International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 1 Issue 1, November 2015 pp. 20-27
http://www.ijcter.com

A SERVEY ON WIRELESS SENSOR NETWORK SECURITY ISSUES & CHALLENGES

Vivek Sharma[1], Manoj Tripathi[2]

[1,2]*Allahabad University*

Abstract - A Wireless Sensor Network (WSN) is an evolving technology and getting significant attention due to its unlimited potential starts from domestic application to battlefield. Wireless Sensor Networks(WSN) are a most challenging and emerging technology for the research due to their vital scope in the field coupled with their low processing power and associated low energy. Today wireless sensor networks are broadly used in environmental control, surveillance tasks, monitoring, tracking and controlling etc. Sensor nodes are tiny, cheap, disposable and self-contained battery powered computers, known as "motes", which can accept input from an attached sensor, process this input data and transmit the results wirelessly to the transit network. Due to the various applications of WSN in homeland security and military, security is the major issue to be taken care of. In this paper we discuss about The combination of these factors demands security for sensor networks at design time to ensure operation safety, secrecy of sensitive data, and privacy for people in sensor environments. Broadcast authentication is a critical security service in sensor networks; it allows a sender to broadcast messages to multiple nodes in an authenticated way. µ TESLA and multi-level µTESLA have been proposed to provide such service for sensor networks.
Keywords-WSN, Security, Attacks, µTESLA

I. INTRODUCTION

Wireless sensor networks are collection of nodes where each node has its own sensor, processor, transmitter and receiver and such sensors usually are low cost devices that perform a specific type of sensing task. Being of low cost such sensors are deployed densely throughout the area to monitor specific event. The wireless sensor networks mostly operate in public and uncontrolled area; hence the security is a major challenge in sensor applications. A sensor node usually has one or a few sensing components, which sense physical phenomenon (e.g., temperature) from its immediate surroundings, and a processing and communication component, which performs simple computation on the sensed data and communicates with base stations as well as other nodes through its immediate neighbor nodes. The control nodes may further process the data collected from sensor nodes, disseminate control commands to sensor nodes, and connect the network to a traditional wired senders [1].

Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. We discuss these issues and challenges in this paper. To address the critical security issues in wireless sensor networks we talk about cryptography and some other techniques regarding application layer.

II. APPLICATION OF WSN

Wireless Sensor Nodes are used in vast area. Here we conclude main area of the applications of WSN.

A. The Military Applications

@IJCTER-2015, All rights Reserved

The military application of sensor nodes includes battlefield surveillance and monitoring, guiding systems of intelligent missiles and detection of attack by weapons of mass destruction [4].

B. The Medical Application

Sensors can be extremely useful in patient diagnosis and monitoring [9]. Patients can wear small sensor devices that monitor their physiological data such as heart rate or blood pressure [4].

C. Industrial Applications

It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc. [4]

III. ATTACKS ON WSN

Wireless sensor networks use layered architecture like wired network architecture. Based on each and every layer WSN faces different attacks .The various attacks violate the sensitivity and security of WSN. The various attacks are explained below.

A. Denial of service

This type of attack results into making unavailable the resources to their intended users. As an example node A sends request to node B for communication and node B sends acknowledge to node A but A keeps on sending request to B continuously. As a result B is not able to communicate with any other nodes and thus becomes unavailable to all of them.

Denial of service attack may also occur at physical layer by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and unfairness in use of networks. In network layer, it occurs by way of neglecting and the greediness of packets resulting into path failure. In transport layer, DOS attack occurs due to flooding and de-synchronization. Most of denial of service attacks may be prevented by powerful authentication and identification mechanisms.

B. Sybil attack

In this attack the attacker gets illegally multiple identities on one node. By this, the attacker mostly affects the routing mechanism. Sybil attacks are generally prevented by validation techniques.[1]

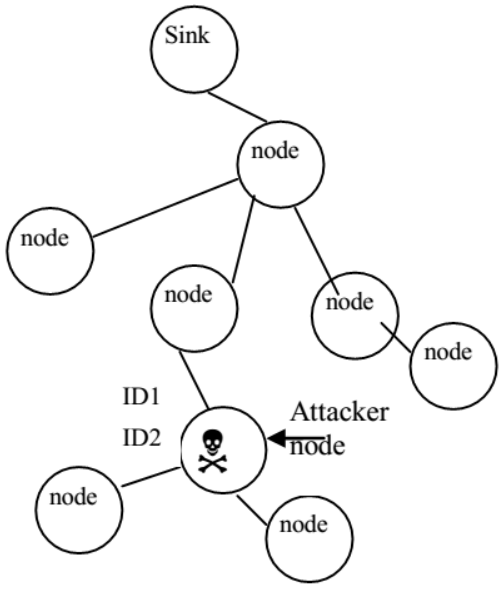

Figure 1: Sybil Attack

B. Node Capturing

A particular sensor might be captured, and information stored on it might be obtained by an adversary.

C. Blackhole / Sinkhole Attack:

In this type of attack, attacker places himself in a network with high capability resources (high processing power and high band width) by which it always creates shortest path. As a result, all data passes through attacker's node [1]. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

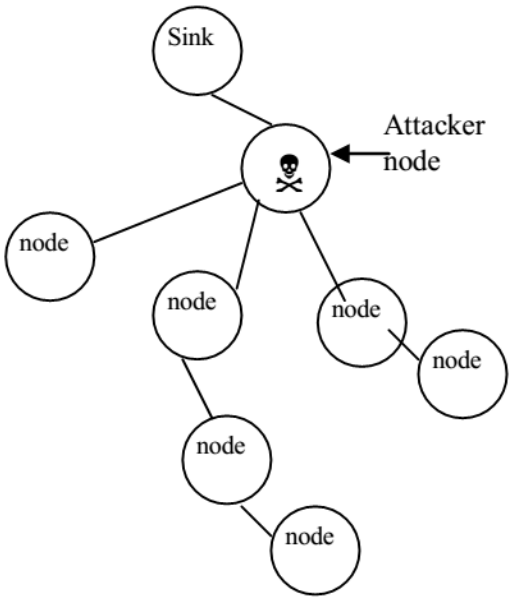

Figure 2: Blackhole/S sinkhole Attack

D. 'Hello flood' Attack

This is one of the simplest attack in wireless sensor networks in which attacker broadcasts HELLO packets with high transmission power to sender or receiver. The nodes receiving the messages assume that the sender node is nearest to them and sends packets by this node. [1] By this attack congestion occurs in the network. This is a specific type of DOS. Blocking techniques are used to prevent Hello Flood attacks.[1]

E. *Wormhole Attack*

In this type of attack, the attacker uses tunneling mechanism to establish himself between them by confusing the routing protocol. Figure 4 shows mechanism of wormhole attack let Y wants to send data by way of broadcasting before sending the data to find path. However the attacker introduces himself as a node X and sends acknowledgement to Y. Y sends data to X that is received by and sends that data to X by tunneling, hiding its own identity. In this case X and Y are not in a single hop but they think they are in a one hop range. The attacker thus may destroy security by interruption, interception, modification and fabrication. [1]

@IJCTER-2015, All rights Reserved

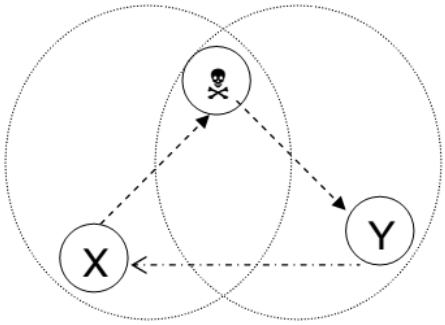

Figure 3: Wormhole Attack

F. 'Hello flood' Attack

This is one of the simplest attack in wireless sensor networks in which attacker broadcasts HELLO packets with high transmission power to sender or receiver. The nodes receiving the messages assume that the sender node is nearest to them and sends packets by this node. By this attack congestion occurs in the network. This is a specific type of DOS. Blocking techniques are used to prevent Hello Flood attacks.

G. Passive Information Gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields.

H. False or Malicious Node

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network.

II. PROPOSED SECURITY SCHEMES AND RELATED WORK

A. Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors' longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks .Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network.

B. SPINS security building blocks

We design two security building blocks: SNEP and µTESLA.µTESLA provides authentication for data broadcast. We bootstrap the security for both mechanisms with a shared secret key between each node and the base station.

@IJCTER-2015, All rights Reserved

1. SNEP

SNEP provides a number of unique advantages. First, it has low communication overhead; it only adds 8 bytes per message. Second, like many cryptographic protocols it uses a counter, but we avoid transmitting the counter value by keeping state at both end points. Third, SNEP achieves semantic security, a strong security property which prevents eavesdroppers from inferring the message content from the encrypted message (see discussion below). Finally, the same simple and efficient protocol also gives us data authentication, replay protection, and weak message freshness. Data confidentiality is one of the most basic security primitives and it is used in almost every security protocol. A simple form of confidentiality can be achieved through encryption, but pure encryption is not sufficient. Another important security property is semantic security, which ensures that an eavesdropper has no information about the plaintext, even if it sees multiple encryptions of the same plaintext. For example, even if an attacker has an encryption of a 0 bit and an encryption of a 1 bit, it will not help it distinguish whether a new encryption is an encryption of 0 or 1. A basic technique to achieve this is randomization: Before encrypting the message with a chaining encryption function (i.e. DES-CBC), the sender precedes the message with a random bit string. This prevents the attacker from inferring the plaintext of encrypted messages if it knows plaintext–cipher text pairs encrypted with the same key. Sending the randomized data over a wireless channel, however, requires more energy. So we construct another cryptographic mechanism that achieves semantic security with no additional transmission overhead. We use two counters shared by the parties (one for each direction of communication) for the block cipher in counter mode (CTR) A traditional approach to manage the counters is to send the counter along with each message. But since we are using sensors and the communicating parties share the counter and increment it after each block, the sender can save energy by sending the message without the counter. At the end of this section we describe a counter exchange protocol, which the communicating parties use to synchronize (or re- synchronize) their counter values. To achieve two-party authentication and data integrity, we use a message authentication code (MAC).The complete message that, A sends to B is:

$$A \rightarrow B: (D)\{KAB,C\}, MAC(K|AB,C\| (D)\{KAB,CA\})$$

Semantic security is provided with the counter each message is encrypted differently. Data Freshness is provided with the help of counter that each data is different.

2. µTESLA overview

Authenticated broadcast requires an asymmetric mechanism; otherwise any compromised receiver could forge messages from the sender. Unfortunately, asymmetric cryptographic mechanisms have high computation communication, and storage overhead, making their usage on resource constrained devices impractical. µTESLA overcomes this problem by introducing asymmetry through a delayed disclosure of symmetric keys, which results in an efficient broadcast authentication scheme. We first explain µTESLA for the case where the base station broadcasts authenticated information to the nodes. Later we discuss the case where the nodes are the sender. µTESLA requires that the base station and nodes be loosely time synchronized, and each node knows an upper bound on the maximum synchronization error. [2]

To send an authenticated packet, the base station 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 (based on its loosely synchronized clock, its maximum synchronization error, and the time schedule at which keys are disclosed). 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]. The node stores the packet in a buffer. At the time of key disclosure, the base station broadcasts the verification key to all the receivers. At the time of key disclosure, the base station broadcasts the verification key to all receivers. When a node

@IJCTER-2015, All rights Reserved

receives the disclosed key, it can verify the correctness of the key (which we explain below). If the key is correct, the node can now use it to authenticate the packet stored in its buffer.

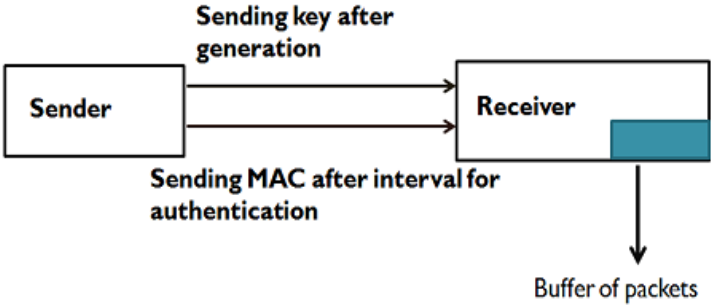

Figure 4: Overview of TESLA mechanism

3. Multilevel µTESLA Mechanism

A multi-level µ TESLA technique is proposed to ex- tend the capabilities of µ TESLA [3, 4]. The basic idea is to construct a multi-level µ TESLA structure, where any higher-level µ TESLA instance is only used to authenticate the commitments of its immediate lower level ones and the lowest level µ TESLA instances are actually used to authenticate the data packets. This extension enables the original µ TESA to be able to cover a long time period and support a large number of receivers [3].Assume a sensor network application requires µ TESLA instances, which may be used by different senders during different periods of time. For convenience, assume m = 2 k, where k is an integer. Before deployment, the central server pre computes µ TESLA instances, each of which is assigned a unique, integer-valued ID between 1 and m. For the sake of presentation, denote the parameters (i.e., the key chain commitment, starting time, duration of each µ TESLA interval, etc.) of the ith µ TESLA instance as Si. Suppose the central server has a hash function H. The central server then computes Ki = H (Si) for all i ∈ {1,..., m}, and constructs a Merkle tree [8] using {K1,...,Km} as leaf nodes. Specifically, K1,...,Km are arranged as leaf nodes of a full binary tree, and each non-leaf node is computed by applying H to the concatenation of its two children nodes.

We refer to such a Merkle tree as a parameter distribution tree of parameters {S1,...,Sm}. Figure 1 shows a parameter distribution tree for eight µ TESLA instances, where K1 = H(S1), K12 = H(K1||K2), K14 = H(K12||K34), etc. The central server also constructs a parameter certificate for each µ TESLA instance. The certificate for the ith µ TESLA instance consists of the set Si of parameters and the values corresponding to the siblings of the nodes on the path from the ith leaf node to the root in the parameter distribution tree.

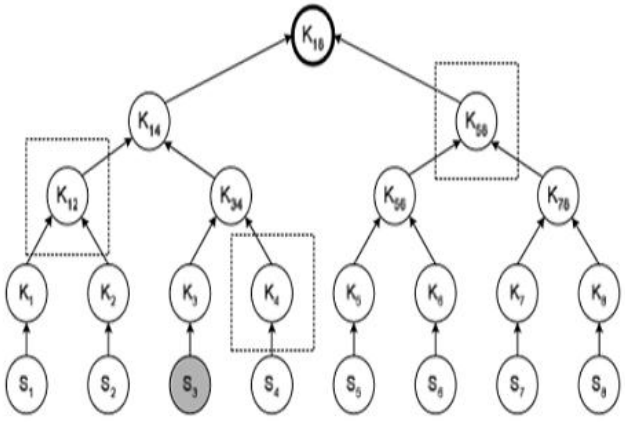

Figure 5: Parameter Distribution Tree

For example, the parameter certificate for the 3rd µ TESLA instance in Figure 5 is ParaCert3 = {S3,K4,K12,K58}. For each sender that will use a given µ TESLA instance, the central server distributes the µ TESLA key chain (or equivalently, the random number used to generate the key

chain) and the corresponding parameter certificate to the node. The central server also pre-distributes the root of the parameter distribution tree (e.g., K18 in Figure 1) to regular sensor nodes, which are potentially receivers of broadcast messages. When a sender needs to establish an authenticated broadcast channel using the ith µ TESLA instance (during a predetermined period of time), it broadcasts a message containing the parameter certificate ParaCerti. Each receiver can immediately authenticate it with the pre- distributed root of the parameter distribution tree. For example, if ParaCert3 = {S3,K4,K12,K58} is used, a receiver can immediately authenticate it by verifying whether H(H(K12||H(H(S3)||K4))||K58) equals the pre-distributed root value K18. As a result, all the receivers can get the authenticated parameters of this µ TESLA instance, and the sender may use it for broadcast authentication.

III. COMPARISON Multi- level µ TESLA And µTESLA

Compared with the multi-level µ TESLA schemes, the most significant gain of the proposed approach is the removal of the authentication delay in distributing the µ TESLA parameters. The multi-level µ TESLA schemes are subject to DOS attacks against the distribution of µ TESLA parameters because of the authentication delay [3]. Specifically, receivers cannot authenticate parameter distribution messages immediately after receiving them, and thus have to buffer such messages. An attacker may send a large amount of bogus messages to consume receivers' buffers and thus prevent the receiver from saving the authentic message. To mitigate or defeat such DOS attacks, the multi-level µ TESLA schemes either use duplicated copies of distribution messages along with a multi-buffer, random selection strategy, or require substantial pre-computation at the sender.

In contrast, the proposed approach does not have these problems. With the proposed approach, senders may still duplicate parameter distribution messages to deal with communication failures. How- ever, unlike multi-level µ TESLA schemes, a sender does not have to compete with malicious attackers, since it can immediately authenticate the parameter distribution message instead of keeping it in the buffer for future authentication. In other words, with the proposed approach, it is sufficient for a receiver to receive one copy of each parameter distribution message.

IV. CONCLUSION

There are certain attacks on WSN, depending upon different layers. This paper gives overview of wireless sensor networks, their security issues and generic solutions. Some applications of wireless Sensor network need a secure communication (like battlefield environment). Traditional solutions are discussed which prevents WSN security on application layer. µTESLA scheme is for single sender and multiple receivers but multilevel µTESLA is for multiple senders and receivers both.

REFERENCES

[1] Abhishek Pandey and R.C. Tripathi, " *A Survey on Wireless Sensor Networks Security* ",in International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2, June 2010

[2] ADRIAN PERRIG, ROBERT SZEWCZYK, J.D. TYGAR, VICTOR WEN and DAVID E. CULLER ," SPINS: Security Protocols for Sensor Networks",In [ACM Journal of] Wireless Networks, 8:5,September 2002, pp. 521 -534

[3] Donggang Liu Peng Ning Sencun Zhu Sushil Jajodia , " A Tree-Based µ-TESLA Broadcast Authentication for Sensor Networks", in Proceedings of the 10th Annual Network and Distributed System Security Symposium (NDSS'03), Febru- ary 2003, pp. 263–276.

[4] Kalpana Sharma and M K Ghose," Wireless Sensor Networks: An Overview on its Security Threats" in IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010

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

[6] A.D. Wood and J.A. Stankovic, (2002) "Denial of Service in Sensor Networks," Computer, vol. 35, no. 10, 2002, pp.

54– 62
[7] D. Liu and P. Ning, "Multi-levelμ TESLA: Broadcast authentication for distributed sensor networks," ACM Transactions in Embedded Computing Systems (TECS), vol. 3, no. 4, 2004.
[8] Karlof, N. Sastry, Y. Li, A. Perrig, and J. Tygar, "Distillation codes and applications to dos resistant multicast authentication"," in Proc. 11th Network and Distributed Systems Security Symposium (NDSS), 2004.
[9] Feng Zhao,Leonidas Guibas,,"Wireless Sensor Networks", Morgan Kaufmann Publications.
[10] R. Merkle, "Protocols for public key cryptosystems," in Proceedings of the IEEE Symposium on Research in Secu- rity and Privacy, Apr 1980.
[11] Applications of Wireless Applications of Wireless Sensor Networks Sensor Networks Kuei-Ping Shih, http://wireless.cs.tku.edu.tw/~kps

@IJCTER-2015, All rights Reserved