UNIT - V

Security in Adhoc and Sensor Network

Syllabus

Security Attacks – Key Distribution and Management – Intrusion Detection – Software based Anti-tamper techniques – Water marking techniques – Defense against routing attacks - Secure Ad hoc routing protocols – Broadcast authentication WSN protocols – TESLA – Biba – Sensor Network Security Protocols – SPINS.

Introduction

Security and Related Aspects in Wireless Sensor Networks

Security Attacks and Security Vulnerabilities in Wireless Sensor Networks

5.1 Introduction

Quick and huge developments in wireless communication, sensor technology, and embedded computing technology have promoted the emergence and development of wireless sensor networks (WSN). Wireless sensor networks consist of a large number of cheap micro sensor nodes deployed in the monitoring area, which is a multi-hop self- organizing network system formed by wireless communication method, whose purpose is to sense, collect, and process cooperatively the information sensed by sensors in the network distributed area and then forward the results to its users.

5.1 Security and Related Aspects in Wireless Sensor Networks

5.1.1 Characteristics of Wireless Sensor Networks

(i) **No Central Node -** Wireless sensor network has no absolutely central node, and all nodes are in equal status. Not only is it the gatherers of information but also the forwarders for other nodes transfer information. Network nodes coordinate behavior with each other through a distributed algorithm.

(ii) **Self-Organization -** A wireless sensor network requires every sensor node to be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well. If self-organization is lacking in a sensor network, the damage resulting from an attack or even the hazardous environment may be devastating.

(iii) **Large-Scale -** A wireless sensor network usually consists of thousands of tiny sensors, not primarily depending on the ability to upgrade individual devices but to improve the reliability and stability of the system depending on large- scale and redundancy of embedded devices to work together.

(iv) **Volatility of Network Topology -** In wireless ad hoc network, various factors such as node mobility and decrease of the remaining power of the power control box in the sensor nodes can lead to network topology changes and make the network topology constantly change which is not regular and unpredictable.

(v) **Multi-hop Routing -** Wireless sensor networks use multi-hop routing mechanism. Due to the limits of transmitting power and the communication coverage radius, when communicating with other nodes out of the coverage, the node needs the intermediate nodes to forward.

(vi) **Data-Centric Networks -** As nodes are randomly deployed, the relationship between the network and node number is entirely dynamic, showing up that there is no necessary connection between the node number and the node position. User directly reports the events of interest to the networks; then the networks report the information accessed in a specified time to the user. Therefore, the wireless sensor network is a data-centric network.

5.1.2 Security Constraints of Sensor Networks

1. Wireless sensor networks have distinctive constraints as compared to traditional networks making the implementation of existing security measures not practicable. In broader terms, these constraints are the upshot of limitations regarding the sensor nodes’ memory, energy, and transmission and processing power as well as due to the ad hoc

and wireless channel. These constraints, which make the design of security measures more complicated.

2. These constraints construct it impossible to employ the existing strong but complex security solutions to the WSNs. In order to design competent and useful security mechanisms for WSNs, it is essential to understand the constraints in WSN. It has been categorized into node constraints and network constraints and is discussed in the subsequent sections.

3. **Node Constraints -** Security solutions need high computation, memory storage and energy resources which create an extra challenge when working with tiny sensor nodes. Table 2.1 lists the specifications of different types of nodes used in wireless sensor networks. The principal challenge of security in WSNs is maximizing security while minimizing resource consumption. The resources in this perspective include energy (battery power), processing (CPU cycles), storage (memory) and the communication bandwidth.

   (3.1) Limited Memory - Typical sensor nodes are tiny devices which come with very limited memory and storage capacity.

   Berkeley's MICA2 possess 4-8

   MHz, 4KB of RAM, 128KB flash and ideally 916 MHz of radio frequency. This means any security solution designed for sensor networks should be lesser in code.

   (3.2) Limited Energy - Energy is another vital factor to consider when designing security procedures for sensor nodes. Given the sensor network topology which makes accessing them after deployment unfeasible, it is very important to restrict the energy consumption and thereby widen the battery life. However, adding security measures to sensor networks necessarily has a considerable impact on its energy consumption, for example, to carry out the encryption and decryption functions, to store, manage and send the encryption keys etc.

(3.3) Limited processing capability - Sensor nodes processors are exceptionally slow (up to few MHz) and they do not support some arithmetic and logic operations. Hence, they cannot carry out very complex cryptographic operations.

(3.4) Limited storage capability - The memory offered for security is very low (only a few KBs). This requires that any security method designed for sensor networks should consume as less memory as possible.

4. **Network Constraints -** Sensor networks having all the constraints of mobile ad hoc networks such as untrustworthy network communication, collision related problems and their lack of physical infrastructure.

(4.1) Unreliable Communication - Wireless communication is intrinsically unreliable and can affect packets to be damaged or dropped. This unreliability in communication poses additional threats to the nodes if dropped packets are taken over by adversaries.

(4.2) Collisions and latency - Sensor networks exploit a dense arrangement of nodes potentially deploying hundreds or thousands of nodes in a sensitive application. This causes the likelihood of collision and latency in packets. However, distinct in traditional networks, the energy limitations of sensor nodes make it not viable to resend packets in case of collision.

(4.3) Limited bandwidth - Wireless links have small communication bandwidth.

The security schemes should utilize the limited bandwidth as possible.

5. **Physical Limitations -** Sensor networks are often installed in public and potentially hostile environments, which make some of their components extremely vulnerable to detain and destruction. To physically secure sensor nodes with tamperproof objects increases the cost.

(5.1) Unattended after deployment - The fact that sensor networks are deployed in applications where they will be left unattended allows adversaries larger access and independence to physically tamper with the nodes. Severe weather conditions and natural disasters such as storms, floods, earth quakes, and shrub fires can also hinder their functioning.

(5.2) Remotely managed - Being remotely managed makes it quite difficult to detect physical tampering with the sensor networks; other issues such as replacing the batteries and redeploying cryptographic keys are also impracticable to do remotely.

(5.3) Unattended Operations - The sensor networks are generally deployed in an environment accessible to adversary. The operations of sensor networks in unattended environment provide an adversary with a greater access to the sensor nodes than the typical PCs situated in a secure place. A security scheme should still defend against possible attacks, even if a small number of sensor nodes are compromised.

(5.4) Nature of Deployment - The topology of the sensor network is not known earlier to the deployment. Hence, the security schemes cannot help from the knowledge of neighboring nodes. A security scheme should prolong to provide services even in the presence of nodes failure.

6. **Energy Consumption -** The factors which consume energy for their operations,

   (i) Sensing energy consumption depends on the hardware and the application.

   (ii) An A/D Converter for sensor consumes only 3.1 μW, in 31 pJ/8-bit of energy at l Volt supply.

The computing unit related with a wireless sensor is a microcontroller/processor with memory which can control and function the sensing, computing and communication unit.

The energy consumption of this unit has principally two parts - **switching energy and leakage energy.** The dynamically changing workload without degrading performance thus saving energy. Leakage energy is the energy consumed when no computation work is made.

Sleeping - To conserve the energy, sensors can be put into sleep-wake up cycles. When a sensor is in sleep slate, it off some units to conserve energy. There are different types of sleep modes.

5.1.3 Wireless Sensor Network – Security Needs

According the characteristics, the wireless sensor networks differ from the traditional wireless networks, facing more demands especially in terms of security. In order to resist different kinds of security attacks and threats and to ensure the confidentiality of the tasks performed, the reliability of data generated, the correctness of data fusion, and the security of data transmission, the security requirements are mainly in the following areas.

(1) **Data Confidentiality -** Data confidentiality is an important network

security need requiring that all sensitive information in the storage and transmission process must ensure its confidentiality. Divulging the content of the information to any unauthorized user is not allowed.

(2) **Data Integrity -** With the assurance of confidentiality, an attacker could not get the real content of information, but the recipient does not guarantee that the data it receives is correct, because malicious intermediate nodes can intercept, tamper, or disturb the information during the transmission. Through data integrity identification, one can ensure that the data won't change anymore during its transference process.

(3) **Data Freshness -** Data freshness view is to emphasize that each of the received data is the latest from the sender, which makes it stop receiving repeated information. The main purpose to ensure the freshness of the data is to prevent replay attacks.

(4) **Availability -** Availability requires the sensor networks that can always provide information access service to the legitimate users according to the preset. But the attacker can make some or all of the sensor network paralyzed by forging and interfering signal or other methods to destroy availability of the system, such as DoS (Denial of Service) attacks.

(5) **Robustness -** Wireless sensor networks are highly dynamic and uncertain, including changes in the network topology and the nodes' disappearing or joining. Therefore, the wireless sensor networks under a variety of security attacks should have strong adaptability, and even if a particular attack succeeds, the performance can make the impact minimized.

(6) **Access Control -** Access control requires the ability to identify the users who access wireless sensor networks to ensure the legitimacy. Access control determines who can access the system, what system resources

can be accessed, and how to use these resources.

5.1.4 Security in Wireless Sensor Networks

1. Security in Wireless Sensor networks is a crucial component for basic network functions similar to packet forwarding and routing. There is no predetermined infrastructure in ad hoc sensor networks and as the name indicates they are formed on the fly.
2. The devices connect to each other in their own communication range through wireless links. Individual devices behave as routers when relaying messages to other devices. The topology of an ad hoc sensor network is not fixed. It changes every time when these mobile stations move in and out of every other's transmission range.
3. All this makes ad hoc networks exceptionally vulnerable to attacks and the security issues become very complex. Therefore, security in ad hoc sensor networks is a harder task than in traditional wired.
4. The wireless links in an ad hoc sensor network makes it susceptible to attacks ranging from passive eavesdropping to active impersonation attack. Thus these attacks violate integrity, availability, authentication and non-repudiation. Nodes wandering freely in a hostile environment with relatively pitiable physical protection cause good probability of being compromised.
5. Therefore, security solutions require considering malicious attacks not only from outside but also from within the WSN.
6. Further, the trust relationships among individual nodes can vary, especially when some of nodes are found to be compromised. To find high survivability of ad hoc networks they need to have a distributed architecture with no central control, which definitely increases vulnerability. Hence, security mechanism needs to be dynamic, and

should be passably scalable.

7. The particular characteristics of WSNs in excess of an improvement to any adversary who intends to compromise security. For example, the sensor nodes use radio-link as a communication medium which is in fact insecure.
8. Broadcast nature of communication medium makes Wireless Sensor Networks more vulnerable to security attacks than wired networks. Conversely, provision of security in WSNs is a challenging task since the resources in sensor nodes devices are not enough for executing complex security protocols.

5.1.5 Secure Communication in Sensor Networks

4. Sensor networks may be deployed in unfriendly environments, especially in military applications. In such situations, the sensors may be captured, and the data/control packets might be intercepted and/or modified. So, security services such as authentication and encryption are necessary to maintain the network operations.
5. Yet, due to the resource constraints, some of the security mechanisms are not feasible in sensor networks.
6. In sensor network security, an essential challenge is the design of protocols to bootstrap the establishment of a secure communications infrastructure from a collection of sensor nodes that been pre-initialized with some secret information but have had no earlier direct contact with each other. This problem is referred to as the bootstrapping problem.

7. A bootstrapping protocol must not only allow a newly deployed sensor network to initiate a secure infrastructure, but it must furthermore allow nodes deployed at a later time to join the network securely. The difficulty of the bootstrapping problem stems from the many limitations of sensor networks like limited resource constraints.

5.1.6 Security Goals and Services of Sensor Networks

The goal of security services in WSNs is to protect information (confidentiality, authentication, integrity, access control, and freshness) and resources (availability) from attacks and mischief in the presence of a resourceful adversary.

1. **Authentication** enables every message sender in the sensor networks, including the base station, sensor nodes and outer users, to prove its identity, that is, the legitimacy of the source of a message to the receiver. It allows the receiver of the message to ensure that received messages are in actuality originated from the claimed source.
2. **Message Integrity** verifies the authenticity of the received message contents. It must be implemented so that the contents of received message have not been modified in transit by an adversary.
3. **Verification** empowers every sensor node in the network to confirm the legitimacy of the received message. It is important that authentication does not imply verification in WS Network environment. A legitimate message sender might send an authenticated message to the sensor nodes; on the other hand, the sensor nodes may not have access to authentication information of the message sender or may not be able of performing efficiently the computation that is required to verify authentication information.
4. **Freshness** ensures that a received message is new and a recent one.

Freshness can mean both data freshness and key freshness.

5. **Confidentiality** prevents unauthorized entity or adversaries from accessing the data being sent to the authorized one. The confidentiality objective is essential in WSNs environment to protect data traveling between the sensor nodes, between the sensor nodes and the base station, and also between the sensor nodes and the outside entity from disclosure. A confidential message should not disclose its contents to an eavesdropper.
6. **Access Control** ensures that only the authorized sensor is involved in providing information to network services and merely an authorized user obtains a certain type of data according to his access privileges. Access control is required in those applications of WSNs, which collect a variety of data.
7. **Availability** ensures the survivability of sensor network to authorized parties when needed, in spite of the presence of internal or external attacks.
8. **Key distribution** is used to provide security for wireless sensor networks, it ensures that the communication should be encrypted and authenticated from distributing the keys among sensors.

5.2 Security Attacks and Security Vulnerabilities in Wireless Sensor Networks

WSNs are vulnerable to various types of attacks. These attacks can be broadly categorized as follows.

1. **Attacks on network availability attacks -** on availability attacks are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.
2. **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.

3. **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. In these attacks, keeping the sensor network available for its intended use is essential. DoS attacks against WSNs may permit real-world damage to the health and safety of people. The DoS attack usually refers to an adversary's attempt to disrupt, subvert, or destroy a network. However, a DoS attack can be any event that diminishes or eliminates a network's capacity to perform its expected functions.

5.2.1 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. 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.

5.2.1.1 Physical Layer Attacks

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. 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 namely,

(i) Jamming and (ii) tampering.

(i) **Jamming -** It is a type of attack which interferes with the radio frequencies that the nodes use in a WSN for communication. A jamming source may be powerful enough to disrupt the entire network. Even with 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 .

(ii) **Tampering -** Sensor networks typically operate in outdoor environments. Due to unattended and distributed nature, the nodes in a WSN are highly susceptible to physical attacks. 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. It has been shown that sensor nodes such as MICA2 motes can be compromised in less than one minute time.

5.2.1.2 Link Layer Attacks

1. The link layer is responsible for multiplexing of data-streams, data frame detection, medium access control, and error control. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation.
2. A collision occurs when two nodes attempt to transmit on the same

frequency simultaneously. 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.

3. 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. For example, a naïve link layer implementation may continuously attempt to retransmit the corrupted packets.
4. Unless these retransmissions are detected early, the energy levels of the nodes would be exhausted quickly. Unfairness is a weak form of DoS attack. 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.

5.2.1.3 Network Layer Attacks

The network layer of WSNs is vulnerable to the different types of attacks as described below.

1. **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. 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.
2. **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.

3. **Sinkhole -** In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbours by forging the routing information. The result is that the neighbour 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.

4. **Sybil attack -** It is an attack where one node presents more than 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. 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.

5. **Wormhole -** A wormhole is low latency link between two portions of a network over which an attacker replays network messages. 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.

6. **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.
7. **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. 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.
8. **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. Byzantine attacks are very difficult to

detect, since under such attacks the networks usually do not exhibit any abnormal behavior.

9. **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.
10. **Resource-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 namely, 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.
11. **Acknowledgment spoofing -** Some routing algorithms for WSNs require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighbouring nodes and spoof the acknowledgments thereby providing false information to the nodes. 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.
12. 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.**

5.2.1.4 Transport Layer Attacks

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

1. **Flooding -** Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding. 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.
2. **De-synchronization -** De-synchronization refers to the disruption of an existing connection. 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.

SL. No.	Layer	Attacks	Defense
1.	Physical cycle	Jamming	Spread-spectrum, priority messages, lower duty region mapping, mode change
2.	Link	Collision Exhaustion Unfairness	Error-correcting code Rate limitation Small frames

3.	Network	Spoofed routing information & Selective forwarding Sinkhole Sybil Wormhole HELLO Flood	Egress filtering, authentication, monitoring Redundancy probing Authentication, monitoring, redundancy Authentication, probing Authentication, packet leashes by using geographic and temporal info Acknowledgment flooding Authentication, verify the bi-directional link authentication
4.	Transport	Flooding De-synchronization	Client puzzles Authentication

Table 5.2.1 Attacks on various layers of a WSN and their countermeasures

5.2.2 Attacks on Secrecy and Authentication

There are different types of attacks under this category as discussed below.

52.2.1 Node Replication Attack

In a node replication attack, an attacker attempts to add a node to an existing WSN by replication (that is copying) the node identifier of an already existing node in the network. 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.

5.2.2.2 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. 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.

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 carry out 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.

Following are some of the common attacks on sensor data privacy.

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. There are two types of attacks studied in this category, that can identify the base station in a WSN without even underrating the contents of the packets being analyzed in traffic analysis.

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, 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.