International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 2 (March-April, 2016), PP. 78-84

A REVIEW ON SECUIRTY ISSUES ON WIRELESS SENSOR NETWORK

Roshni Kapoor[1], Ashutosh Rastogi[2]
Dept. of Electronics & Communication
Babu Banarasi Das University
Lucknow, Uttar Pradesh
[1]Kapoor.roshni1993@gmail.com
[2]ashutoshrastogi1984@gmail.com

***Abstract*— Wireless Sensor Network (WSN) are spatially distributed sensor nodes to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. Wireless Sensor Networks are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. In this article we present a survey of security issues in WSNs. First we outline the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs. We then present a holistic view of security issues. These issues are classified into two categories: cryptography and secure routing. Along the way we highlight the advantages and disadvantages of various WSN security protocols and conclude with possible future research on security inWSNs.**

Keywords— Data Confidentiality, Sinkhole attack, Sybil Attack and Flooding Attack.

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, vibration, pressure, humidity, motion or pollutants and to cooperatively pass their data through the network to a main location A sensor node might vary in size from that of a shoebox down to the size of a grain of dust. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attacks. Security is a common concern for any network system, but security in Wireless Sensor Network is of great importance to ensure its application success. For example, when sensor network is used for military purpose, it is very important to keep the sensed information confidential and authentic [1] Providing security for WSN represents a rich field of research problems as many existing security schemes for traditional networks are not applicable for WSN. Moreover, analysis of security requirements gives right directions to develop or implement the proper safeguards against the security violations[2].

A security scheme in WSNs must provide efficient key distribution while maintaining the ability for communication between all relevant nodes. In addition to key distribution, secure routing protocols must be considered. These protocols are concerned with how a node sends messages to other nodes or a base station. A key challenge is that of authenticated broadcast [3,4] Existing authenticated broadcast methods often rely on public key cryptography and include high computational overhead making them infeasible in WSNs. Secure routing protocols proposed for use in WSNs, such as SPINS [5], must consider these factors. Additionally, the constraint on energy in WSNs leads to the desire for data aggregation. This aggregation of sensor data needs to be secure in order to ensure information integrity and confidentiality [6, 7]. In Section 2 we discusses about the types of security , In Section 3 we focuses on the security issues that arise in WSN because of its resource restriction ,In Section 4 essential requirements for ensuring WSN security, In Section 5 briefly describes some attacks at different layers and some proposed countermeasures ,In Section 6 discusses about the defensive measures of WSN directing two important security aspects which are cryptography and key management and In Section 7 we discuss about the communication protocols.

II. TYPES OF SECUIRTY

A. Low Level of Mechanism

The sensor networks is secured through Low-level Security primitives which includes

- Key establishment and trust setup
- Secrecy and authentication
- Privacy
- Robustness to communication denial of service
- Secure routing
- Resilience to node capture

B. Key establishment and trust setup

The establishment of cryptographic keys is the primary requirement for setting up the sensor network. The computational power of the sensor devices is limited Following the public key cryptographic primitives is too Expensive. In Key establishment techniques, there is a need to scale to networks with hundreds or thousands of nodes. The communication patterns of sensor networks differ from the traditional networks. Here the sensor nodes set up keys not only with their neighbors and also with data aggregation nodes.

C. Privacy

The sensor networks have force privacy concerns like other traditional networks. The sensor networks are deployed initially for legitimate purpose may be later used in unanticipated ways. Hence it is important to provide awareness about the presence of sensor nodes and data acquisition.

D. Robustness to communication denial of service

After an adversary attempts to disrupt the network's operation by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed. More sophisticated attacks are also possible; the adversary might inhibit Communication by violating the 802.11 medium access control (MAC) protocol by, say, transmitting while a neighbor is also transmitting or by continuously requesting channel access with a request-to send signal.

E. Secure Routing

The crucial service to enable communication in sensor networks is routing and data forwarding. Many security vulnerabilities are present in the current routing protocols. For example, denial of- service attacks can be launched on the routing protocol for preventing communication by the attackers. The injection of malicious routing information into the network is one of the simplest attacks which results in routing inconsistencies. Simple authentication is used for protection against injection attacks. Here some routing protocols are susceptible to replay by the attacker of legitimate routing messages.

F. Resilience to node capture

Resiliency against node capture attacks is one of the most challenging issues in sensor networks. The sensor nodes are placed in locations easily accessible to attackers in most applications. Hence there is possibility for the attackers to capture sensor nodes, extract cryptographic secrets, modify their programming, or replace them with malicious nodes under the control of the attacker.

III. SECUIRTY ISSUES

A. Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

B. Memory and Storage Space Constraints

A sensor is a tiny device with only a small amount of memory and stage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

C. Power Limitation

Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor (i.e., its battery life). The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead (e.g., initialization vectors needed for encryption/decryption), and the energy required to store security parameters in a secure manner (e.g., cryptographic key storage).

B. Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

C. Unreliable Transfer

Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling. More importantly, if the protocol lacks the appropriate error handling it is possible to lose critical security packets. This may include, for example, a cryptographic key.

D. Conflicts

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem [8].

IV. SECURITY REQUIREMENTS

Wireless Sensor Network is vulnerable to various attacks like any other conventional network, but its limited resource characteristics and unique application features requires some extra security requirements including the typical network requirements. The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include:

A. Authenticity and integrity

Only providing data confidentiality is not enough to ensure the data security in WSN. As an adversary can change messages on communication or inject malicious message, authentication of data as well as sender are also crucial security requirements. Source authentication provides the truthfulness of originality of the sender. Whereas, data authentication ensures the receiver that the data has not been modified during the transmission.

B. Data Confidentiality

Data confidentiality is one of the vital security requirements for WSN because of its application purpose (for example, military and key distribution applications Sensor nodes communicate sensitive data, so it is necessary to ensure that any intruder or other neighboring network could not get confidential information intercepting the transmissions. One standard security method of providing data confidentiality is to encrypt data and use of shared key so that only intended receivers can get the sensitive data. Section 5 discusses more on this cryptography issues for WSN. Data Confidentiality is whether the information stored on a system is protected against unintended or unauthorized access.

C. Availability

We cannot ignore the importance of availability of nodes when they are needed. For example, when WSN is used for monitoring purpose in manufacturing system, unavailability of nodes may fail to detect possible accidents. Availability ensures that sensor nodes are active in the network to fulfil the functionality of the network. It should be ensured that security mechanisms imposed for data confidentiality and authentication are allowing the authorized nodes to participate in the processing of data or communication when their services are needed. As sensor nodes have limited battery power, unnecessary computations may exhaust them before their normal lifetime and make them unavailable. Sometimes, deployed security protocols or mechanisms in WSN are exploited by the adversaries to exhaust the sensor nodes by its resources and makes them unavailable for the network. So, security policies should be implied so that sensor nodes do not do extra computation or do not try to allocate extra resources for security purpose.

D. Nonrepudiation

This denotes that a node cannot deny sending a message it has previously sent. Non- repudiation is the assurance that someone cannot deny something. It refers to the ability to ensure that a node to a contract or a communication cannot deny the authenticity of their signature on a message that they originated.

E. Freshness

Data Freshness implies that the data is recent and ensures that no adversary can replay old messages. This prevents the adversaries from confusing the network by replaying the captured messages exchanged between sensor nodes. To achieve freshness, security protocols must be designed in such a way that they can identify duplicate packets and discard them preventing replay attack Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy should also be considered.

• Forward secrecy: a sensor should not be able to read any future messages after it leaves the network.

• Backward secrecy: a joining sensor should not be able to read any previously transmitted message.

V. SECUIRTY ATTACKS

WSNs are vulnerable to various types of attacks. According to the security requirements in WSNs, these attacks can be categorized:

• Attacks on secrecy and authentication: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

• Attacks on network availability: attacks on availability are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.

For securing the Wireless Sensor Networks, it is necessary to address the attacks and then take counter measures at the design time of WSN. This section lists and gives brief discussion about the major attacks against Wireless Sensor Network.

A. Physical Attack

This attack is also known as node capture. In this type of attack, attackers gain full control over some sensor nodes through direct physical access [11]. As the cost of sensor nodes must be kept as Cheap as possible for WSN, sensor nodes with tamper proofing features are impractical. This is why sensor nodes are susceptible to be physically being accessed. Physical attacks have significant impacts on routing and access control mechanisms of WSN. For example, getting key information stored on sensor node's memory gives attacker the opportunity of unrestricted access to WSN.

For performing physical attack an adversary may require expert knowledge, costly equipment's and other resources. Also, most of the time physical attack requires the victim node to be removed from the deployment area for a certain amount of time.

B. Attacks at Different Layer

Besides physical attack, adversaries perform a large number of attacks remotely. These attacks take place affecting different networking layers of WSN. This subsection describes some of these well-known attacks

1) Physical Layer

Physical layer is responsible for actual data transmission and reception, frequency selection, carrier frequency generation, signaling function and data encryption. [9]This layer also addresses the transmission media among the communicating nodes. WSN uses shared and radio based transmission medium which makes it susceptible to jamming or radio interference.

1.1) Jamming

In physical layer, jamming is a common attack that can be easily done by adversaries by only knowing the wireless transmission frequency used in the WSN. [10] Says the attacker transmits radio signal randomly with the same frequency as the sensor nodes are sending signals for communication. This radio signal interferes with other signal sent by a sensor node and the receivers within the range of the attacker cannot receive any message.

2) Link Layer

The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error control. This layer is vulnerable to data collision when more than one sender tries to send data on a single transmission channel.

2.1) DoS Attack by Collision Generation

In link year, collision is generated to exhaust the sensor node's energy. In order to generate collision, the attacker listens to the transmissions in WSN. When he finds out the starting of a message, he sends his own radio signal for a small amount of time to interfere with the message [11] which causes CRC error at the receiving end. Because of this attack, the receivers cannot receive the message correctly.

3) Network Layer

Network layer is responsible for routing messages from one to another node which are neighbors or may be multi hops away for example, node to base station or node to cluster leader. The network layer for WSN is usually designed considering the power efficiency and data centric characteristics of WSN. There are several attacks exploiting routing mechanisms in WSN. Some familiar attacks are listed here.

3.1) Selective Forwarding

Selective forwarding is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to minimize the suspicion to the neighbor nodes. The impact

Becomes worse when these malicious nodes are at closer to the base station [12]. Then many sensor nodes route messages through these malicious nodes. As a consequence of this attack, a WSN may give wrong observation about the environment which affects badly the purpose of mission critical applications such as, military surveillance and forest fire monitoring.

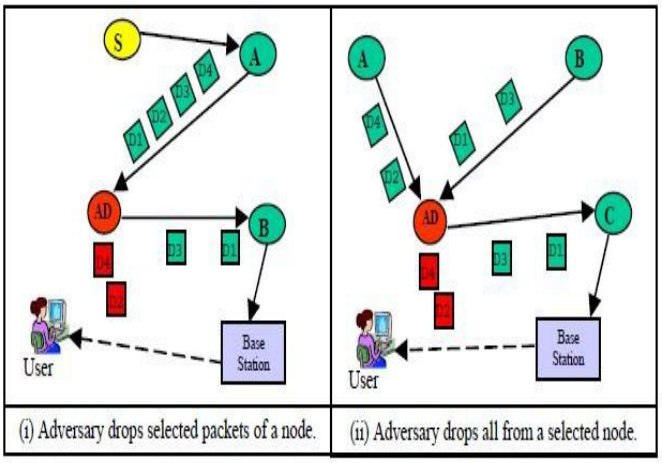

FIGURE 1.SELECTIVE FORWARDING ATTACK

3.2) Sinkhole attack

In sinkhole attack, a compromised node attracts a large number of traffic of surrounding neighbors by spoofing or replaying an advertisement of high quality route to the base station [13]. The attacker can do any malicious activity with the packets passing through the compromised node.

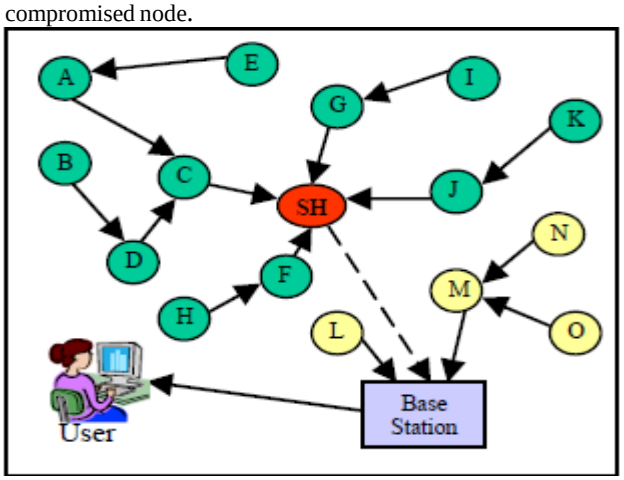

FIGURE 2. SINKHOLE ATTACK

3.3) Wormhole Attack

Wormhole is a critical attack, where the attacker receives packets at one point in the network, tunnels them through a less latency link than the network links to another point in the network and replay packets there locally [14]. This convinces the neighbor nodes of these two end points that these two distant points at either end of the tunnel are very close to each other. If one end point of the tunnel is at near to the base station, the wormhole tunnel can attract significant amount of data traffic to disrupt the routing and operational functionality of WSN. In this case, the attack is similar to sinkhole as the adversary at the Other side of the tunnel advertises a better route to the base station.

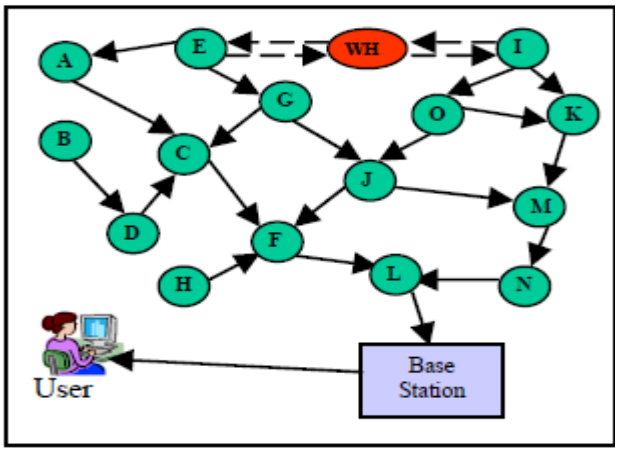

FIGURE 3.WORMHOLE ATTACK

3.4) Sybil Attack

In Sybil attack, a malicious or subverted node forges the identities of more than one node or fabricates identity. This attack has significant effect in geographic routing protocols [13]. In the location based routing protocols, nodes need to exchange location information with their neighbors to route the geographically addressed packets efficiently. Sybil attack disrupts this protocol functionality simultaneously being at more than one place. Identity verification is the key requirement for countering against Sybil attack. Unlike traditional networks, verification of identity in WSN cannot be done with a single shared symmetric key and public key algorithm because of computational limitation of WSN.

4) Transport Layer

In network layer end to end connections are managed.

4.1) Flooding Attack

According to [15] and [16], at this layer, adversaries exploit the protocols that maintain state at either end of the connection. For example, adversary sends many connection establishment requests to the victim node to exhaust its resources causing the Flooding attack. One solution against this attack is to limit the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node.

VI. DEFENCE AGAINST SECUIRTY

A. Cryptography

Selecting the most appropriate cryptographic method is vital in WSNs because all security services are ensured by cryptography.

Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time, and power consumption.
In this section, we focus on the selection of cryptography in WSNs.

Public key cryptography, discussed first, is followed by symmetric key cryptography.

They are as follows:

1. Public Key Cryptography in WSN
2. Symmetric Key Cryptography in WSN

1) Public key cryptography in WSN

Many researchers believe that the code size, data size, processing time, and power consumption make it undesirable for public key algorithm techniques, such as the Diffie–Hellman key agreement protocol [17] or RSA signatures [18], to be employed in WSNs. Public key algorithms such as RSA are computationally intensive and usually execute thousands or even millions of multiplication instructions to perform a single security operation. Further, a microprocessor's public key algorithm efficiency is primarily determined by the number of clock cycles required to perform a multiply instruction.

2) Symmetric key cryptography in WSN

The constraints on computation and power consumption in sensor nodes limit the application of public key cryptography in WSNs. Thus, most research studies focus on symmetric key cryptography in sensor networks. Popular encryption schemes, RC4 [19], RC5 [20], were evaluated on six different microprocessors, the execution time and code memory size were measured for each algorithm and platform. The experiments indicated uniform cryptographic cost for each encryption class and each architecture class. The impact of caches was negligible while Instruction Set Architecture (ISA) support was limited to specific effects on certain algorithms.

B. Secure Routing Protocol

Many routing protocols have been specifically designed for WSNs. These routing protocols can be divided into three categories according to the network structure: flat-based routing, hierarchical- based routing, and location-based routing [21]. In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, nodes play different roles in the network. In location-based routing, sensor node positions are used to route data in the network. Although many sensor network routing protocols have been proposed in literature, few of them have been designed with security as a goal. Lacking security services in the routing protocols, WSNs are vulnerable to many kinds of attacks.

1) Broadcast Authentication

Previous proposals for authenticated broadcast are impractical in WSNs for the following reasons:

• Most proposals rely on public key cryptography for the authentication. However, public key cryptography is impractical for WSNs;

• Even one-time signature schemes that are based on symmetric key cryptography have too much overhead.

µTESLA and its extensions have been proposed to provide broadcast authentication for sensor networks. µ*TESLA* is an authenticated broadcast protocol which was proposed by Perrig *et al.* for the SPINS protocol [8]. µ*TESLA* introduces asymmetry through a delayed disclosure of symmetric keys resulting in an efficient broadcast authentication scheme. µ*TESLA* requires that the base station and nodes be loosely time synchronized, and that each node knows an upper bound on the maximum synchronization error. To send an authenticated packet, the base station simply computes a MAC on the packet with a key that is secret at that point in time. When a node gets a packet, it can verify that the corresponding MAC key was not yet disclosed by the base station. Since a receiving node is assured that the MAC key is known only by the base station, the receiving node is assured that no adversary could have altered the packet in transit.

2) Secure Routing

The goal of a secure routing protocol is to ensure the integrity, authentication, and availability of messages. The proposed secure routing protocols for WSNs in the literature are based on symmetric key cryptography, except the work in which is based on public key cryptography. SPINS is a suite of security protocols optimized for sensor networks [8]. SPINS includes two building blocks: SNEP and µ*TESLA*. SNEP provides data confidentiality, two- party data authentication, and data freshness for peer-to-peer communication (node to base station). µ*TESLA* provides authenticated broadcast as discussed before. We discuss SNEP in this subsection. SPINS assumes that each node is redistributed with a master key *K* which is shared with the base station at creation time. All other keys, including a key *Kencr* for encryption, a key *Kmac* for MAC generation and a key *Krand* for random number generation, are derived from the master key using a strong one-way function. SPINS uses RC5 for confidentiality.

VII. COMMUNICATION PROTOCOLS

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

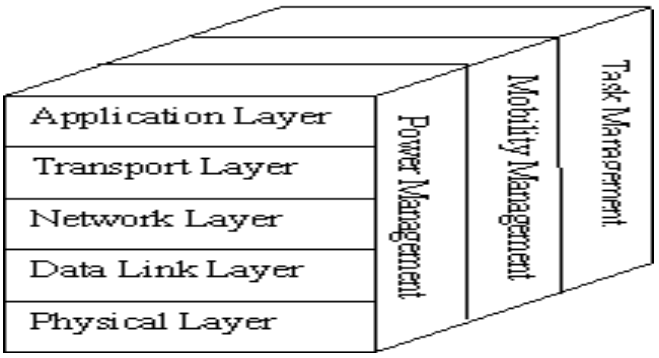

FIGURE 4. LAYERED ARCHITECTURE OF WSN

A. 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.

B. 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. To secure data link layer, Karloff et al [2]

Proposed a link layer security architecture"TinySec" for wireless sensor networks. Naveen Sastry et al [4] proposed ZigBee or the 802.15.4 Standard for hardware based symmetric key encryption. Some researchers also proposed the possible use of public key cryptography [3, 9], secure code distribution [10] to create secure key

During network deployment and maintenance.

C. 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 [5, 6, 15].WSN use ID based protocols and data centric protocols for routing mechanism. In WSN, each node in the network acts as a router, so as to create secure routing protocol. Encryption and decryption techniques are used for secure routing [8, 13, 14].

C. 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.

D. 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 [11] 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) [12] is a key management protocol for sensor networks. It provides multiple keying mechanisms in this regard. By data Aggregation we can optimize data, network's traffic load etc. Wagner [7] describes resilient aggregation technique for cluster based WSN. Cryptography techniques used by him including the layer wise possible attacks and existing protocols described above are summarized in table2 below.

WSN Layer	Types of Attacks	Existing Protocols
Physical Layer	Denial or Service Attack	
Data Link Layer	Denial or Service Attack	Link Layer Security Protocol
Network Layer	Denial or Service Attack, wormholes , sinkholes, Sybil attacks	Routing Protocol
Transport Layer	Denial or service attack	
Application Layer	Malicious Node	Aggregation scheme

TABLE1: SUMMARY OF WSN LAYERS, POSSIBLE ATTACKS ON THEM AND THE EXISTING PROTOCOLS

VIII. CONCLUSION

This paper gives an idea of a major subset of security problems that Wireless Sensor Network faces because of its exceptional design characteristics, communication and deployment pattern. At the same time, this paper includes brief discussion on the important security aspects that are required to design a secure Wire Sensor Network. There are many security solutions or mechanisms that have been proposed for Wireless Sensor Network; some of which are concerned about specific security attacks whereas some are concerned about specific security aspect. There is no standard security mechanism that can provide overall security for WSN. Providing such mechanism is not possible also as WSNs are implemented in various application domains with different level of security requirements. Designing a secure WSN needs proper mapping of security solutions or mechanisms with different security aspects. This also imposes a research challenge for WSN security. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications. In particular, the addition of public key cryptography and the addition of public-key based key management.

REFERENCES

[1] Dr.T.Lalitha Mrs.A.Jayanthila Devi (2014) "Security in Wireless Sensor Networks: Key Management Module in EECBKM"
[2] Deepika Thakral Neha Dureja *Department CSE, MMU Mullana Department CSE, MMU Mullana Haryana, India. Haryana, India. (2012)* "A Review on Security Issues in Wireless Sensor Networks"
[3] E. Shi and A. Perrig, "Designing Secure Sensor Networks," *Wireless Commun. Mag.*, vol. 11, no. 6, Dec. 2004 pp. 38–43.
[4] I. F. Akyildiz *et al.*, "A Survey on Sensor Networks," *IEEE Commun. Mag.*, vol. 40, no. 8, Aug. 2002, pp. 102–114.
[5] A. Perrig *et al.*, "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, vol. 8, no. 5, Sept. 2002, pp.521–34.
[6] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," *SenSys '03: Proc. 1st*
[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114, August 2002.
[8] E. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In *Proceeding of the 3rd International Conference on Security in Pervasive Computing* pages 104–118, 2006.
[9] John Paul Walters, Zhenjiang Liang, Weisong Shi and Vipin Chaudhary. Wireless sensor network security: A survey. *Security in Distributed, Grid, and Pervasive Computing*, 2006.
[10] S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.
[11] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In ICSNC '06: Proceedings of the International *Conference on Systems and Networks Communication*, page 40, Washington, DC, USA, 2006. IEEE Computer Society.
[12] Mayank Saraogi. Security in Wireless Sensor Networks. In *ACM SenSys*, 2004.
[13] I. Khalil, S. Bagchi, and N. B. Shroff. Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Computer. Netw.* 51(13):3750– 3772, 2007.
[14] A. Wood and J. Stankovic. Denial of service in sensor networks. In *Computer*, volume 35, page 54U″ 62, 2002.

[15] D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. In *IEEE Pervasive Computing*, volume 7, pages 74–81, 2008.
[16] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Info. Theory*, vol. 22, no. 6, Nov. 1976, pp.644–54.
[17] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM*, vol. 26, no. 1, 1983, pp. 96–99.
[18] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, Handbook *of Applied Cryptography*, Boca Raton, FL: CRC Press, 1996.
[19] R. L. Rivest, "The RC5 Encryption Algorithm," *Fast Software Encryption*, B. Preneel (Ed.), Springer, 1995, pp. 86–96.
[20] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Commun.* vol. 11, no. 6, Dec. 2004, pp. 6–28.
[21] Yong Wang, Garhan Attebury "A survey of security issue in wireless sensor network" IEEE Communications Surveys, • 2nd Quarter 2006
[22] H. Chan and A. Perrig, "Security and Privacy in Sensor Network IEEE Communications Surveys & Tutorials • 2nd Quarter 2006