Problem Specification
CHAPTER III

PROBLEM SPECIFICATION

3.1 Wireless Sensor Network Security Issues

Security mechanisms in WSN are developed in view of certain constraints. Among these, some are pre-defined security strategies, whereas some are direct consequences of the hardware limitations of sensor nodes.

Energy Efficiency:

The requirement for energy efficiency suggests that in most cases computation is favored over communication and is three orders of magnitude more expensive than computation. The requirement also suggests that security should never be overdone on the contrary, tolerance is generally preferred to over aggressive prevention. More computationally intensive algorithms cannot be used to incorporate security due to energy considerations.

No Public-Key Cryptography

Public-key algorithms remain prohibitively expensive on sensor nodes both in terms of storage and energy. No security schemes should rely on public-key cryptography. However it has been shown that authentication and key exchange protocols using optimized software implementations of public-key cryptography is very much viable for smaller networks.

Physically Tamper-able

Since sensor nodes are low-cost hardware that is not built with tamper-resistance in mind, their strength has to lie in their number. Even if a few nodes go down, the network survives. The network should instead be resilient to attacks. The concept of resilience, or equivalently, redundancy-based defense is widely demonstrated.
Multiple Layers of Defense

Security becomes an important concern because attacks can occur on different layers of a networking stack (as defined in the Open System Interconnect model). Naturally it is evident that a multiple layer of defence is required, i.e. a separate defence for each layer. The issues mentioned here are in general

3.2 Security Requirements

Availability

Sensors are strongly constrained by many factors, e.g., limited computation and communication capabilities. Additional computations or communications consumes additional energy and if there is no more energy, data will not be available. Energy is another extremely limited resource in large scale Wireless sensor network. A single point failure will be introduced while using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network. Moreover, Wireless sensor network are vulnerable to various attacks. The adversary is assumed to possess more resources such as powerful processors and expensive radio bandwidth than sensors. Equipped with richer resources, the adversary can launch even more serious attacks such as DoS attack, resource consumption attack and node compromise attack.

Confidentiality

Data confidentiality is the most important issue in network security. Confidentiality, integrity and authentication security services are required to thwart the attacks from adversaries mentioned in the above section. These security services are achieved by cryptographic primitives as the building blocks. Confidentiality means that unauthorized third parties cannot read information between two communicating parties. A sensor network should not leak sensor readings to its
neighbours. Especially in a military application, the data stored in the sensor node may be highly sensitive.

In many applications, nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a Wireless sensor network. Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. Generally, encryption is the most widely used mechanism to provide confidentiality.

**Integrity and Authenticity**

Confidentiality only ensures that data cannot be read by the third party, but it does not have guarantee that data is unaltered or unchanged. Integrity means the message one receives is exactly what was sent and it was unaltered by unauthorized third parties or damaged during transmission. Wireless sensor network use wireless broadcasting as communication method.

Thus it is more vulnerable to eavesdropping and message alteration. Measures for protecting integrity are needed to detect message alteration and to reject injected message. Authentication ensures that the sender was entitled to create the message and that the contents of the message have not been altered. In the public key cryptography, digital signatures are used to seal a message as a means of authentication. In the symmetric key cryptography, MACs are used to provide authentication. When the receiver gets a message with a verified MAC, it is ensured that the message is from an original sender. Digital signature is based on asymmetric key cryptography (e.g., RSA), which involves much more computation overhead in signing/decrypting and verifying/encrypting operations. It is less resilient against DoS attacks since an attacker may feed a victim node with a large number of bogus signatures to exhaust the victim’s computation resources for verifying them.
Data Freshness

Data freshness means that the data is recent and any old data has not been replayed. Data freshness criteria are necessary in case of shared-key cryptography where the key needs to be refreshed over a period of time. An attacker may replay an old message to compromise the key.

Self Organization

Due to the ad-hoc nature of WSN it should be flexible, resilient, adaptive and corrective in regards to security measures. The availability of small and cheap wireless sensing devices increased significantly in the past few years and large-scale real-world sensor networks begin to appear. Such a large number of sensors deployed in the real-world allow for accurately monitoring a variety of physical phenomena, like weather conditions (temperature, humidity, atmospheric pressure etc) traffic levels on highways or rooms occupancy in public buildings. Making these sensors and their data available on a common web interface opens several interesting application scenarios. Users can query the available sensor data in real-time and use the query results to perform decisions or any kind of monitoring tasks. Since sensor data typically inherently relates to the specific sensor location, geo-based web interfaces like Google Maps or Windows Live Local are particularly suited to support real-world sensor querying. Systems providing the necessary software infrastructure and tools for data acquisition, storage and online visualization of globally available sensor data begun to appear in the last few years.

3.3 Problem Statement

The WSN Security is a mature research area. Data encryption and authentication has been the subject of several research efforts. However, few security solutions for wireless sensor network exit. Most of the current security solutions are developed to be quite general to fit many different platforms and scenarios. The existing security solution deliver security feature at the link and network layer. Wireless sensor network can successfully operate in the presence of component transfer failure or malicious attack, Data collection and Aggregation is
challenging in Wireless sensor network. In WSN data collection and aggregation are unsecure because of sensor node incompatibility. So providing security to Sensor network is very important.

Sensor networks are usually deployed in hostile and unattended environment where an adversary can read and modify the content of the data packet. For such situation the most popular type of attack is the external attack and replay attack. Node need to be authenticated before data transmission takes place.

Network life time is also an important issue in sensor networks. In external attack the nodes does not belong to the network try to read and modify the packet. If node read and modify the packet sink will not get the correct data. For that new method also need to authenticate the node before data transmission. In this use concept of mobile sink to prolong network lifetime and overcome the sink neighbourhood problem.

In mobile sink sensor networks, sink traverse the network to collect data. If a node sense some critical data and sink is not its range, for that situation sensor node transmit the data to mobile sink immediately. That proved to be an existing protocol for critical data transmission and make it as the secure protocol to avoid external attack and node authentication during data transmission. It securely collects the data from network and critical data transmission to mobile sink in mobile sink sensor networks.

These research works have to investigate three security problems that exist in the above counter-attack approach.

- No longer valid if the adversary can selectively compromise or jam nodes. This is because the route computation in the above multi-path routing algorithms is deterministic in the sense that for a given topology and given source and destination nodes, the same set of routes is always computed by the routing algorithm. As a result, once the routing algorithm becomes known to the adversary, it can compute the set of routes for any given source and destination. Then the adversary can
pinpoint to one particular node in each route and compromise (or jam) these nodes. Such an attack can intercept all shares of the information, rendering the above counter-attack approaches ineffective.

- Very few node-disjoint routes can be found when the node density is moderate and the source and destination nodes are several hops apart.

- The set of routes is computed under certain constraints, the routes may not be spatially dispersive enough to circumvent a moderate-size black hole. In reality, a stronger attack could be formed, whereby the adversary selectively compromises a large number of sensors that are several hops away from the sink to form clusters of black holes around the sink.

Nowadays, Compromised node and Denial-of-Service are two keys of attacks in Wireless Sensor Network (WSN). Protection of sending the data from source to destination through this model circumvents black holes formed by these attacks. For this, to explore the potential of random dispersion for information delivery in WSN. Depending on the type of information available to a sensor; Present to develop our distributed scheme for propagating information. By sharing one-hop neighborhood information, a sensor node maintains a list of id’s data of all nodes within its transmission range. When a source node wants to send shares to the sink, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than zero, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on.

3.4 Attacks on Wireless Sensor Network

Acknowledgment spoofing

The most direct attack against a routing protocol [96] in any network is to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in
Chapter - III

Problem Specification

the network. Some routing protocols use link layer acknowledgments. Attacker may spoof acks show in Figure 3.1.

Goals: convince that weak link is strong or that dead node is alive. Consequently weak link may be selected for routing; packets send through that link may be lost or corrupted.

Figure 3.1 Acknowledgment spoofing

HELLO flood attack

Many WSN routing protocols require nodes to broadcast HELLO packets after deployment, which is a sort of neighbour discovery based on radio range of the node. Laptop class attacker can broadcast HELLO message [57] to nodes and then advertises high quality route to sink shown in Figure 3.2.

Figure 3.2 Hello flood attack

Sinkhole

In a sinkhole attack [82], an attacker makes a compromised node look more attractive to surrounding nodes by forging routing information. The end result is that
surrounding nodes will choose the compromised node as the next 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 will flow through the adversary’s node.

**False routing information**

Injecting fake routing control packets into the network shown in Figure 3.3, examples: attract / repeal traffic, generate false error messages. Consequences: routing loops, increased latency, decreased lifetime of the network, low reliability. Example: captured node attracts traffic by advertising shortest path to sink, high battery power [96].

![Figure 3.3 False Routing algorithm](image)

**Sybil**

The Sybil attack [93] is a case where one node presents more than one identity to the network. Protocols and algorithms which are easily affected include fault tolerant schemes, distributed storage, and network topology maintenance. For example, a distributed storage scheme may rely on there being three replicas of the same data to achieve a given level of redundancy. If a compromised node pretends to be two of the three nodes, the algorithms used may conclude that redundancy has been achieved while in reality it has not.
3.5 **Attacks on Routing Protocols**

All of the proposed sensor network routing protocols are highly black hole to attack. Adversaries can attract or repel traffic flows, increase latency, or disable the entire network with sometimes as little effort as sending a single packet. In this section, Conducted survey the proposed sensor network routing protocols and highlight the relevant attacks. Most of the routing protocols for WSN are vulnerable to various types of attacks. Some of these attacks are listed below[34].

**Routing Table Overflow** in this type of attack, an adversary node advertises routes to non-existent nodes, to the authorized node present in the network. The main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes. Proactive routing protocols are more vulnerable to this attack compared to reactive routing protocols.

**Routing table poisoning** in this case, the compromised nodes in the network send fictitious routing updates or modify genuine route update packets sent to other honest nodes. Routing table poisoning may result in sub-optimal routing, congestion in some portions of the network, or even make some parts of the network inaccessible.

**Packetreplication** in this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power and other resources available to the nodes and also causes unnecessary confusion in the routing process.

**Routecache poisoning:** in reactive (i.e. on-demand) routing protocols such as Ad Hoc On-Demand Distance Vector (AODV) [David B. Johnson et al.] each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past[100]. Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar objectives.

**Routing based attack** on-demand routing protocols that use *duplicate suppression* during the route discovery process are vulnerable to this attack [Hu et
An adversary node which receives a `routeresquest` packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same `routeresquest` packet can react. Nodes that receive the legitimate `routeresquest` packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node [35]. It is extremely difficult to detect such attacks in WSN.

### 3.6 Data Gathering - Collection and Aggregation Mathematical Attack

Sensor Network are “Adversary”, Any sensor Z in the network can be an adversary and can attempt to disrupt the communication between any two legitimate sensors, as sensor X and Y, by launching the following two attack.

- Impersonation attack
- Eavesdropping attack

#### Impersonation attack

Sensor Z notices that it is adjacent to sensor X. If sensor y is not, thus sensor z attempts to convince sensor X that it (Z) is fact of sensor y. If sensor Z succeeds, then sensor x may start to exchange data message with sensor Z, thinking that it is communicating with sensor Y.

#### Eavesdropping attack

Sensor z notice that it is adjacent to both sensor X and Y, and that sensor X and Y are adjacent to one another. Thus, when sensor X and Y start to exchange data message, sensor Z can copy each exchanged data message between X and Y.
Here X is adjacent Y means to get the Y information. In some time the mutual authentication is adversary to other unknown node shown in Figure 3.4. Example the Z adjacent to X or Z adjacent to Y. Here Z copy the both information from X and Y.

Ns-2 simulation is used to develop and test algorithm which are likely to arise during the research. The simulation results indicate that data collection and aggregation function can achieve energy saving under various attack patterns with different ratios of compromised nodes and reason about the uncertainty in the collection and aggregation results.