ISSN:0975-9646

Study of Security in Wireless Sensor Networks

Pooja Kumari[1], Mukesh Kumar[2], Rahul Rishi[3]
M.Tech Student[1], Assistant Professor[2], Associate Professor[3]
Department of Computer Science and Engineering
The Technological Institute of Textile and Science, Bhiwani, Haryana

Abstract:-Wireless Sensor Network (WSN) is an emerging technology that shows great assure for various futuristic applications both for public and military. Many researchers tried to develop further cost and energy efficient computing devices and algorithms for WSN but the most challenging is to fit the security of WSN into that strained environment. However, security is crucial to the success of applying WSN. So it becomes essential to be familiar with the security aspects of WSN before designing WSN system. When sensor networks are deployed in an aggressive terrain, security becomes extremely important, as they are prone to different types of despite attacks. The intent of this paper is to investigate security problems and various security requirements. We identify the attacks at all the layers of WSN network architecture and also tried to find their possible solution.

Keywords:-Sensor, security, attack.

I. INTRODUCTION

A Wireless Sensor Network is a combination of wireless networking and embedded system technology that monitors physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Initially, Wireless Sensor Networks were mainly used for military surveillance.

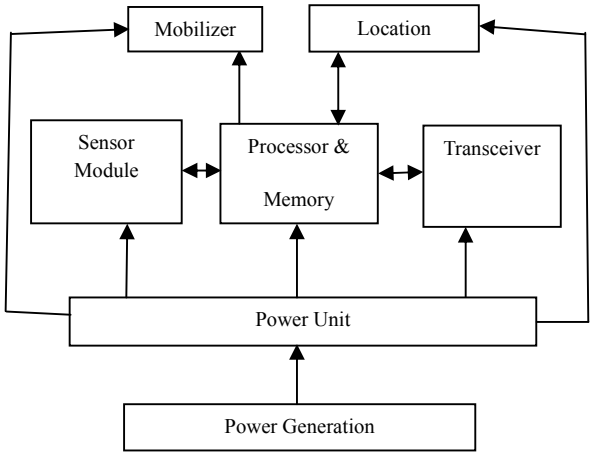

Fig 1: Wireless Sensor Network architecture

The basic idea of sensor network is to disperse tiny sensing devices; which can sense some changes of incidents and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Sensors that are in use today can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties [1]. The communication among the sensors is done using wireless transceivers in wireless sensor networks. Sensor networks concern to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. The figure 2 shows the complexity of wireless sensor networks, which generally consist of a data acquisition network and a data distribution network which is monitored and controlled by a manager center. The superfluity of available technologies makes even the selection of components difficult and also makes the design of a consistent, reliable, robust overall system.

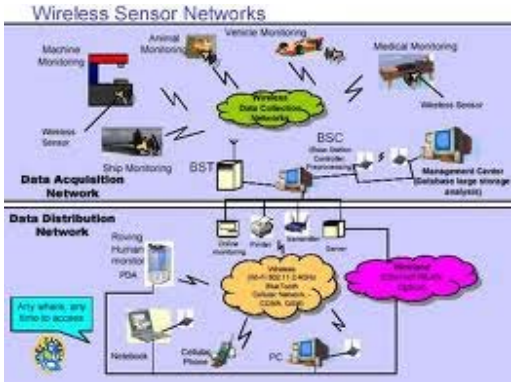

Fig 2: Wireless Sensor Networks

Security is a common concern for any network system, but security has a great importance in Wireless Sensor Network 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. As many existing security schemes for traditional networks are not applicable for WSN so providing security for WSN represents a rich field of research. For example, WSN requires unimportant security mechanism to minimize the overhead so that performance of network remains unaffected. The reason is that WSN has less resources and network than traditional networks. The battery power and memory size is very limited and computational ability is also very limited. A typical sensor node processor is of 4-8 MHz, having 4KB of RAM and 128KB flash [3]. Sensor nodes are dispersed randomly in the unreachable manner, wild environment without any infrastructure support and operate unsupervised.

II. OBSTACLES IN DEVELOPING SECURITY PROTOCOLS FOR SENSOR NETWORKS

Normally, sensor nodes interact with their surrounding environment because they are densely distributed. A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Due to these constraints it is challenging to directly utilize the existing security approaches to the area of wireless sensor networks. Hence, to develop the useful security mechanisms, it is necessary to know and understand these constraints first [2].

A. *Very Limited Resources*

Certain amount of resources is needed for all security approaches for the implementation, including data memory, code space and energy to power the sensor.

1) Limited memory and storage space: A sensor is a tiny device with only a small amount of memory and storage space for the code. So it is necessary to limit the code size of security algorithms to build an effective security mechanism. For example, one common sensor type (TelosB) has an 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage[8]. The total code space of TinyOS, the de-facto standard operating system for wireless sensors, is approximately 4K [5], and the core scheduler occupies only 178 bytes.

2) Power limitation: Since sensor nodes are usually operated by limited batteries, however, energy is a very scarce resource for such sensor systems and has to be managed wisely in order to extend the life of the sensor nodes for the duration of a particular mission. Energy consumption in a sensor node can be due to either "useful" or "wasteful" sources. Sensor nodes cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, to extend the life of the individual sensor node and the entire sensor network the battery charge taken with them must be preserved. 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

Unreliable communication is another threat to sensor security. The security of the network relies heavily on the communication protocol.

1) Unreliable transfer: The packet-based routing of the sensor network is connectionless thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. If the protocol lacks the appropriate error handling it is possible to lose critical security packets, for example, a cryptographic key. [6]

2) Conflicts: The communication may still be unreliable, due to the broadcast nature of the wireless sensor network even if the channel is reliable. In a high density network there is a major problem that if packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail.

3) Latency: The difficulty arises to achieve synchronization among sensor nodes due to the multi-hop routing, network congestion, and nodes processing that lead to greater latency in the network. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution.

C. Unattended Operation

The sensor nodes may be left unattended for long periods of time depending on the function of the particular sensor network. There are three main caveats to unattended sensor nodes:

1) Exposure to Physical Attacks: The sensor may be distributed in an environment open to adversaries, bad weather, and so on The physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network.

2) Managed Remotely: Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamper proof seals) and physical maintenance issues (e.g., battery replacement).

3) No Central Management Point: As a sensor network is a distributed network without any central management point, this will increase the property of being able to survive and grow of the sensor network. It will make the network organization difficult, inefficient, and fragile when designed improperly.

III. SECURITY REQUIREMENTS

Sensor networks are used in a number of domains that handle sensitive information. Due to this, there are many considerations that should be investigated and are related with protecting sensitive information traveling between nodes (which are either sensor nodes or the base station) from been disclosure to unauthorized third parties.

A. Data Confidentiality

Data confidentiality is the most important issue in network security. Confidentiality requirement is needed to ensure that sensitive information is well protected and not revealed to unauthorized third parties. 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.

B. Authentication

In the case of sensor networks, it is essential for each sensor node and base station to have the ability to verify that the data received was really send by a trusted sender and not by an adversary that tricked legitimate nodes into accepting false data. If such a case happens and false data are supplied into the network, then the behavior of the network could not be predicted and most of times will not outcome as expected.

C. Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous, for example for the health care sector where lives are endangered. Thus, data integrity ensures that any received data has not been altered in transit.

D. Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Data Freshness shows that the data is recent. This is an important security requirement to ensure that no message has been replayed meaning that the messages are in an ordering and they cannot be reused. To achieve freshness, network protocols must be designed in a way to identify duplicate packets and discard them preventing potential mix-up.

E. Availability

The wireless sensor network will introduce some extra costs to adjust the traditional encryption algorithms. Availability ensures that services and information can be accessed at the time that they are required. Lack of availability may affect the operation of many critical real time applications like those in the health care sector that require a 24 / 7 operation that could even result in the loss of life. Therefore, it is critical to ensure resilience to attacks targeting the availability of the system and find ways to fill in the gap created by the capturing or disablement of a specific node by assigning its duties to some other nodes in the network.

F. Self-Organization

A wireless sensor network is a an ad hoc network which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. No infrastructure is present in a sensor network for network management. For example, the dynamics of the whole network inhibits the idea of pre-installation of a shared key between the base station and all sensors [8].Several random key predistribution schemes have been proposed in the context of symmetric encryption techniques [9, 10, 11, 12].

G. Time Synchronization

Some form of time synchronization is required in most sensor network applications. In order to preserve power, an individual sensor's radio may be turned off for periods of time. As the packet travels between two pair wise sensors so sensors may wish to compute the end to end delay. For some applications sensor network may require group synchronization. In [20], the authors propose a set of secure synchronization protocols for sender-receiver (pair wise), multi hop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

H. Secure-Localization

The utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, non-secured location information can easily manipulated by an attacker by reporting false signal strengths, replaying signals, etc.

IV. ATTACKS AND SECURITY SCHEMES IN WIRELESS SENSOR NETWORK

As security is of more concern in any network so it is necessary to address the attacks and then take counter measures at the design time of WSN. A sensor node is considered as being compromised when an attacker, through various means, can either read or modify its internal memory. This section lists and gives brief discussion about the major attacks against Wireless Sensor Network.

A. Physical Attack

This attack is also called as node capture. Sensor networks typically operate in hostile outdoor environments. In such 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, i.e., threats due to physical node destructions [13]. In this type of attack, attackers gain full control over some sensor nodes through direct physical access [14]. Sensor nodes with tamper proofing features are impractical, as the cost of sensor nodes must be kept as cheap as possible for WSN. 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 like it becomes easier for an attacker to get unrestricted access to WSN by getting key information stored on sensor node's memory. An adversary may require expert knowledge, costly equipments and other resources for performing physical attack.

B. Attacks at Different Layer

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. 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.

Jamming: In physical layer, jamming is a common attack. The attacker needs to know only the wireless transmission frequency in WSN. The frequency of the radio signals that attacker uses is same as the frequency of the sensor network [15]. 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. Thus, affected nodes become completely isolated as long as the jamming signal continues and no messages can be exchanged between the affected nodes and other sender nodes. For preventing physical layer jamming [12] suggests frequency hopping as a countermeasure. In frequency hopping spread spectrum, nodes change frequency in a predetermined sequence. But, it is not suitable for WSN because every extra frequency requires extra processing and the range of possible frequencies for WSN is limited. [5] Suggests Ultra Wide Band transmission technique as an anti jamming solution. UWB transmission is based on sending very short pulses in order of nanoseconds across a wide frequency band and is very difficult to detect. This technique is suitable for WSN because of its low energy consumption.

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.

Denial of Service: Denial of Service (DoS) [16], [17] is produced 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 network's capability to provide a service.

For example, consider the following Fig. 3. Assume a shortest path exists from **X** to **Z** and **C** and **Z** cannot hear each other, that nodes **B** and **C** cannot hear each other, and that **Y** is a malicious node attempting a denial of service attack. Suppose **X** wishes to communicate with **Z** and that **X** has an unexpired route to **Z** in its route cache. **X** transmits a data packet toward **Z** with the source route **X --> A --> B --> Y --> C --> D --> Z** contained in the packet's header. When **Y** receives the packet, it can alter the source route in the packet's header, such as deleting **D** from the source route. Consequently, when **C** receives the altered packet, it attempts to forward the packet to **Z**. Since **Z** cannot hear **C**, the transmission is unsuccessful.

$$X \Longleftrightarrow A \Longleftrightarrow B \Longleftrightarrow Y \Longleftrightarrow C \Longleftrightarrow D \Longleftrightarrow Z$$

Figure 3: Denial of service attack

3) Network Layer

Network layer provides routing of messages from one node to another node which are neighbors or may be multi hops away for example, node to base station or node to cluster leader. There are several attacks exploiting routing mechanisms in WSN. Some familiar attacks are listed here.

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. This attack can be extended to forward messages to wrong nodes and thus misdirecting the traffic. Two different countermeasures have been proposed against selective forwarding attack. One defense is to send data using multi path routing [16]. Another one is detection of compromised nodes which are misbehaving in terms of selective forwarding and route TKK T-110.5190 Seminar on Internet working the data seeking an alternative path.

Black hole/Sinkhole Attack: In this attack, a malicious node acts as a black hole [17] to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the Communicating nodes (for example, sink and sensor node), 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.

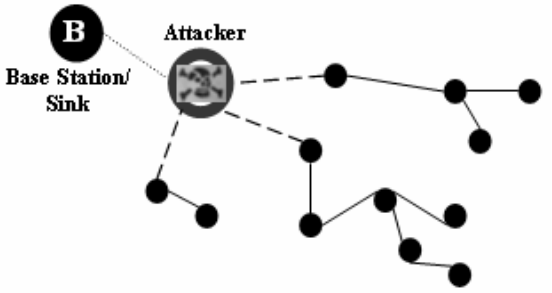

Figure 4: Conceptual view of Black hole Attack

Figure 4 shows the conceptual view of a black hole/sinkhole attack. Both the sinkhole and wormhole attacks are difficult to detect especially in WSNs those use routing protocols in which routes are decided based on information advertisements such as remaining energy or minimum hop count to base station. [18] Suggests using geographic routing protocol which has better resilience against these attacks. GPSR [19] and GEAR [20] are such geographic based routing protocols.

Hello Flood Attack: Hello flood attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker. The key solution against Hello Flood attack is

authentication. An authenticated broadcast protocol for example, μTESLA is an efficient one for this purpose. This protocol is based on symmetric key cryptography with minimum packet overheads.

Wormhole Attack: Wormhole attack 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. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information.

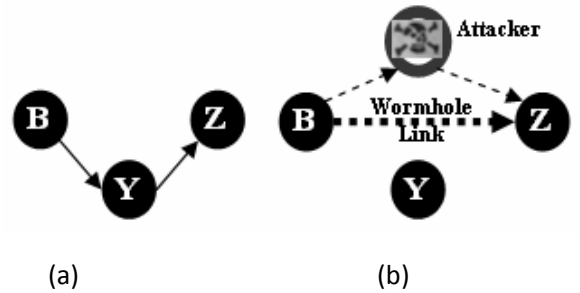

Figure 5: Wormhole Attack

Figure 5 (a & b) shows a situation where a wormhole attack takes place. When a node B (for example, the base station or any other sensor) 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 B, and will mark this node as its parent. Hence, even if the victim nodes are multi - hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

Sybil Attack: In many situations sensors in WSN need to work together to perform a task so they can use distribution of subtasks and redundancy of information.

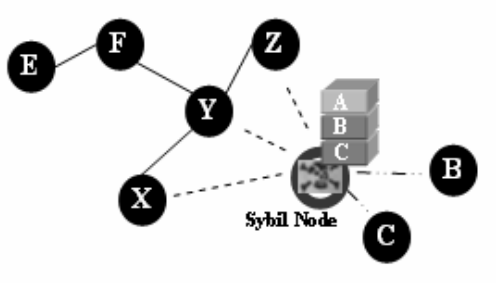

Figure 6: Sybil Attack

In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes (Figure 6). This type of attack where a node forges the identities of more than one node is the Sybil attack [21], [22]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [22]. 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. Newsome et al. in [15] shows with quantitative analysis that random key pre distribution scheme can be used to defend against Sybil attack. For this purpose, they associated sensor node's identity with its assigned key using one way hash function. According to their mechanism, the network is able to verify part or all of the keys that an identity claims to have and thus counters against Sybil attack.

4) Transport Layer

In transport layer end to end connections are managed.

Flooding Attack: 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

5) Application Layer

In application layer, data is collected and manages. Here, sensor nodes can be subverted to reveal its information including disclosure of cryptographic keys hence compromising the whole sensor network. Moreover, a node can be compromised to malfunction and generate inaccurate data and this effect can be worse enough when the node is a cluster leader in WSN [23].

V. PROPOSED SECURITY SCHEMES AND RELATED WORK

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In this section we review and map various security schemes proposed or implemented so far for wireless sensor networks.

A. Security Schemes for Wireless Sensor Networks

[24] Gives an analysis of secure routing in wireless sensor networks. [25] Studies how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's life time. [3] Aims at increasing energy efficiency for key management in wireless sensor networks and uses. Younis et.al. [32] Network model for its application. Wood et al. [27] studies DoS attacks against different layers of sensor protocol stack. [40] Presents a probabilistic secret sharing

protocol to defend Hello flood attacks. REWARD [34] is a routing algorithm which fights against black holes in the network. [28] Proposes separate security schemes for data with various sensitivity levels and a location-based scheme for wireless sensor networks that protects the rest of the network, even when parts of the network are compromised. In Table 1 we summarize various security schemes along with their main properties proposed so far for wireless sensor networks.

TABLE 1

Summary of various security schemes for wireless sensor networks

Security Schemes	Attacks Deterred	Network Architecture	Major Features
JAM [34]	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based [35]	DoS Attack (Jamming)	Hybrid (mainly wireless partly wired) sensor network	Uses wormholes to avoid jamming
Statistical En-Route Filtering [29]	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key,Pre-distribution etc. [20]	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting sybil entity
Bidirectional Verification, Multi-path multi-base station routing [29]	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security [28]	Information or Data Spoofing	Traditional wireless sensor network	Efficient resource management, Protects the network even if part of the network is compromised
TIK [23]	Wormhole Attack,Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Predistribution [25], [26],[9]	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
[34]	Data and Information Spoofing	Distributed Sensor Network, Large-scale wireless sensor network with dynamic nature	Suitable for large wireless sensor networks which allows addition and deletion of sensors, Resilient to sensor node capture
REWARD [30]	Black hole attacks	Traditional wireless sensor network	Uses geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect black hole attacks
TinySec [31]	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & μTESLA [6]	Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

VI. HOLISTIC SECURITY IN WIRELESS SENSOR NETWORKS

A holistic approach [33] improves the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option.

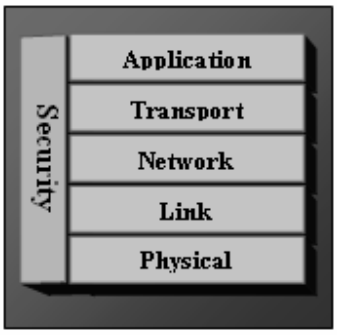

Figure 7: Holistic view of Security in wireless sensor networks

In holistic approach security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not exceed the assessed security risk at a specific time, the security measures must be able to exhibit a graceful degradation if there is no physical security ensured for the sensors and if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measure should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, we can improve the security for the whole network.

VII. CONCLUSION

WSN security is a very important issue which is motivated towards ensuring security under the strict constraints of computational power, energy and other hardware constraints. Super small sensor nodes, super low power consumption and having low cost made wireless sensor network an attracting uncountable application domain to sense and collect data. But, these attractive features made wireless sensor network challenging to integrate security mechanism into it. This paper gives an idea of a major paradigm 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 wireless sensor network. In this paper we discussed well known attacks at every layer of the network and their proposed counter measures because security of a wireless sensor network is dependent on securing all the layers of the network. This paper gives an idea about how the adversaries can actually attack the wireless sensor network exploiting its vulnerabilities and what kind of security awareness should be taken into account when incorporating security mechanisms in wireless sensor network. Finally this paper explores some security schemes like holistic security scheme which could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

REFERENCES

[1] Pathan,A-S.K.,Islam, H. K., Sayeed, S. A., Ahmad, F. and Hong, C.S., "A Framework for Providing E-Services to the Rural Areas usuing Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

[2] D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwo od, MD, 2000.

[3] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In *ICSNC '06: Proceedings of the In- ternational Conference on Systems and Networks Comunication* , page 40, Washington, DC, USA, 2006. IEEE Computer Society.

[4] http://www.xbow.com/wireless home.aspx, 2006.

[5] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. System architecture directions for networked sensors. In Architectural Support for Programming Languages and Operating Systems, pages 93–104, 2000.

[6] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang. Fast authenticated key establishment protocols for self-organizing sensor networks. In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pages 141–150. ACM Press, 2003.

[7] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: security protocols for sensor networks. Wireless Networking, 8(5):521–534, 2002.

[8] L. Eschenauer and V. D. Gligor. A key-management scheme for distributedsensor networks. In Proceedings of the 9th ACM conference on Computer and communications security, pages 41–47. ACM Press, 2002.

[9] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy, page 197. IEEE Computer Society, 2003.

[10] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM conference on Computer and communications security, pages 41–47. ACM Press, 2002.

[11] J. Hwang and Y. Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN '04), pages 43–52, New York, NY, USA, 2004. ACM Press.

[12] D. Liu, P. Ning, and R. Li. Establishing pairwise keys in distributed sensor networks. ACM Trans. Inf. Syst. Secur., 8(1):41–77, 2005.

[13] X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan. Sensor network configuration under physical attacks. Technical Report Technical Report (OSU-CISRC-7/ 04-TR45), Dept. of Computer Science and Engineering, The Ohio-State University, July 2004.

[14] 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 (SPC, pages 104–118, 2006.

[15] John Paul Walters, Zhengqiang Liang, Weisong Shi and Vipin Chaudhary. Wireless sensor network security: A
survey. Security in Distributed, Grid, and Pervasive Computing, 2006.

[16] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. SIGMOBILE Mob. Comput.Commun. Rev., 5(4):11–25, October 2001

[17] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.
[18] Y. W. Law and P. Havinga. How to secure a wireless sensor network. pages 89–95, Dec. 2005.
[19] B. Karp and H. T. Kung. Gpsr: greedy perimeter stateless routing for wireless networks. In MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, pages 243–254, New York, NY, USA, 2000. ACM Press.
[20] N.-C. Wang, P.-C. Yeh, and Y.-F. Huang. An energy-aware data aggregation scheme for grid-based wireless sensor networks. In IWCMC '07:Proceedings of the 2007 international conference on Wireless communications and mobile computing, pages 487–492, New York, NY, USA, 2007. ACM.
[21] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).
[22] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.
[23] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In ICSNC '06: Proceedings of the In-
ternational Conference on Systems and Networks Communication, page 40, Washington, DC, USA, 2006. IEEE Computer Society.
[24] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.
[25] Yuan, L. and Qu, G., "Design space exploration for energy-efficient secure sensor network", Proc. The IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2002, 17-19 July 2002, pp. 88 – 97.
[26] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key
Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 1-16 Oct. 2002 pp. 129 – 136.
[27] Younis, M., Youssef, M., and Arisha, K., "Energy-aware routing in cluster-based sensor networks" Proc. 10th IEEE International Symposium on Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003.
(ISCC 2003). vol.1, pp. 335 - 340.
[28] Wood, A. D. and Stankovic, J. A., "Denial of Service in Sensor Networks", Computer, Volume 35, Issue 10, Oct. 2002 pp. 54 - 62.
[29] Hamid, M. A., Rashid, M-O., and Hong, C. S., "Routing Security in Sensor Network: Hello Flood Attack and Defense", to appear in IEEE ICNEWS 2006, 2-4 January, Dhaka.
[30] Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.
[31] Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., and Srivastava, M.B., "On communication security in wireless ad-hoc sensor networks", 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002, 10-12 June 2002, pp. 139 – 144.
[32] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.
[33] Avancha, S, "A Holistic Approach to Secure Sensor Networks", PhD Dissertition, University of Maryland, 2005.
[34] Eschenauer, L. and Gligor, V. D., "A key-management scheme for distributed sensor networks", Proc. ACM CCS'02, 18-22 November 2002, pp. 41-47.