Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

"A SURVEY ON SECURITY FRAMEWORKS FOR WIRELESS SENSOR NETWORKS"

Ramesh L[1], Dr. A. Marimuthu [2]
[1]*Research Scholar,* [2]*Associate Professor*
[1,2]*PG and Research Department of Computer Science, Government Arts college, Coimbatore-18*

Abstract—Wireless Sensor Networks (WSN) is an emerging technology now-a-days and has a wide range of applications such as battlefield surveillance, traffic surveillance, forest fire detection, flood detection etc. But wireless sensor networks are susceptible to a variety of potential attacks which obstructs the normal operation of the network. The wireless sensor network nature of communication is unsafe and unprotected because of deployment in hostile environment, limited resources, an automated nature and untrusted broadcast transmission media. The most of security techniques are not sufficient in WSN network and security is a vital requirement for network.

The intent of this paper is to investigate the security related frameworks. The introductory section gives brief information on the WSN components and its architecture. Then it deals with some of the major security issues and challenges over wireless sensor networks (WSNs).
Keywords—Attacks, wireless sensor network, security

I. INTRODUCTION

The field of sensor network is well known due to its popularity in research community. It is a collection of thousands of self-organized sensor nodes capable of wireless communication. Since the nodes are not so wealthy in terms of resources, therefore complex algorithms cannot be played over it. Security is the main preconcert to socialize this network for common usage. For making the WSN secure, cryptography plays an important role. There are many algorithms proposed so far: symmetric, asymmetric and hybrid. But complex algorithms, which had been proposed for MANETs, are not successful over WSN. To design the network cryptographically (completely) secure, security must be integrated into every node of the network. So security should be implemented at every point of the network. Cryptography is a standard method to provide security in a network. But here in WSN, cryptographic algorithms should be designed such that it is robust in nature but does not use more memory, more power, and more energy so as the lifetime of the is also dependent upon the nature of the application and algorithm might be specific to the application.

1.1. Security Requirements

Confidentiality – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. In a WSN, the issue of confidentiality should address the following requirements: (i) a sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so, (ii) key distribution mechanism should be extremely robust, (iii) public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks.

Authentication - Authentication ensures the reliability of the message by identifying its origin. By authenticating other nodes, cluster heads, and base stations before granting a limited resource, or

revealing information. In a WSN, the issue of authentication should address the following requirements: (i) communicating node is the one that it claims to be, (ii) receiver node should verify that the received packets have undeniably come from the actual sender node.

Integrity - Integrity ensures the reliability of the data and refers to the ability to confirm that a message has not been tampered with, altered or changed while on the network. In a WSN, the issue of integrity should address the following requirements: (i) only the nodes in the network should have access to the keys and only an assigned base station should have the privilege to change the keys. This would effectively thwart unauthorized nodes from obtaining knowledge about the keys used and preclude updates from external sources. (ii) It protects against an active, intelligent attacker who might attempt to disguise his attack as noise.

Availability - Availability ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. In a WSN, the issue of availability should address the following requirements: (i) the security mechanisms should be available all the time; a single point of failure should be avoided, (ii) the mechanism is used as a central access control system to ensure successful delivery of every message to its recipient node.

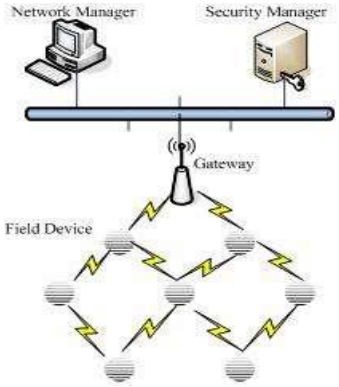
1.2. Significance of Cryptography in Wireless Sensor Networks

Since the popularity of WSN increasing for a wide variety of applications such as climate change, environmental monitoring, traffic monitoring and home automation. So to keep the WSN secure is a challenging task. Cryptography is one way to provide security. It can be provided through by symmetric key techniques, asymmetric key techniques and hash function. Since WSN are very constrained in terms of computing, communication and battery power, it requires a light weight cryptographic algorithm. Due to constraints of sensor nodes, the selection of cryptographic technique is vital in WSN. Cryptography in WSN can be explained in the following three aspects: symmetric, asymmetric and hash function.

1.3 WSN Architecture

In a typical WSN we see following network components –Sensor nodes (Field devices) – Each sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for

a) Interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.
b) Gateway or Access points – A Gateway enables communication between Host application and field devices.
c) Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.
d) Security manager – The Security Manager is responsible for the generation, and management of keys. The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, high power Wi-Fi links etc.



II. SECURITY ISSUES IN WIRELESS SENSOR NETWORKS

A WSN consists of a large number of sensor nodes that are inherently resource constrained devices. These nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. These constraints are due to limited energy and physical size of the sensor nodes. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSNs. In order to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes.

Some of the major Security issues of a WSN are listed below.

***Energy constraints*:** Energy is the biggest constraint for a WSN. In general, energy consumption in sensor nodes can be categorized in three parts: (i) energy for the sensor transducer, (ii) energy for communication among sensor nodes, and (iii) energy for microprocessor computation. The study in [1] found that each bit transmitted in WSNs consumes about as much power as executing 800 to 1000 instructions. Thus, communication is more costly than computation in WSNs. Any message expansion caused by security mechanisms comes at a significant cost. Further, higher security levels in WSNs usually correspond to more energy consumption for cryptographic functions. Thus, WSNs could be divided into different security levels depending on energy cost [2, 3].

***Memory limitations*:** A sensor is a tiny device with only a small amount of memory and storage space. Memory is a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate results of computations. There is usually not enough space to run complicated algorithms after loading the OS and application code. In the SmartDust project, for example, TinyOS consumes about 4K bytes of instructions, leaving only 4500 bytes for running security algorithms and applications [1]. A common sensor type- TelosB- has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage [4]. The current security algorithms are therefore, infeasible in these sensors [5].

Unreliable communication: Unreliable communication is another serious threat to sensor security. Normally the packet-based routing of sensor networks is based on connectionless protocols and thus inherently unreliable. Packets may get damaged due to channel errors or may get dropped at highly congested nodes. Furthermore, the unreliable wireless communication channel may also lead to damaged or corrupted packets. Higher error rate also mandates robust error handling schemes to be implemented leading to higher overhead. In certain situation even if the channel is reliable, the communication may not be so. This is due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission [1].

***Higher latency in communication*:** In a WSN, multi-hop routing, network congestion and processing in the intermediate nodes may lead to higher latency in packet transmission. This makes synchronization very difficult to achieve. The synchronization issues may sometimes be very critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution [6].

***Unattended operation of networks*:** In most cases, the nodes in a WSN are deployed in remote regions and are left unattended. The likelihood that a sensor encounters a physical attack in such an environment is therefore, very high. Remote management of a WSN makes it virtually impossible to detect physical tampering. This makes security in WSNs a particularly difficult task.

III. SECURITY ATTACKS IN WIRELESS SENSOR NETWORKS

WSNs are vulnerable to various types of attacks. These attacks can be broadly categorized follows[14]

- ***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.
- ***Stealthy attack against service integrity*:** in a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node.

3.1 Denial of service attacks

Wood et al. have defined a DoS attack as an event that diminishes or attempts to reduce a network's capacity to perform its expected function [19]. This attack may have specific target; for example, an entity may suppress all messages directed to particular destination(e.g., the security audit service).There are several standard techniques existing in the literature to cope with some of the more common denial of service attacks, although in a broader sense, development of a generic defense mechanism against DoS attacks is still an open problem. Moreover, most of the defense mechanisms require high computational overhead and hence not suitable for resource-constrained WSNs. Since DoS attacks in WSNs can sometimes prove very costly, researchers have spent a great deal of effort in identifying various types of such attacks, and devising strategies to defend against them. Some important types of DoS attacks in WSNs are discussed below.

3.1.1 Physical layer attacks

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [1]. As with any radio-based medium there exists the possibility of jamming in WSNs. There are two broad categories of attack on WSNs in the physical layer: **(i) jamming and (ii) tampering.** They are described as follows.

***Jamming*:** it is a type of attack which interferes with the radio frequencies that the nodes using in WSN[19, 14]. A jamming source may either be powerful enough to disrupt the entire network or less powerful jamming sources, an adversary can potentially disrupt communication in the entire network by strategically distributing the jamming sources. An intermittent jamming may also prove detrimental [19].

Tampering: sometimes the nodes are physically tampered by an adversary this type of condition is called as tampering. This type of attacks may damage, replace the nodes to acquire information. Sensor networks typically operate in outdoor environments. Due to unattended and distributed nature, the nodes in a WSN are highly susceptible to physical attacks [15]. The physical attacks may cause irreversible damage to the nodes. The adversary can extract cryptographic keys from the captured node, tamper with its circuitry, modify the program codes or even replace it with a malicious sensor [18]. It has been shown that sensor nodes such as MICA2 motes can be compromised in less than one minute time [12].

3.1.2 Link layer attacks

The link layer is responsible for multiplexing of data-streams, data frame detection, medium access control, and error control [1]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously [19]. When packets collide, they are discarded and need to be retransmitted. An adversary may strategically cause collisions in specific packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions. Repeated collisions can also be used by an attacker to cause resource exhaustion[19]. For example, a naïve link layer implementation may continuously attempt to retransmit the corrupted packets. Unless these retransmissions are detected early, the energy levels of the nodes would be exhausted quickly. Unfairness is a weak form of DoS attack [29]. An attacker may cause unfairness by intermittently using the above link layer attacks. In this case, the adversary causes degradation of real-time applications running on other nodes by intermittently disrupting their frame transmissions.

3.1.3 Network layer attacks

The network layer of WSNs is vulnerable to the different types of attacks such as: **(i) spoofed routing information, (ii) selective packet forwarding, (iii) sinkhole, (iv) Sybil, (v) wormhole,(vi) blackhole and grayhole, (vii) HELLO flood, (viii) Byzantine, (ix) information disclosure,(x) acknowledgment spoofing etc.** These attacks are described briefly in the following:

***Spoofed routing information*:** the most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network [16]. These disruptions include creation of routing loops, attracting or repelling network traffic from selected nodes, extending or shortening source routes, generating fake error messages, causing network partitioning, and increasing end-to-end latency.

***Selective forwarding*:** in a multi-hop network like a WSN, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others [16].

***Sinkhole*:** In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbors by forging the routing information [19, 16, 17]. The result is that the neighbor nodes choose the compromised node as the next-hop node to route their data through. This type of attack makes selective forwarding very simple as all traffic from a large area in the network would flow through the compromised node.

Sybil attack: it is an attack where one node presents more that one identity in a network. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in

distributed data storage systems in peer-to-peer networks [18]. Newsome et al describe this attack from the perspective of a WSN [17]. In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation, and foiling misbehavior detection. Regardless of the target (voting, routing, aggregation), the Sybil algorithm functions similarly. All of the techniques involve utilizing multiple identities. For instance, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional "votes". Similarly, to attack the routing protocol, the Sybil attack would rely on a malicious node taking on the identity of multiple nodes, and thus routing multiple paths through a single malicious node.

***Wormhole*:** a wormhole is low latency link between two portions of a network over which an attacker replays network messages [16]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to sinkhole attack as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network.

***Blackhole and Grayhole*:** in the *blackhole attack*, a malicious node falsely advertises good paths (e.g., the shortest path or the most stable path) to the destination node during the path-finding process (in reactive routing protocols), or in the route update messages (in proactive routing protocols). The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node concerned. A more delicate form of this attack is known as the *grayhole attack*, where the malicious node intermittently drops data packets thereby making its detection more difficult.

***HELLO flood*:** most of the protocols that use *HELLO* packets make the naïve assumption that receiving such a packet implies that the sender is within the radio range of the receiver. An attacker may use a high-powered transmitter to fool a large number of nodes and make them believe that they are within its neighborhood [16]. Subsequently, the attacker node falsely broadcasts a shorter route to the base station, and all the nodes which received the *HELLO* packets, attempt to transmit to the attacker node. However, these nodes are out of the radio
range of the attacker.

***Byzantine attack*:** in this attack, a compromised node or a set of compromised nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets in non-optimal routes, and selectively dropping packets [19]. Byzantine attacks are very difficult to detect , since under such attacks the networks usually do not exhibit any abnormal behavior.

***Information disclosure*:** a compromised node may leak confidential or important information to unauthorized nodes in a network. Such information may include information regarding the network topology, geographic location of nodes, or optimal routes to authorized nodes in the network.

***Reource-depletion attack*:** in this type of attack, a malicious node tries to deplete resources of other nodes in a network. The typical resources that are targeted are: battery power, bandwidth, and computational power. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to other nodes.

***Acknowledgment spoofing*:** some routing algorithms for WSNs require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighboring nodes and spoof the acknowledgments thereby providing false information to the nodes [16]. In this way, the attacker is able to disseminate wrong information in the network about the

status of the nodes, since some acknowledgment may arrive from nodes which are not alive in reality. In addition to above categories of attacks, there are various types of possible attacks on the routing protocols in WSNs. Most of the routing protocols in WSNs are vulnerable to attacks such as: **routing table overflow, routing table poisoning, packet replication, route cache poisoning, rushing attacks etc.** A comprehensive discussion on these attacks have been done in[20].

3.1.4 Transport layer attacks

The attacks that can be launched on the transport layer in a WSN are flooding attack and De synchronization attack.

Flooding: Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding [19]. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

***De-synchronization*:** De-synchronization refers to the disruption of an existing connection [19]. An attacker may, for example, repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data causing them instead to waste energy attempting to recover from errors which never really exist.

Layer	Attacks	Defense
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
Link	Collision Exhaustion Unfairness	Error-correcting code Rate limitation Small frames
Network	Spoofed routing information & Selective forwarding Sinkhole Sybil Wormhole HELLO Flood Acknowledgment flooding	Egress filtering, authentication, monitoring Redundancy probing Authentication, monitoring, redundancy Authentication, probing Authentication, packet leashes by using geographic and temporal info Authentication, verify the bi-directional link Authentication
Transport	Flooding De-synchronization	Client puzzles Authentication

Table 1. Attacks on various layers of a WSN and their countermeasures
Source: Y. Wang, G. Attebury, and B. Ramamurthy, IEEE Communications Surveys and Tutorials, Vol. 8, no. 2, pp. 2- 23, 2006.

3.2 Attacks on secrecy and authentication

There are different types of attacks under this category. They are described in Sections 3.2.1 through 3.2.2.

3.2.1 Node replication attack

In a *node replication attack*, an attacker attempts to add a node to an existing WSN by replication (i.e. copying) the node identifier of an already existing node in the network [21]. A node replicated and joined in the network in this manner can potentially cause severe disruption in

message communication in the WSN by corrupting and forwarding the packets in wrong routes. This may also lead to network partitioning and communication of false sensor readings. In addition, if the attacker gains physical access to the entire network, it is possible for him to copy the cryptographic keys and use these keys for message communication from the replicated node. The attacker can also place the replicated node in strategic locations in the network so that he could easily manipulate a specific segment of the network, possibly causing a network partitioning.

3.2.2 Attacks on privacy

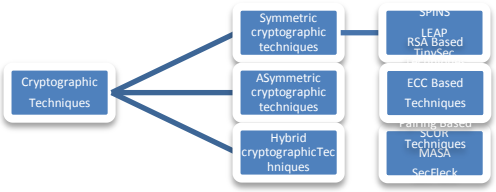
Since WSNs are capable of automatic data collection through efficient and strategic deployment of sensors, these networks are also vulnerable to potential abuse of these vast data sources. Privacy preservation of sensitive data in a WSN is particularly difficult challenge [22]. Moreover, an adversary may gather seemingly innocuous data to derive sensitive information if he knows how to aggregate data collected from multiple sensor nodes. This is in analogy to the *panda hunter problem*, where the hunter can accurately estimate the location of the panda by systematically monitoring the traffic [23]. The privacy preservation in WSNs is even more challenging since these networks make large volumes of information easily available through remote access mechanisms. Since the adversary need not be physically present to carryout the surveillance, the information gathering process can be done anonymously with a very low risk. In addition, remote access allows a single adversary to monitor multiple sites simultaneously [24]. Following are some of the common attacks on sensor data privacy [22, 24]:

- ***Eavesdropping and passive monitoring*:** This is most common and easiest form of attack on data privacy. If the messages are not protected by cryptographic mechanisms, the adversary could easily understand the contents. Packets containing control information in a WSN convey more information than accessible through the location server, Eavesdropping on these messages prove more effective for an adversary.
- ***Traffic analysis*:** In order to make an effective attack on privacy, eavesdropping should be combined with a traffic analysis. Through an effective analysis of traffic, an adversary can identify some sensor nodes with special roles and activities in a WSN. For example, a sudden increase in message communication between certain nodes signifies that those nodes have some specific activities and events to monitor. Deng et al have demonstrated two types of attacks that can identify the base station in a WSN without even underrating the contents of the packets being analyzed in traffic analysis[25].
- ***Camouflage*:** An adversary may compromise a sensor node in a WSN and later on use that node to masquerade a normal node in the network. This camouflaged node then may advertise false routing information and attract packets from other nodes for further forwarding. After the packets start arriving at the compromised node, it starts forwarding them to strategic nodes where privacy analysis on the packets may be carried out systematically. It may be noted from the above discussion that WSNs are vulnerable to a number of attacks at all layers of the TCP/IP protocol stack. However, as pointed out by authors in [16], there may be other types of attacks possible which are not yet identified. Securing a WSN against all these attacks may be a quite challenging task.

IV. SECURITY MECHANISMS FOR WIRELESS SENSOR NETWORKS

It is important to select the most appropriate cryptographic method because all the security requirements 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. However, sensor nodes are limited in their computational and memory capabilities, so the traditional cryptographic techniques cannot be simply transferred to WSNs. Consequently, to

meet the above mentioned security requirements, either the existing techniques have to be adapted or novel techniques have to be developed. Based on the existing cryptographic techniques, we can classify them into three classes: symmetric cryptographic techniques, asymmetric cryptographic techniques and hybrid cryptographic techniques. Asymmetric cryptographic techniques can further be classified into three classes: RSA based techniques, ECC based techniques and pairing based techniques. In this section we discuss the various types of cryptographic techniques evaluated for wireless sensor networks until now.



V. APPLICATIONS OF WSN

Following are some of salient areas of applications of WSN:

Military Applications

Sensor nodes admit battlefield surveillance ,monitoring, and also lets in guiding systems of intelligent missiles and sensing of attack by weapons of mass wipeout.

Medical Application

Sensors can be wear by patient which will highly useful in patient diagnosis and monitoring Sensor devices will monitor the patient's physiological data such as heart rate, temperature, etc.

Environmental Applications

It includes Flood Detection, Precision Agriculture, traffic, Wild fire etc.

Industrial Applications

It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc.

Infrastructure Protection Application

It includes power grids monitoring, water distribution monitoring etc.routing of sensor networks is based on connectionless protocols and thus inherently.

VI. PROPOSED SECURITY SCHEMES

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.

6.1 Security scheme for wireless sensor networks:

Network sniffing (Eves dropping) is a network layer attack consisting of clicking packets from the network to transmit by the other's computer and reading the data context in search of sensitive information.

Like passwords, session tokens on any kind of confidential information.

The attack could be done using tools called network sniffers. These tool collect packets on the network and depends on Quality of tool

Propose wireless intrinsic secrecy mechanism for sensor network which uses an efficient symmetric key encryption protocol which is used to minimize the attacks of network sniffing.

6.2 Intrinsic Secrecy in wireless Sensor Networks

A Intrinsic approach improves the performance of wireless sensor networks with respect to security under changing environmental conditions. The Intrinsic approach of security concern about only focusing on free from eavesdropping attack.

6.3. Free from Eavesdropping

With the advancement in wireless technology, people and organizations have become highly dependent on wireless form of communication. More and More wireless applications are emerging that require transmission of private data. Such as Net banking via wireless access point and mobile payment using device to device link.

It is highly essential to prevent this private data from eavesdropping attack, which becomes difficult in a wireless communication due to its inherent broadcast nature. Even though the existing cryptographic techniques have improved significantly to ensure a secure communication, there are still many issues associate with them which has resulted in the introduction of network security pardigram for wireless network called intrinsic secrecy.

VII. CONCLUSION

The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. Consequently, many innovative security protocols and techniques have been developed to meet this challenge. There are many ways to provide secrecy, one is cryptography. Selecting the most appropriate cryptography method for sensor nodes is fundamental to provide security provider in WSNs. This paper summarizes the attacks and their classifications in wireless sensor networks. This will hopefully motivate future researchers to come up with smarter and more robust security mechanisms and make their network protector.

REERENCES

[1] Hill, J., R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. 2000. “System Architecture Directions for Networked Sensors.” In *Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems,* 93-104, New York : ACM Press.

[2] Slijepcevic, S., M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava. June 2002. “On Communication Security in Wireless Ad-hoc Sensor Networks.” In *Proceedings of 11th IEEE International Workshop on Enabling Technologies: Infrastruture for Collaborative Enterprises (WETICE’02),* 139-144, Pittsburg, Pennsylvania, USA.

[3] Yuan L., and G. Qu. July 2002. “Design Space Exploration for Energy-Efficient Secure Sensor Networks.” In *Proceedings of IEEE International Conference on Application-Specific Systems, Architectures, and Processors(ASAP’02)*, 88-100, San Jose, California, USA.

[4] URL:http://www.willow.co.uk/html/telosb_mote_platform.html. 2010. (Accessed on July 11, 2012).

[5] Perrig, A., R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. 2002. “SPINS: Security Protocols for Sensor Networks.” *Wireless Networks*, 8 (5): 521-534.

[6] J.A. Stankovic, J. A. , T. Abdelzaher, C. Lu, L. Sha, and J. Hou. July 2003. “Real-Time Communicationand Coordination in Embedded Sensor Networks.” In *Proceedings of the IEEE,* 91(7): 1000-1022.

[7] Eschenauer L., and V. D. Gligor. November 2002. "A Key-Management Scheme for Distributed Sensor Networks." In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02),* 41-47, Washington DC, USA.

[8] Chan, H., A. Perrig, and D. Song. May 2003. Random Key Pre-Distribution Schemes for Sensor Networks." In *Proceedings of the IEEE Symposium on Security and Privacy (S&P'03)*, 197, Berkeley, California, USA.

[9] Hwang J., and Y. Kim. 2004. "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),* 43-52, ACM Press, New York.

[10] Liu, D., P. Ning, and R. Li. 2005. "Establishing Pairwise Keys in Distributed Sensor Networks." *ACM Transactions on Information Systems Security*, 8 (1): 41-77.

[11] Anderson, R., and M. Kuhn.1997. "Low Cost Attacks on Tamper Resistant Devices." In Proceedings of the 5th International Workshop on Security Protocols (IWSP), Lecture Notes in Computer Science(LNCS), Vol 1361, 125-136.

[12] Hartung, C., J. Balasalle, and R. Han. 2004. "Node Compromise in Sensor Networks: The Need for Secure Systems." Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, Colorado, USA.

[13] Hu L., and D. Evans. February 2004. "Using Directional Antennas to Prevent Wormhole Attacks." In *Proceedings of the 11th Annual Network and Distributed System Security Symposium(NDSS'04)*, 131-41, San Diego, California, USA.

[14] Komerling O., and M. G. Kuhn. 1999. "Design Principles for Tamper-Resistant Smart Card Processors." In *Proceedings of USENIX Workshop on Smartcard Technology*, 9-20, Chicago, Illinois, USA.

[15] Sastry, N., U. Shankar, and D. Wagner. September 2003. "Secure Verification of Location Claims." In *Proceedings of the 2nd ACM Workshop on Wireless Security*, 1-10, Sandiego, California, USA.

[16] Seshadri, A., A. Perrig, L. Van Doorn, and P. Khosla. May 2004. "SWATT: Software-Based Attestationfor Embedded Devices." In *Proceedings of the IEEE Symposium on Security and Privacy*, 272-282, Oakland, California, USA.

[17] Wang, X., W. Gu, S. Chellappan, K.Schoseck, and D. Xuan. May 2005. "Lifetime Optimization of Sensor Networks under Physical Attacks." In *Proceedings of IEEE International Conference onCommunications(ICC)*, Vo 5, 3295-301.

[18] Wang, X., W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii. February 2005. "Search-Based Physical Attacks in Sensor Networks: Modeling and Defense." Technical Report, Department of Computer Science and Engineering, Ohio State University.

[19] Wood A. D., and J.A. Stankovic. 2002. "Denial of Service in Sensor Networks." *IEEE Computer*, 35(10), 54-62.

[20] Carman, D. W., P. S. Krus, and B. J. Matt. 2000. "Constraints and Approaches for Distributed Sensor Network Security." Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, USA.

[21] Parno, B., A. Perrig, and V. Gligor. May 2005. "Distributed Detection of Node Replication Attacks in Sensor Networks." In *Proceedings of the IEEE Symposium on Security and Privacy (S&P'05),* 49-63, Oakland, California, USA.

[22] Gruteser, M., G. Schelle, A. Jain, R. Han, and D. Grunwald. May 2003. "Privacy-Aware Location Sensor Networks." In *Proceedings of the 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX),* Vol 9, 28, Lihue, Hawaii, USA.

[23] Ozturk, C., Y. Zhang, and W. Trappe. October 2004. "Source-Location Privacy in Energy-Constrained Sensor Network Routing." In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN'04),* 88-93, Washington DC, USA.

[24] Chan H., and A. Perrig. 2003. "Security and Privacy in Sensor Networks." *IEEE Computer Magazine*, 36 (10): 103-105.

[25] Deng, J., R. Han, and S. Mishra. 2004. "Countermeasures against Traffic Analysis in Wireless Sensor Networks." Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.

AUTHOR PROFILE

L.RAMESH received the B.Sc(CS). and M.Sc(CS) Degrees from Bharathiar University,Coimbatore,Tamilnadu, India, in 2012 and 2014 respectively,currently he doing his research in a broad field of Network security in Government Arts College, Coimbatore.

Dr.A.Marimuthu MCA., M.Phil., MBA(Systems)., Ph.D.., received his UG and PG Degree from Gobi Arts and Science college, Bharathiar University, Tamilnadu, India. Received his MBA (Systems) Degree from Periyar University, Salem,India. Received his Ph.D Degree from Vinayaga Mission University, India. He had 20 years of teaching experience and 10 years of Research experience. He has attended, presented and published more than 20 research paper in various national and international conferences and journals. Professional activities include guided various projects for MCA, M.Sc Computer Science and M,Sc Information Technology Students. He has produced 15 M.Phil Scholars. Currently eight Ph.D scholars are pursuing their research program in Computer Science under his Supervision.

