Abstract

Wireless Sensor Networks (WSNs) consist of low power, low-cost smart devices which have limited computing resources. With a widespread growth of the applications of WSN, the security mechanisms are also a rising big issue. A lot of real world applications have already been deployed and many of them will be based on wireless sensor networks. These applications include geographical monitoring, medical care, manufacturing, transportation, military operations, environmental monitoring, industrial machine monitoring, and surveillance systems. This paper discusses typical constraints, security goals, threat models and typical attacks on sensor networks and their defensive techniques or countermeasures relevant to the sensor networks, including security methods. The most critical area prone to attack is nearby the base station as the data is more aggregated, that should be kept secure using a number of defensive techniques as stated. This need has existed in military communications for thousands of years. In this paper, we focus on network protocols that provide security services. Wireless sensor network is an emerging technology that shows applications both for public as well as military purposes. Monitoring is one of the main applications. A large amount of redundant data is generated by sensor nodes. This paper compares all the protocols which are designed for security of wireless sensor network on the basis of security services and propose an improved protocol that reduces communication overhead by removing data redundancy from the network.


1. INTRODUCTION

An ideal sensor network protocol should provide data authentication, confidentiality, integrity of data and protection from replay. The security and efficiency being the basic parameters used to design a new sensor network protocol. A wireless sensor node integrates one or more sensors, a processor, a communication unit, a power supply and management unit and, if need be, a security and actuation unit [2]. Depending on the sensing task for which the network is deployed, there can be multiple sensors integrated within a single node. A WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm. Wireless
sensor network is one of the most exciting and challenging research areas. The important functions which need to be monitored are the communicated data between each node, the movement of nodes, etc. In recent years, the sensor has made a great progress. Sensor networks have been gaining popularity as a low cost solution to the various applications. Their low cost gives an opportunity to exploit them in the military, industrial and home applications. Sensors have started replacing the human factor in various industrial processes. These small embedded systems have become an integral part of large networks and participate in the distributed applications. As our daily life is getting more advanced, a variety of “sensitive” data used is stored, altered, manipulated, or communicated by the means of electronic systems. Hence, arises the need to deal with the security of these systems as an important aspect. Security has been the topic of research for cryptography, computing, and networking applications. As a matter of fact, security is a metric, which has to be, implemented at each increasing step in the system design, keeping in mind other factors such as development cost, performance, and power consumed. Security is a requirement for an increasing number of growing embedded system applications ranging from low-end products such as PDAs, wireless handsets, smart id-cards, to high-end products such as routers, firewalls, gateways, storage and web-servers. A survey among internet users has rated security as a primary concern in the adoption of new services and applications. Sensor nodes are used in a variety of applications which require constant monitoring and detection of specific events.

2 Security Requirements

2.1 Confidentiality
Confidentiality means keeping information secret from unauthorized parties. A sensor network should not leak sensor readings to neighboring networks. The confidentiality objective is required in sensors environment to protect information traveling between the sensor nodes of the network or between the sensors and the base station from disclosure, since an adversary having the appropriate equipment may eavesdrop on the communication. By eavesdropping, the adversary could overhear critical information such as sensing data and routing information.

2.2 Authentication
In a sensor network, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. As in conventional systems, authentication techniques verify the identity of the participants in a communication, distinguishing in this way legitimate users from intruders. In the case Could not be predicted, and most of the times the mission of WSN will not be accomplished as expected. node and base station to have the ability to verify that the data received was really sent by a trusted sender and not by an adversary that tricked legitimate nodes of sensor networks, it is essential for each sensor into accepting false data. If such a case happens and false data are supplied into the network, then its behavior

2.3 Integrity
Data integrity ensures the receiver that the received data is not altered in transit by an adversary. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous, for example, for the healthcare sector where lives are endangered. Integrity controls must be implemented to ensure that information is not altered in any unexpected way.

2.4 Freshness
One of the many attacks launched against sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network. Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. To achieve freshness, network protocols must be designed in a way to identify duplicate packets and discard them preventing potential mix-up.

2.5 Availability
Availability ensures that services and information can be accessed at the time they are required. In sensor networks there are many risks that could result in loss
of availability such as sensor node capturing and denial of service attacks. The availability of a sensor and sensor network may decrease for the following reasons [1]:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.

Attacks

Attacks against wireless sensor networks are categorized as invasive or non-invasive. Non-invasive attacks generally consist of side channel attacks such as power, timing or frequency based attacks. There is not much work published about side channel attacks that target WSN specifically, but many of the problems found with other embedded systems, such as timing attacks against MAC generation or encryption, could be used against sensor nodes. Invasive attacks are much more common and the more important of these are described in the following sections. Several attacks on sensor networks are listed as follows:

A. Denial-of-Service (DoS) attack

In the denial-of-Service (DoS) attack, the hacker's objective is to render target machines inaccessible by legitimate users. There are two types of DoS attacks:

- Passive attack: Selfish nodes use the network but do not cooperate, saving battery life for their own communications, they do not intend to directly damage other nodes.
- Active attack: Malicious nodes damage other nodes by causing network outage by partitioning while saving battery life is not a priority. Dos attacks can happen in multiple WSN protocols layers. At physical layer, the DoS attack could be jamming and tempering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer, this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

B. Attacks on Information in Transit

The most common attacks against WSNs are on information in transit between nodes. Information in transit is vulnerable to eavesdropping, modification, injection that can be prevented using well established confidentiality, authentication, integrity and replay protection protocols. Traffic analysis can potentially be a big problem in WSNs allowing an attacker to map the routing layout of a network, enabling very tightly targeted attacks to disrupt chosen Portions of a network for greatest effect.

C. Node Replication Attack

A node replication attack involves an attacker inserting a new node into a network which has been cloned from an existing node, such cloning being a relatively simple task with current sensor node hardware. This new node can act exactly like the old node or it can have some extra behavior, such as transmitting information of interest directly to the attacker. A node replication attack is serious when the base station is cloned. However, as for many deployments, the base station is both in a secure location and much more powerful than the rest of the sensor nodes, so cloning is much more difficult.

D. Routing attack

As with almost all networks there are a number of attacks that target the routing protocol of WSNs, all of which are necessarily insider attacks. Some are as follows:

- Selective forwarding

Selective forwarding is a way to influence the network traffic by believing that all the participating nodes in network are reliable to forward the message. In selective forwarding attack, malicious nodes simply drop certain messages instead of forwarding every message. Malicious or attacking nodes can refuse to route certain messages and drop them. If they drop all the packets through them, then it is called a blackhole attack. However, if they selectively forward the packets, then it is called selective forwarding. Effectiveness of this attack
depends on two factors. First the location of the malicious node, the closer it is to the base station the more traffic it will attract. Second is the percentage of messages it drops. When selective forwarder drops more messages and forwards less, it retains its energy level thus remaining powerful to trick the neighboring nodes.

b. Sinkhole attacks
In sinkhole attacks, adversary attracts the traffic to a compromised node. The simplest way of creating sinkhole is to place a malicious node where it can attract most of the traffic, possibly closer to the base station or malicious node itself deceiving as a base station. One reason for sinkhole attacks is to make selective forwarding possible to attract the traffic towards a compromised node. The nature of sensor networks where all the traffic flows towards one base station makes this type of attacks more susceptible.

c. Sybil attacks
In Sybil attack, a single node presents multiple identities to all other nodes in the WSN. This may mislead other nodes, and hence routes believed to be disjoint w.r.t node can have the same adversary node. Sybil attacks can be used against routing algorithms and topology maintenance; it reduces the effectiveness of fault tolerant schemes such as distributed storage and dispersity. Another malicious factor is geographic routing where a Sybil node can appear at more than one place simultaneously.

d. Wormholes
In wormhole attacks, an adversary positioned closer to the base station can completely disrupt the traffic by tunneling messages over a low latency link. Here an adversary convinces the nodes which are multi hop away that they are closer to the base station. This creates a sinkhole because adversary on the other side of the sinkhole provides a better route to the base station.

e. Flooding
Sometime, the malicious node can cause immense traffic of useless messages on the network. This is known as the flooding. Sometimes, malicious nodes replay some actual broadcast messages, and hence generating useless traffic on the network. This can cause congestion, and may eventually lead to the exhaustion of complete nodes. This is a form of Denial of Service attack. Security in wireless sensor networks is a critical issue keeping in view limitations and application domains of sensor networks. In sensor networks there is need to maintain a delicate balance between security and network operations. The techniques such as Link Layer encryption and authentication, multipath routing, identity verification and authenticated broadcast seem to be good solution for security in WSN. However attacks such as Sinkhole and Wormholes pose lot of challenges to secure routing protocol design. Geographical Routing Protocols is one example of routing protocols which are able to withstand most of the WSN routing based attacks, as the legitimate nodes are able to estimate the location of the adversary nodes. Hence attacks such as Sybil are effective. Effective and Efficient countermeasures are still lacking against these attacks, which can be applied after the design of these routing protocols has completed. So there exist a severe need to design such routing protocols in which these attacks are ineffective.

3. SECURITY SOLUTIONS IN SENSOR NETWORKS

Security schemes can be applied to provide security in wireless sensor networks, but keeping in view their resource starved nature it is very difficult to do so. Some researchers are striving to develop improved WSN protocols, others are attempting to improve node design; still others are working to resolve security issues including the main WSN security threat of insecure radio links with eavesdropping and information corruption possible. Most security Mechanisms that exist today require intensive computation and memory which is the limiting factor in wireless sensor networks. Many security mechanisms require repeated transmission/communications between the sensor nodes which are further drawn in their resources. The number of security suites already exists that are at least some way appropriate for use in WSNs, and combat some of the threats to these networks. This section review some of the more popular and more suitable solutions here.
3.1 SPINS: Security Protocols For Sensor Networks
Adrian Perrig et al.[5] proposed “SPINS” a suite of security protocols optimized for sensor networks. SPINS has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments.

3.1.1 SNEP: Sensor Network Encryption Protocol
SNEP provides a number of advantages.
1. It has low communication overhead as it only adds 8 bytes per message.
2. Like many cryptographic protocols it uses a counter, but avoids transmitting the counter value by keeping state at both end points.
3. SNEP achieves semantic security, which prevents eavesdroppers from inferring the message content from the encrypted message.
4. Finally, SNEP protocol offers data authentication, replay protection, and weak message freshness. However, sending data over the RF channel requires more energy. So, SNEP construct another cryptographic mechanism that achieves semantic security with no additional transmission overhead. It relies on a shared counter between the sender and the receiver for the block cipher in counter mode (CTR). Since the communicating parties share the counter and increment it after each block, the counter does not need to be sent with the message. To achieve two-party authentication and data integrity, SNEP uses a message authentication code (MAC). The combination of these mechanisms form Sensor Network Encryption Protocol SNEP.

3.1.2 μTesla: Authenticated Broadcast
Asymmetric digital signatures are impractical for sensor networks for the authentication, as they require long signatures with high communication overhead of 50-1000. Earlier TESLA protocol provided efficient authenticated broadcast. However, TESLA was not designed for sensor networks. Adrian Perrig et al. proposed μTESLA to solve the following inadequacies of TESLA in sensor networks:
• TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. μTESLA uses only symmetric mechanisms.
• Disclosing a key in each packet requires too much energy for sending and receiving. μTESLA discloses the key once per epoch.
• It is expensive to store a one-way key chain in a sensor node. μTESLA restricts the number of authenticated senders.

3.2 TINYSEC
Karlof et al. designed the replacement for the unfinished SNEP, known as TinySec [6]. Inherently it provides similar services, including authentication, message integrity, confidentiality and replay protection. A major difference between TinySec and SNEP is that there are no counters used in TinySec. For encryption, it uses CBC mode with cipher text stealing, and for authentication, CBC-MAC is used. TinySec XORs the encryption of the message length with the first plaintext block in order to make the CBC-MAC secure for variably sized messages. There are two packet formats defined by TinySec. These are TinySec-AUTH, for authenticated messages, and TinySec-AE, for authenticated and encrypted messages. For the TinySec-AE packet, a payload of up to 29 Bytes is specified, with a packet header of 8 Bytes in length. Encryption of the payload is all that is necessary, but the MAC is computed over the payload and the header. The TinySec-AUTH packet can carry up to 29 Bytes of payload. The MAC is computed over the payload and the packet header, which is 4 Bytes long. Generally, the security of CBC-MAC is directly related to the length of the MAC. TinySec specifies a MAC of 4 Bytes, much less than the conventional 8 or 16 Bytes of previous security protocols. In the context of sensor networks, Karlof et al. argue that this is not detrimental. Should an adversary repeatedly attempt blind forgeries, it will succeed after $2^{31}$ attempts. Adversaries can only assess the validity of an attempted forgery by forwarding it to an authorized recipient. This implies that approximately $2^{31}$ packets must be sent to forge just one malicious packet. In sensor networks, this is an adequate level of security, and for an attempt like the one described above, it would take approximately 20 months (on a 19.2kb/s channel) to be successful. Implicitly, there is an effective denial of service attack launched in this way, as the radio channel would be locked for an extended period as attempts are made. It is argued that a simple heuristic, whereby the nodes signal the base station when the
rate of MAC failures exceeds a predetermined threshold would alleviate the problem should such an attack occur.

3.3 MINISEC
MiniSec [7] is a secure network layer protocol that claims to have lower energy consumption than TinySec while achieving a level of security which matches that of Zigbee. A major feature of MiniSec is that it uses offset codebook (OCB) mode as its block cipher mode of operation, which offers authenticated encryption with only one pass over the message data. Normally two passes are required for both secrecy and authentication. Another major benefit of using OCB mode is that the ciphertext is the same length as the plaintext, disregarding the additional fixed length tag, four bytes in MiniSec's case, so padding or ciphertext stealing is not necessary. Another primary feature MiniSec has over the other security suites mentioned here is strong replay protection without the transmission Overhead of sending a large counter with each packet or the problems associated with synchronized counters if packets are dropped. To achieve this MiniSec has two modes of operation, one for unicast packets MiniSec-U, and one for broadcast packets.

3.4 LEAP: Localized Encryption and Authentication Protocol
Sencun Zhu et. al.[8] proposed LEAP Protocol, which is a key management protocol for sensor networks. LEAP is designed to support secure communications in sensor networks; therefore, it provides the basic security services such as confidentiality and authentication. In addition, LEAP is to meet several security and performance requirements that are considerably more challenging to sensor networks. LEAP has the following properties:

- LEAP assumes that no single keying mechanism is appropriate for all the secure communications that are Needed in sensor networks. As such, LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network.

- LEAP includes an efficient protocol for local broadcast authentication based on the use of one-way key chains.

- A distinguishing feature of LEAP is that its key sharing approach supports in-network processing, while restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. LEAP can prevent or increase the difficulty of launching many security attacks on sensor networks. The key establishment and key updating procedures used by LEAP are efficient and the storage requirements per node are small. LEAP is feasible for the current generation sensor nodes.

3.5 ZIGBEE
Zigbee[9] Coordinator acts as “Trust Manager”, which allows other devices to join the network and also distributes the keys. It plays the three roles as follows:

1: Trust manager, whereby authentication of devices requesting to join the network is done,

2: Network manager, maintaining and distributing network keys, and

3: Configuration manager, enabling end-to-end security between devices. It operates in both Residential Mode and Commercial Mode. The Trust Center running Residential Mode is used for low security residential applications. Commercial Mode is designed for high-security commercial applications. There are three types of keys employed, Master Key, Link Key and Network Key. Master keys are installed first, either in the factory or out of band. They are sent from the Trust Center and are the basis for long-term security between two devices. The Link key is a basis of security between two devices and the Network keys are the basis of security across the entire network. Link and Network keys, which are either installed in the factory or out of band, employ symmetrical key-key exchange (SKKE) handshake between devices. The key is transported from the Trust Center for both types of keys. This operation occurs in commercial mode, as residential mode does not allow for Authentication 3.6 802.15.4 The 802.15.4 standard[10] provides link layer security services, and has three modes of operation, unsecured, an Access Control List (ACL) mode and secured mode. In unsecured mode, as the name implies, no security services are provided. In
ACL mode the device maintains a list of devices with which it can communicate. Any communication from devices not on the list is ignored. However, it must be noted that this mode offers no cryptographic security so it is trivial for the message source address to be spoofed. Secured mode offers seven security suites and depending on which is used any of four security services are offered, these being access control, data encryption, frame integrity and sequential freshness. One cryptographic algorithm, AES-128, is employed for all security suites, which allows for a very small implementation. For high security the full 128-bit message integrity code (MIC) can be added to each transmitted message but the MIC can be truncated to 64 or 32 bits to trade security for shorter message length. 802.15.4 Security suites should be implemented on the radio chips all the necessary cryptographic computations are performed in hardware and reduces energy consumption. Some problems were found with security modes at the lower levels but higher level protocols overcome these limitations. Hence, 802.15.4 standard, if implemented correctly, can be used as a good base for building higher level, fully featured security suites.

4. CONCLUSION AND FUTURE WORK
Each of the authentication mechanisms are to be examined in a simulated environment and evaluated under the headings speed of operation, power consumption, efficiency and security level offered. The details for these mechanisms are available in section 3 and in addition a comparison table is given in the Table 4.1 of this paper. This is to further evaluate the effectiveness of these protocols and define their more desirable characteristics. There is currently no one solution that can be plugged-in to an application to provide all the necessary. The future goal of this research is to develop a new authentication protocol, by combining the most desirable traits of what currently exists and implementing some new ideas, which is optimal for implementation in wireless sensor network application security primitives.

| Encryption | Yes | Yes | Yes | Yes | Yes | Yes |
| Freshness (CTR) | Yes | No | No | Yes | Yes | Yes |
| Overhead (Bytes) | 8 | Variable | 4 | 4,8or 16 | 4,8or 16 | 4/3 |
| MAC Used | Yes | Yes | Yes | Yes | Yes | Yes |
| Key Agreement | Symmetric Delayed | Pre-Deployed | ANY | Trust Center | ANY |

| Table 4.1 Comparison Table |

REFERENCES


