus laptop-class attacks:

In mote class (sensor-class) attacks, an adversary attacks a WSN by using a few nodes with similar capabilities as that of network nodes. In laptop-class attacks, an adversary can use more powerful devices like laptop, etc. and can do much more harm to a network than a malicious sensor node. These types of attackers can jam the radio link in its immediate vicinity. An attacker with laptop-class devices have greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna and hence they can affect much more than an attacker with only ordinary sensor nodes. A single laptop-class attacker might be able to eavesdrop on an entire network.

3. Passive versus active attacks:

Passive attacks are in the nature of eavesdropping on, or monitoring of packets exchanged within a WSN. The active attacks involve some modifications of the data steam or the creation of a false stream in a WSN.

B. Security Attacks

An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. The attacks which act on the network layer are called routing attacks. Wireless networks are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. These attacks are normally due to one or more vulnerabilities at the various layers in the network. The following are the attacks that happen while routing the messages.

1) Denial of Service

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. 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. In this attack the attacker gets illegally multiple identities on one node. By this, the attacker mostly affects the routing mechanism. Sybil attacks are generally prevented by validation techniques.

2) Black hole/ Sinkhole Attack:

In this attack, attacker places himself in a network with high capability resources (high processing power and high band width) by which it always creates shortest path. As a result, all data passes through attacker's node. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations. Fig 2 shows the conceptual view of a black hole/sinkhole attack.

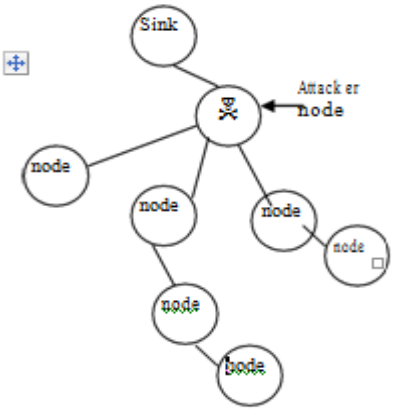

Fig 2: Black hole/Sinkhole Attack

3) Sybil Attack

Generally, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attacks are generally prevented by validation technique.

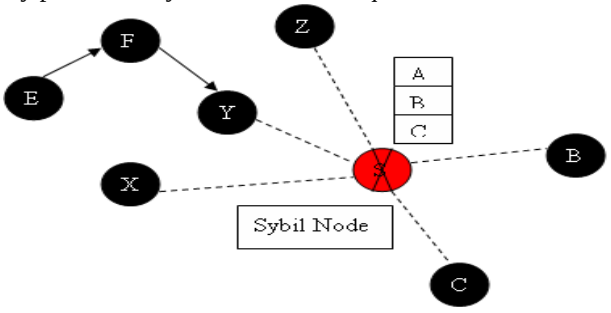

Fig 3: Sybil Attack

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

4) 'Hello flood' Attack

It is one of the simplest attacks in wireless sensor networks in which attacker broadcasts HELLO packets with high radio 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. By this attack congestion occurs in the network. This is a specific type of DOS. Blocking techniques are used to prevent Hello Flood attacks.

5) Wormhole Attack

Wormhole attack [17], [18] is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Fig 4 shows mechanism of wormhole attack let node X broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node X, and will mark this node as its parent. Hence, even if the victim nodes are multihop apart from X, attacker in this case convinces them that X is only a single hop away from them, thus creates a wormhole.

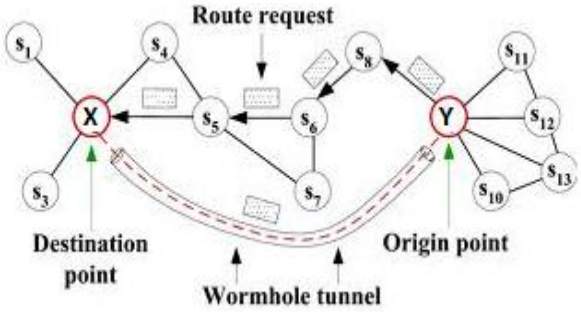

Fig 4: Worm hole Attack

Wormhole attack is a significant threat to wireless sensor networks, because this type 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 the neighboring information.

V. RELATED WORKS AND SECURITY SOLUTIONS IN WSN

In this section, we review some of the popular security solutions and combat some of the threats to the sensor networks.

A. SPINS

SPINs has two security building blocks: (a) Sensor Network Encryption Protocol (SNEP) and µTESLA. SNEP provides data confidentiality, two-party data authentication, integrity, and freshness. µTESLA provides authentication for data broadcast. We bootstrap the security for both mechanisms with a shared secret key between each node and the base station .SNEP uses encryption to achieve confidentiality and message authentication code (MAC) to achieve two-party authentication and data integrity.

SNEP provides a number of unique advantages. First, it has low communication overhead since it only adds 8 bytes per message. Second, like many cryptographic protocols it uses a counter, but we avoid transmitting the counter value by keeping state at both end points. Third, SNEP achieves even semantic security, a strong security property which prevents eavesdroppers from inferring the message content from the encrypted message. Finally, the same simple and efficient Protocol also gives us data authentication, replay protection, and weak message freshness. SNEP offers the following nice properties:

1. Data authentication: If the MAC verifies correctly, a receiver can be assured that the message originated from the claimed sender.

2. Semantic security: Since the counter value is incremented after each message, the same message is encrypted differently each time. The counter value is long enough that it never repeats within the lifetime of the node.

3. Replay protection: The counter value in the MAC prevents replaying old messages. Note that if the counter were not present in the MAC, an adversary could easily replay messages.

4. Weak freshness: If the message verified correctly, a receiver knows that the message must have been sent after the previous message it received correctly (that had a lower counter value). This enforces a message ordering and yields weak freshness.

5. Low communication overhead: The counter state is kept at each end point and does not need to be sent in each message. µTesla is a new protocol which provides authenticated broadcast for severely resource-constrained environments. In a broadcast medium such as sensor network, asymmetric digital signatures are impractical for the authentication, as they require long signatures with high communication overhead. µTesla protocols provide efficient authenticated broadcast [19], [20] and achieves asymmetric cryptography by delaying the disclosure of the symmetric keys. µTesla constructs authenticated broadcast from symmetric primitives, but introduces asymmetry with delayed key disclosure and one-way function key chains. µTESLA solves the following inadequacies of TESLA in sensor networks:

- TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. µTESLA uses only symmetric mechanisms.
- Disclosing a key in each packet requires too much energy for sending and receiving. µTESLA discloses the key once per epoch.
- It is expensive to store a one-way key chain in a sensor node. µTESLA restricts the number of authenticated senders.

B. TINYSEC

It provides similar services, including authentication, message integrity, confidentiality and replay protection. A major difference between TinySec and SNEP is that there are no counters used in TinySec. For encryption, it uses CBC mode with cipher text stealing and for authentication, CBC-MAC is used. There are two packet formats defined by TinySec. These are TinySec-Auth, for authenticated messages, and TinySec-AE, for authenticated and encrypted messages. For the TinySec-AE packet, a payload of up to 29 Bytes is specified, with a packet header of 8 Bytes in length.TinySec uses cipher block chaining (CBC) mode and

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

encrypts the data payload and authenticates the packet with a MAC. Encryption of the payload is all that is necessary, but the MAC is computed over the payload and the header. The TinySec- Auth packet can carry up to 29 Bytes of payload. The MAC is computed over the payload and the packet header, which is 4 Bytes long.

C. Localized Encryption and Authentication Protocol (LEAP)

LEAP is a key management protocol for sensor networks designed to support in- network processing, while restricting the impact of a compromised node to the network. Design of the LEAP protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements. LEAP has the following properties:

- LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. The protocol used for establishing and updating these keys is communication and energy efficient, and minimizes the involvement of the base station.
- LEAP includes an efficient protocol for inter-node local broadcast authentication based on the use of one-way key chains.
- Key sharing approach of LEAP supports source authentication without precluding in-network processing and passive participation. It restricts the security impact of a node compromise to the immediate networneighborhood of the compromised node.

VI. CONCLUSION

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks. The challenges of Wireless Sensor Networks are also briefly discussed. This survey will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

REFERENCES

[1] Woo Kwon Koo, Hwaseong Lee, Yong Ho kim, Dong Hoon Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks", International Conference on Information Security and Assurance,2008.

[2] Al-Sakib Khan Pathan, hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Feb 20-22, 2006 ICACT2006.

[3] Xiao Chen, Jawad Drissi, "An Efficient Key Management Scheme in Hierarchical Sensor Networks", IEEE MASS 2005 Workshop-WSN05.

[4] Jan Steffan, Ludger Fiege, Mariano Cilia Alejandro Buchman," Scoping in Wireless Sensor Network", 2nd workshop on middleware for pervasive and Ad-Hoc Computing Toronto, Canada, 2004 ACM 1-58113-951-9.

[5] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEE, 2009.

[6] E. Yoneki and J. Bacon, "A survey of Wireless sensor Network technologies: research trends and middleware's role", Technical Report, 2005.http://www.cl.cam.ac.uk/TechReport, ISSN 1476-2986.

[7] J.P.Walters, Z.Liang, W.Shi, and V. Chaudhary, "Wireless Sensor Network Security-a survey", Security in Distributed, Grid, Mobile, and pervasive Computing, Auerbach Publication, CRC Press, 2007.

[8] L.L. Fernandes,"Introduction to Wireless Sensor Networks Report", University of Trento.2007,

[9] A. T. Zia, "A Security Framework for Wireless Sensor Networks".2008,

[10] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey" Journal of Theoretical and Applied Information Technology, 2010, PP. 14-27.

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

[12] Cauligi S. Raghavendra,"PEGASIS: Power- Efficient Gathering in sensor Information System", 2002 IEEE Aerospace Conference Proceeding – Volume 3, Big Sky, MT; UNITED STATES; 9-16 Mar. 2002 pp. 3-1125 to 3-1130. 2002.

[13] Siva D. Muruganathan, Daniel C.F. MA,Rolly I. Bhasin, Abraham O. Fapojuwo," A Centralized Energy- Efficient Routing Protocol for Wireless Sensor Network", IEEE Communications Magazine. Vol. 43, no. 3, pp. S8-13. Mar. 2005.

[14] Christian Herman and Waltenegus dargie,"Senceive: A Middleware for a Wireless Sensor Network", 22nd international Conference on Advanced Information Networking and Applications, 2008.

[15] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen, "SPINS: Security Protocols for Sensor Networks", Department of Electrical Engineering and Computer Sciences, University of California, Berkly, 2002.

[16] Sencun Zhu, Sanjeev Setia, Sushil Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Network", Aug. 2004, publish in ACM.

[17] Y.C. Hu, A. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03), vol. 3, San Francisco, CA, Mar. 2003, pp. 1976-1986 .

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 3, September 2012

[18] Y.C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[19] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar, "Efficient and secure source authentication for multicast", In Network and Distributed System Security Symposium, NDSS 01, February 2001.

[20] Adrian Perrig, Ran Canetti, J.D. ygar, and Dawn Song, "Efficient authentication and signing of multicast streams over lossy channels" In IEEE Symposium on Security and Privacy, May 2000.

[21] Abhishek Pandey and R.C. Tripathi, "A Survey on Wireless Sensor Networks Security" in International Journal of Computer Applications (0975-8887).

WSN Layer	**Types of attacks**	**Existing protocols**
Physical Layer	Denial of service attack	
Data Link Layer	Denial of service attack	Link Layer security protocol (TinySec, PEGASIS, LEACH)
Network Layer	Denial of service attack, Wormholes, Sinkholes, Sybil attacks.	Routing protocols (ID based, data-centric)
Transport Layer	Denial of service attack	
Application Layer	Malicious Node	Aggregation scheme

Table 1: summery of WSN layers, possible attacks on them and the existing protocols.