Security in Sensor Networks

19

19.1 Introduction

The rapid development of wireless technology in the last few years has created new interest in low-cost wireless sensor networks. Wireless sensor networks (WSNs) or just sensor networks are grids or networks made of spatially distributed autonomous but cooperating tiny devices called sensors, all of which have sensing capabilities that are used to detect, monitor, and track physical or environmental conditions, such as temperature, sound, vibration, pressure, motion, or pollutants, at different locations [1]. A sensor, similar to that in Fig. 19.1, is a small device that produces a measurable response to a change in a physical condition. Sensor nodes can be independently used to measure a physical quantity and to convert it into a signal that can be read by an observer or by an instrument [1]. The network may consist of just a few or thousands of tiny, mostly immobile, usually, randomly deployed nodes, covering a small or large geographic area. In many cases, sensor networks do not require predetermined positioning when they are randomly deployed making them viable for inaccessible terrains where they can quickly self-organize and form a network on the fly.

The use of sensors to monitor physical or environmental conditions is not new. Sensors have been used in both mechanical and electrical systems for a long time. However, what is new and exciting is that the new sensor nodes are now fitted with onboard tiny processors forming a new class of sensors that have the ability to partially process the collected data before sending it to the fusing node or base station. The sensor nodes now also have sophisticated protocols that help in reducing the costs of communications among sensors and can implement complex power saving modes of operations depending on the environment and the state of the network [2]. The accuracy of the data gathered has also greatly improved.

These recent advances have opened up the potential for WSN. According to David Culler et al. [3], wireless sensor networks could advance many scientific pursuits while providing a vehicle for enhancing various forms of productivity, including manufacturing, agriculture, construction, and transportation. In the

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_19

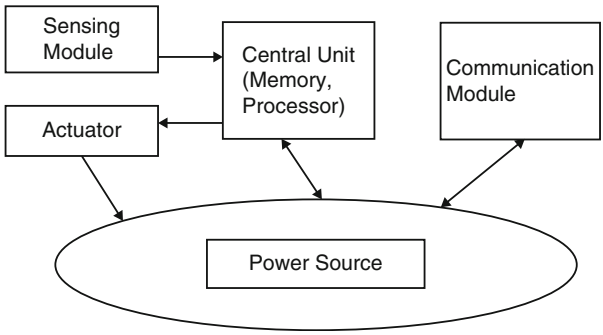

Fig. 19.1 A wireless sensor node

military, they are good for command and control, intelligence, and surveillance. In health, they are beneficial in monitoring patients, and in commercial application they can be used in managing inventory, monitoring production lines and product quality, and monitoring areas prone to disasters [4]. New technologies are creating more powerful and yet smaller devices. This miniaturization trend is leading us to ubiquitous computing capacities that are exponentially faster and cheaper with each passing day. With these developments, researchers are refocusing and developing techniques that use this miniaturization process to build radios and exceptionally small mechanical structures like sense fields and forces in physical environments that could only be imagined just a few years ago. Culler et al. believe that these inexpensive, low-power communication devices can be deployed throughout a physical space, providing dense sensing close to physical phenomena, processing and communicating this information, and coordinating actions with other nodes including a base station [3].

However, as wireless sensor networks with vast potential of applications unfold and their role in dealing with sensitive data increases, the security of these networks has become one of the most pressing issues in further development of these networks. This chapter gives a general discussion of the challenges and limitations of WSNs and how these challenges and limitations contribute to the security problems faced by the sensor network. We survey several interesting security approaches aimed at enhancing security, and we conclude by considering several potential future directions for security solutions.

19.2 The Growth of Sensor Networks

WSNs have evolved slowly from simple point-to-point networks with simple interface protocols providing for sensing and control information and analog signal providing a single dimension of measurement to the current large number and sophisticated wireless sensor node networks. The development of the microprocessor boasted the sensor node with increased onboard intelligence and processing capabilities, thus providing it with different computing capabilities. The sensor node is now a microprocessor chip with a sensor on board. The increased

intelligence in the node and the development of digital standards such as RS-232, RS-422, and RS-485 gave impetus to the creation of numerous sensor networking schemes [5]. In addition, the popularization of the microcontrollers and the development of BITBUS, a field bus developed by Intel to interconnect stand-alone control units and terminals, thus making them able to interchange data telegrams, further improved the sensor node communication capabilities, thus bringing the dream of sensor networks closer [5].

Another outstanding development that further made the road to fully functioning sensor networks possible was the development of the Manufacturing Automation Protocol (MAP) by General Motors to reduce the cost of integrating various networking schemes into a plant-wide system. As Jay Warrior observes, this further resulted in the development of the Manufacturing Messaging Specification (MMS), a specification that made it possible for the networked nodes to exchange real-time data and supervisory control information [5]. With the development of other communication protocols that allowed simultaneous analog and digital communication for smart instruments, the sensor network, as we know it today, was born. Currently, there is a whole spectrum of different sensor network protocols for the many different types of sensor networks in use today.

19.3 Design Factors in Sensor Networks

Several factors influence the design philosophy of sensor networks. Among these factors are first whether the nodes are stationary or moving and whether the network is deterministic or self-organizing. Most sensor network applications use stationary nodes. However, there are a good number of applications that use mobile nodes. In this case, therefore, the network is bound to use more energy because of the need to track the moving node and the increase in bandwidth requirements for periodic reporting which increases traffic. In a deterministic topology, the positions of the nodes and the routes in the network are predetermined, and the nodes are manually placed. In a self-organizing topology, node positions are random, and the routes are also random and unreliable. Routing in these networks, therefore, becomes the main design concern. Also since self-organizing sensor networks demand a lot of energy, direct routing is not desirable, and multi-hop routing is more energy efficient. However, multi-hop routing requires considerable routing management techniques. In addition to routing and energy, other factors also influence the design philosophy of sensor networks [4]:

19.3.1 Routing

Communication in wireless sensor networks, like in traditional network communication, is based on a protocol stack with several layers as seen in Fig. 19.2. This stack also combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and

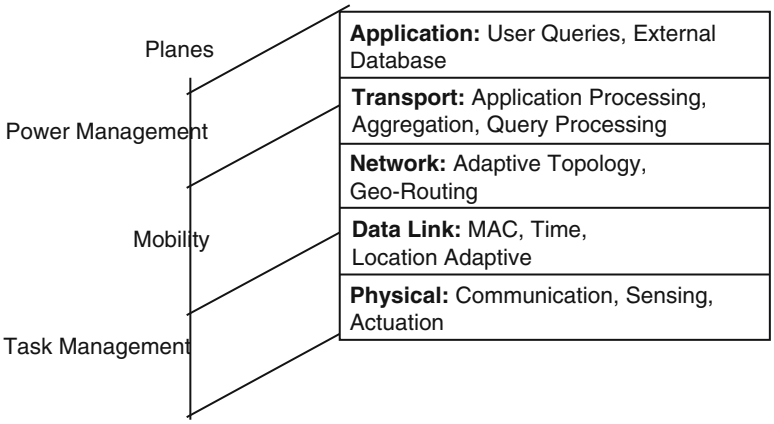

Fig. 19.2 Sensor network protocol stack

promotes cooperation between nodes [4]. To achieve all these, the stack consists of five layers and three management planes, and these are physical layer, data link layer, network layer, transport layer, application layer, power management plane, mobility management plane, and task management plane. This stack is different from those of the traditional networks made of nonsensor nodes like the TCP/IP and the ISO's OSI.

- *Physical layer*—is responsible for several tasks including frequency selection, carrier frequency generation, signal detection, modulation, and data encryption.
- *Data link layer*—is responsible for a number of tasks including multiplexing of data streams, data frame detection, medium access, and error control.
- *Network layer*—is responsible for network routing. Routing in sensor networks, unlike in the traditional networks, is influenced by the following [4]:
  - Power efficiency as an important consideration
  - Sensor networks being mostly data centric
  - Data aggregation being useful only when it does not hinder the collaborative efforts of the sensor nodes
  - An ideal sensor network having attribute-based addressing and location awareness
- *Transport layer*—not yet in place. Because, unlike traditional networks, protocols like TCP where the end-to-end communication schemes are possible, here there is no global addressing. The development of global addressing schemes is still a challenge.
- *Application layer*—also not available. Although there are many application areas for sensor networks, application layer protocols are yet to be developed.

Based on the above discussion, therefore, sensor networks are largely still multi-hop wireless networks whose nodes can be either a host or a router, forwarding

packets to other nodes in the network. In many sensor networks, the information collected from a large number of sensors is either lightly proceeded locally at the node or transmitted un-proceeded to the base station or other sensors using one of the three routing techniques: one-to-many, many-to-one, and one-to-one/point-to-point. However, the two most fundamental communication primitives are broadcast (one-to-many) and point-to-point (one-to-one).

Broadcast Communication The broadcast packet routing technique is used extensively in wireless sensor networks due to the large number of sensor nodes in any wireless sensor network. Broadcasting, as a means of node communication, is highly desirable in this environment because of the limited signal range for each node. In the broadcast mode, the node that initiates the broadcast of a packet is referred to as the source or sender node and all others as receivers. The receivers of broadcast packet then forward the packet to their nearest adjacent neighbors which causes the packet to move throughout the network enabling all network nodes to eventually receive the broadcast packet.

Point-to-Point Communication Though not common, point-to-point routing is still important for many applications in wireless sensor networks, including games based on wireless sensor networks and data-centric storage where nodes store information about the detected events using the geographic location as the key. Point-to-point routing can also be used to send data from the detection node to the storage node [6].

19.3.1.1 Routing Protocols

There are several routing protocols in use today for sensor networks, including data centric, hierarchical, and location based [7].

Data-Centric Routing Because the sensor network may have thousands of nodes which are randomly deployed, it is inconceivable to have network-wide external addressing and network-layer-managed routing protocols found in traditional networks. In data-centric routing, the sink node, desiring data, sends out an attribute-based query to the surrounding nodes in the region. The attributes in the query specify the desired properties of the data. The sink then waits for the data [7]. If each node were to send out data to other nodes in the region, there would result a considerable redundancy of data and an inefficient use of scarce energy. For these reasons, data-centric routing techniques are more resource efficient. Common data-centric routing protocols include sensor protocols for information via negotiation (SPIN) and directed diffusion [7].

Hierarchical Routing Hierarchical routing involves multi-hop communication and the aggregation and fusion of data within clusters of nodes in order to decrease the number of transmitted messages to the sink nodes which leads to conservation of energy. There are several hierarchical protocols in use today, including LEACH, PEGASIS, TEEN, and APTEEN [8].

Location-Based Routing In location-based routing, each node maintains a location list consisting of location information for a number of nodes in a region of a sensor network. Each node periodically updates its location list by receiving information about locations and location lists of all its direct neighbors. It also, in turn, sends its location and location list to all its adjacent nodes. This keeps the location list of all nodes in the region current and up to date.

19.3.2 Power Consumption

Most sensor networks are entirely self-organizing and operate with extremely limited energy and computational resources. Because most nodes may be either in inaccessible environments, replenishing them with new power may be almost impossible. The life of a sensor node, therefore, may be in question, and it may not be able to transmit critical data when desired. The functionality of the network, therefore, depends on the consumption rate of energy by node units.

19.3.3 Fault Tolerance

If a sensor network is to face any one sensor node failure, we would like the network to be able to sustain all its functionalities. That is to say that the sensor network should be as reliable as possible and continue to function as much as possible in light of the failed node.

19.3.4 Scalability

We want to have a network such that the addition of more nodes to the network does not have any diverse effects to the functionality of the network.

19.3.5 Production Costs

Wireless sensor networks most often use large numbers of sensor nodes. The unit cost of each individual sensor node plays a crucial role in determining the overall costs of the entire sensor network. We would like a well-functioning network having a least per unit cost for individual nodes.

19.3.6 Nature of Hardware Deployed

A sensor node consists of four basic parts: the sensing unit, the processing unit, the transceiver unit, and the power unit. All these units must be packaged in a very

small, matchbox-sized package. In addition, all these units and the overall sensor node must consume very low power.

19.3.7 Topology of Sensor Networks

Because a normal sensor network may contain thousands of sensor nodes deployed randomly throughout the field of observation, the wireless sensor network resulting may have uneven densities depending on how the nodes were deployed. Nodes can be deployed by dropping them from a plane, carefully placing them, or dropping by artillery. Also not every deployed sensor may work as expected. So the topology of the resulting network may determine the functionality of the wireless sensor network.

19.3.8 Transmission Media

In a wireless sensor network, the nodes are linked by a wireless medium. The medium could be by radio-like RF and Bluetooth, infrared, or optical waves. Both infrared and optical links require no obstructions like objects in the line of sight. The functionality of the network may depend on these media.

19.4 Security in Sensor Networks

Modern wireless sensor networks many times consist of hundreds to thousands of inexpensive wireless nodes, each with some computational power and sensing capability and usually operating in random unsupervised environments. The sensors in the network act as "sources" as they detect environmental events either continuously or intermittently whenever the occurrence of the event triggers the signal detection process. The data picketed up is either lightly processed locally by the node and then sent off or just sent off to the "sink" node or a base station. This kind of environment presents several security challenges.

19.4.1 Security Challenges

The most pressing of these challenges include the following:

19.4.1.1 Aggregation

Data aggregation in sensor networks is the process of gathering data from different sensor "source" nodes and expressing it in a summary form before it is sent off to a "sink" node or to a base station. There are two types of data aggregation: *in-stream* aggregation, which occurs over a single stream, generally over a time window, and *multi-stream* aggregation, which occurs across the values of multiple streams,

either at the same time or over a time window. Data aggregation is essential in sensor networks because as it combines data from different "source" nodes, it eliminates redundancy thus minimizing the number of transmissions and hence saving energy. In fact, significant energy gains are possible with data aggregation. The gains are greatest when the number of sources is large and when the sources are located relatively close to each other and far from the sink [9]. However, as sensor network applications expand to include increasingly sensitive measurements of everyday life, preserving data accuracy, efficiency, and privacy becomes an increasingly important concern as this is difficult to do with many current data aggregation techniques.

19.4.1.2 Node Capture/Node Deployment

Node compromise is a situation where a sensor node can be completely captured and manipulated by the adversary [10]. The conditions for node compromise are made possible as a result of sensor nodes in a wireless sensor network being randomly deployed many times in inaccessible or hostile environments. Usually these nodes are also unsupervised and unattended. In this kind of environments, nodes are undefendable and easy to compromise or totally captured by an adversary. There are several ways to capture a sensor node. One approach is the physical capture where an adversary can physically capture the node because of the node being in a hostile or unprotected environment. In another approach, software is used. Software-based capture occurs when an attacker uses software like a virus to capture a node.

19.4.1.3 Energy Consumption

Sensor networks are mostly and entirely self-organizing and operate with extremely limited energy and computational resources. Conservation of energy by sensor nodes results in minimizing their transmit power in order to maintain acceptable connectivity. This may prevent the network from maintaining the security solution like good cryptographic algorithms needed to protect critical data.

19.4.1.4 Large Numbers of Nodes/Communication Challenges

Because modern wireless sensor networks consist of hundreds to thousands of inexpensive wireless nodes, this large number of nodes presents a challenge of guaranteeing a secure, reliable, sometimes ad hoc communication among sensor nodes or groups of sensor nodes which sometimes can be mobile units. For example, since sensor nodes are typically battery driven, large numbers of them in a network make it a challenge to find and replace or recharge batteries.

19.4.2 Sensor Network Vulnerabilities and Attacks

Because of these limitations and the high dependency on the physical environment of deployment, sensor networks pose unique challenges that traditional security techniques like secrecy, authentication, privacy, cryptography, and robustness to

denial-of-service attacks used in traditional networks cannot be applied directly [11]. This means that existing security mechanism fit for traditional networks cannot be used wholesale in sensor networks. Yet there are no comprehensive security mechanisms and best practices for sensor networks. One of the reasons why traditional network security mechanisms and best practices fail with sensor networks is because many of these security mechanisms and best practices are taken and viewed as stand-alone. To achieve any semblance of desired security in a sensor network, these security mechanisms and best practices must be a part of and be embedded into every design aspect of the sensor network, including the communication protocols and deployment topologies. For example, we cannot talk about the security of a sensor network if that network lacks secure routing protocols. Secure routing protocols are essential security entities in sensor networks because a compromised routing protocol compromises the network nodes and a single compromised network sensor node completely compromises the entire network. Current sensor network routing protocols suffer from many security vulnerabilities as we will see shortly.

We have established that sensor networks have a number of issues that separate them from traditional networks. Among these are the vulnerability of sensor nodes to physical compromise, significant power and processing constraints, aggregation of node outputs, and compromising individual nodes. Physical vulnerability includes physical node access and compromise or local eavesdropping. Power and processing constraints prevent sensor networks from running good security encryptions. And aggregation of output may grossly obscure the effects of a malicious attack from spreading throughout the network.

Sensor network adversaries target and exploit these weaknesses and other network loopholes embedded within these limitations. Let us look at some of these next.

19.4.2.1 Possible Attacks

There are several possible attack types, including *eavesdropping*, *disruption*, *hijacking*, and *rushing* [12, 13]:

Eavesdropping Here, the attacker (eavesdropper) aims to determine the aggregate data that is being *output* by either the node or the sensor network. The attacker captures the message from the network traffic either by listening for some time to the network traffic transmitted by the nodes or directly compromising the nodes. There are two types of eavesdropping:

- *Passive*: The attacker's presence on the network remains unknown to the sensor nodes and uses only the broadcast medium to eavesdrop on all messages.
- *Active*: The attacker actively attempts to discern information by sending queries to sensors or aggregation points or by attacking sensor nodes.

Disruption The intent of the attacker here is to disrupt the sensor's working. It is usually done in two ways:

- *Semantically*: where the attacker injects messages, corrupts data, or changes values in order to render the aggregated data corrupt or useless. Examples of this type of attacks includes the following [14]:
  - *Routing loop*: where an attacker injects malicious routing information that causes other nodes to form a routing loop causing all packets injected into this loop to go round in circles and eventually resulting into wasting precious communication and battery resources
  - *General DoS attacks*: where an attacker injects malicious information or alters the routing setup messages which end up preventing the routing protocol from functioning correctly
  - *Sybil attack*: where a malicious node influenced by an attacker creates multiple fake identities to perform desired attacks on the network
  - *Blackhole attack*: where a malicious node influenced by the attacker advertises a short distance to all destinations, thus attracting traffic destined to those destinations into the blackhole
  - *Wormhole attack*: where two nodes are caused to use an out-of-band channel to forward traffic between each other, enabling them to mount several other attacks along the way
- *Physically*: where the attacker tries to upsets sensor readings by directly manipulating the environment. For example, generating heat in the vicinity of sensors may result in erroneous values being reported.

Hijacking In this case, the attacker attempts to alter the aggregated output of an application on several network sensor nodes.

Rushing Attack According to YihChun Hu et al. [13], in an on-demand protocol, a node needing a route to a destination floods the network with ROUTE REQUEST packets in an attempt to find a route to the destination. To limit the overhead of this flood, each node typically forwards only one ROUTE REQUEST originating from any Route Discovery. In fact, all existing on-demand routing protocols, such as AODV, DSR, LAR, AODV, and others, only forward the REQUEST that arrives first from each Route Discovery. In the rushing attack, the attacker exploits this property of the operation of Route Discovery. The rushing attack is a very powerful attack that results in denial of service, and it is easy to perform by an attacker.

19.4.3 Securing Sensor Networks

The choice of a good security mechanism for wireless sensor networks depends on network application and environmental conditions. It also depends on other factors like sensor node processor performance, memory capacity, and energy. While in traditional networks, standard security requirements, such as availability, confidentiality, integrity, authentication, and nonrepudiation, are sufficient for security, in sensor networks, special security requirements such as message freshness, intrusion detection, and intrusion tolerance are necessary in addition.

19.4.3.1 Necessary Conditions for a Secure Sensor Network

Any security solution to sensor networks must preserve the confidentiality, integrity, authentication, and nonreplay of data within the network [14, 15].

Data Confidentiality Confidentiality of data in a sensor network is achievable only if those with access to network data are authorized to do so. Under no circumstances should sensor readings leak outside the network. The standard approach for preventing this from happening is to use encryption. This requires the use of a secret key that only intended receivers possess.

Data Integrity The integrity of data in any network means that data in that network is genuine, undiluted without authorization. This implies that data between the sender and the receiver is unaltered in transit by an adversary.

Data Authentication The process of authentication of both network data and users is very important in preserving network data integrity and preventing unauthorized access to the network. Without authenticating mechanisms in place, an attacker can easily access the network and inject dangerous messages without the receivers of the new altered data knowing and making sure that the data being used originates from a malicious source.

Data Freshness/Nonreplay Adrian Perrig et al. [15] define sensor network data freshness to mean recent data which for a sensor network would ensure that no adversary replayed old messages. There are two types of freshness: weak freshness, which provides partial message ordering but carries no delay information, and strong freshness, which provides a total order on a request-response pair and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network [15].

These conditions are essential for the security of sensor networks. The problem that remains is how to ensure that these conditions hold throughout the wireless sensor network. This is still a big challenge and a problem for current research in sensor networks.

19.5 Security Mechanisms and Best Practices for Sensor Networks

We cannot ensure the confidentiality, integrity, authentication, and freshness of data in sensor networks without paying attention to the following issues particular to sensor networks:

- *Data aggregation.* Aggregation is generally consensus-based compromise, where missing readings from one or a few nodes may not significantly affect the overall system. Data aggregation is used in sensor networks to reduce energy consumption. With aggregation, however, raw data items from sensor nodes are

invisible to the base station throwing in doubt the authenticity of the aggregated data. Without securing the data aggregation process, a compromised sensor node may forge an aggregation value and mislead the base station into trusting a false reading.

- *Antijamming*. Attackers can cause denial of service by jamming the base station or any other sensor node in the network. Attackers can also jam sensor radio frequencies. Protocols and services must be in place to stop this from happening.
- *Access control*. Access control is a process of granting the user the access right to the sensor network resources. It is essential to have an effective and efficient access control mechanisms, especially via a base station to authenticate user requests to get access to the network resources.
- *Key management*. Key management is crucial in supporting the basic security tenants like authentication and encryption in sensor networks. As the number of applications for sensor networks grows, an effective key management scheme is required.
- *Link-layer encryption*. Most widely used encryption schemes in sensor networks today involve the use of pre-distribution of key broadcasts by sensor nodes to thousands of sensors for pairwise exchange of information. But this scheme does not square well with known sensor network security problems like node compromise, low network connectivity, and a large communication overhead. However, a link-layer key management scheme can mitigate these problems and therefore be more efficient.
- *Data replication*. Data replication is the process of storing the same data on several sensor network nodes which created enough redundancy which in turn improves on reliability and availability and hence security.
- *Resilience to node capture*. One of the most challenging issues facing sensor networks is that of node capture. Online traditional networks can get high physical security; however, sensor networks are usually deployed in environments with limited physical security if any.

19.6 Trends in Sensor Network Security Research

Although we have outlined the difficulties in making a sensor network secure due to inherent limitations, it is, however, possible to design security protocols that are specific for a particular security issue. This is the direction that current sensor network security research is taking [15].

19.6.1 Cryptography

There are several cryptographic approaches being used to secure sensor networks. One of the first tasks in setting up a sensor network is to establish cryptographic system with secure keys for secure communication. It is important to be able to encrypt and authenticate messages sent between sensor nodes. However, doing this

requires prior agreement between the communicating nodes on keys for performing encryption and authentication. Due to resource constraints in sensor nodes, including limited computational power, many key agreement schemes like trusted server, public key, and key pre-distribution used in traditional networks are just not applicable in sensor networks. Also pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory this requires when the network size is large. Although, over the years, efforts have been made to propose several approaches to do this, the inherent limited computational power of sensor nodes and the huge numbers of network nodes are making public key cryptographic primitives too expensive in terms of system overhead in key establishment [16]. Modern research has tried to handle the key establishment and management problem network wide by the use of a shared unique symmetric key between pairs of nodes. However, this also does not scale well as the number of nodes grows [16].

19.6.2 Key Management

Because of sensor node deployment and other sensor network limitations like limited computation capabilities, it is not possible to use key management as usually done in traditional networks where there may be a relationship in key sharing among members of the network. Because of these difficulties in sensor networks, if there were to be a single shared key, a compromise of just one node, may be through capture, would lay the entire network bare. A new framework of key exchange is needed. Eschenauer and Gligor [17] first proposed a framework of key exchange where a sensor randomly chooses m keys from the key pool with n keys before the deployment. After the node is deployed, it then contacts all its immediate neighbors to see if it shares any key with them. What must be noted in this solution is the noninvolvement of the base station in this key management framework. Several extensions of this framework have been developed including the following [18]:

- *The q-composite random key pre-distribution framework*—where two nodes share a common key hashed from q common keys. This approach adds more strength to the above approach. Because now an intruder would need to capture communication from more nodes in order to be able to compute a shared key.
- *Multi-key reinforcement framework*—where a message from a node is partitioned into several fragments and each fragment is routed through a separate secure path. Its advantages are balanced by its high overhead.
- *Random-pairwise framework*—where in the pre-deployment phase, N unique identities are generated for each network node. Each node identity is matched up with other m randomly selected distinct node identities, and a unique pairwise key is generated for each pair of nodes. The new key and the pair of node identities are stored on both key rings. After deployment, the nodes then broadcast their identities to their neighbors.

Other frameworks include a localized encryption and authentication protocol (LEAP) by Zhu et al. [19]. Under LEAP, it is observed that there are different types of messages in a sensor network. This leads to the use of four keys: individual, group, cluster, and pairwise key [18].

19.6.3 Confidentiality, Authentication, and Freshness

It is common knowledge to all security professionals that the use of strong cryptographic techniques strengthens the security of communication. In sensor networks, like in traditional networks, this is also the case. During authentication in sensor networks, the sending node, using a shared key with the receiving node, computes a Message Authentication Code (MAC) on the message about to be transmitted using a known hash function. The receiving node, upon receipt of the message, applies the shared key and the same hash function to the message to generate a new MAC. If this MAC agrees with the sender node's MAC, then the message has not been tempered with, and the receiving node knows that the message has been sent by the sending node since it is only this sending node that shares the key with the receiving node. Several studies including [15] SPINS have used this approach. SPINS has two building blocks: Secure Network Encryption Protocol (SNED) providing data confidentiality, a two-part data authentication, and data freshness and micro-Timed, Efficient, Streaming, Loss-tolerant Authentication (μTESLA) which provides authentication to node streaming broadcasts. In addition to SPINS, TinySec [20] which also supports message confidentiality, integrity, and authentication in wireless sensor networks also uses this approach. There are several other works on message confidentiality, authentication, and integrity, including that of Perrig et al. [15].

19.6.4 Resilience to Capture

While sensor networks, because of their size and deployment, are ideal for information gathering and environmental monitoring, node compromise poses a very serious security problem in these networks. While existing ad hoc security solutions can address a few security problems, on a limited number of nodes in a network, many of these solutions cannot scale up when the numbers of nodes in the network grows. Also when the node number is high and typically these nodes are unattended, they are prone to node compromise.

To overcome this problem, Yang et al. [20] have proposed a novel location-based key management solution through two techniques in which they bind symmetric secret keys to geographic locations and then assign those location-bound keys to sensor nodes based on the nodes' deployed locations. There are two approaches to this scheme: location-binding keys and location-based keys. In both of these approaches, the network terrain is divided into a grid where each cell on the grid is associated with multiple keys. Each node in a grid stores one key

for each of its local neighboring cells and a few randomly selected remote cells. Any genuine real event must be validated by multiple keys bound to the specific location of that event. This requirement rules out any bogus event which might be a result of an attacker obtaining multiple keys from some compromised nodes because such event cannot combine all necessary keys to make the event genuine.

Exercises

1. Sensor networks are different from traditional networks. Discuss five reasons why.
2. Wireless sensor networks are different from wireless ad hoc networks. Discuss by giving reasons why this is so.
3. It is difficult to implement security mechanisms that are proven to work in traditional networks, even in wireless ad hoc networks in sensor networks. Why is this the case?
4. Discuss several ways to prevent node capture in sensor networks.
5. Encryption is very difficult to implement in sensor networks. However, there have been several papers exploring limited ways of doing this. Look for one or two papers, and discuss what approaches are being used.

Advanced Exercises

1. Since sensor networks are severely constrained by resources, can the deployment of sensor networks under a single administrative domain make it easier to secure these networks?
2. Based on question 1 above, can introducing redundancy or scaling the network help in creating secure sensor networks?
3. Again based on 1 above, is it possible to continue operating a sensor network with a selected number of sensors taken out? Is it possible to identify those nodes?
4. Devise ways (some cryptographic) of securing wireless communication links against eavesdropping, tampering, traffic analysis, and denial of service.
5. Is it possible to design an asymmetric encryption protocol with all computations based on the base station?

References

1. Wikipedia. http://en.wikipedia.org/wiki/Sensor
2. Seapahn M, Koushanfar F, Potkonjak M, Srivastava MB. Coverage problems in wireless Ad-hoc sensor networks. http://web.cs.ucla.edu/~miodrag/papers/Meguerdichian_Infocom_01.pdf
3. David C, Estrin D, Mani SM (2004) Overview of sensor networks. Computer 37:41–50
4. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci A (2002) A survey on sensor networks. IEEE Commun Mag 40:102–114

5. Jay W. Smart sensor networks of the future. DA Systems. http://archives.sensorsmag.com/articles/0397/net_mar/main.shtml
6. Ortiz J, Moon D, Baker CR. Location service for point-to-point routing in wireless sensor networks. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.710&rep=rep1&type=pdf
7. Sure A, Iyengar SS, Cho E (2006) Ecoinformatics using wireless sensor networks: an overview. Ecolo Inform 1:287–293
8. Subramanian NVK. Survey on energy-aware routing and routing protocols for sensor networks. http://www.csee.umbc.edu/~younis/Publications/JAdHoc/SensNetRouting.pdf
9. Krishnamachari B, Estrin D, Wicker S. The impact of data aggregation in wireless sensor networks. ACM Digital Library. http://dl.acm.org/citation.cfm?id=708078
10. De P, Liu Y, Das SK (2006) Modeling node compromise spread in wireless sensor networks using epidemic theory. In: Proceedings of the 2006 international symposium on a world of wireless, mobile and multimedia networks (WoWMoM'06)
11. Stankovic JA. Research challenges for wireless sensor networks. http://doi.acm.org/10.1145/1121776.1121780
12. Anand M, Ives Z, Lee I (2005) Quantifying eavesdropping vulnerability in sensor networks, ACM international conference proceeding series. In: Proceedings of the 2nd international workshop on data management for sensor networks, vol 96
13. Hu YC, Perrig A, Johnson DB (2003) Rushing attacks and defense in wireless Ad Hoc network routing protocols. ACM Digital Library. http://dl.acm.org/citation.cfm?id=941317
14. Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. http://www.csee.umbc.edu/courses/graduate/CMSC691A/Spring04/papers/sensor-route.pdf
15. Perrig A, Szewczyk R, Wen V, Culler D, Tygar JD (2002) SPINS: security protocols for sensor networks. http://www.netsec.ethz.ch/publications/papers/mc2001.pdf
16. Perrig A, Stankovic J, Wagner D (2004) Security in wireless sensor networks. Commun ACM 47(6):53–57
17. Eschenauer L, Gligor VD (2002) A key-management scheme for distributed sensor networks. In: ACM conference on computer and communications security. ACM, New York
18. Sabbah E, Majeed A, Kyoung-Don K, Liu K, Abu-Ghazaleh N (2006) An application-driven perspective on wireless sensor network security. Q2SWinet'06, October 2, 2006
19. Zhu S, Setia S, Jajodia S (2003) LEAP: efficient security mechanisms for large-scale distributed sensor networks. In: The 10th ACM conference on computer and communication security (CCS '03), 2003
20. Karlof C, Sastry N, Wagner D (2004) TinySec: a link layer security architecture for wireless sensor networks. In: ACM SenSys, 2004