CHAPTER 1

INTRODUCTION

Wireless sensor nodes are self organized nodes. The integration of sensing, computing and communication of nodes provide opportunities in diversified applications such as environmental monitoring (Werner et al 2006), habitat monitoring, structural monitoring, health monitoring, wearable computing, disaster recovery, context-aware computing, smart environment, urban warfare, medical domain, hazard detection, earth science and exploration and so on. The limitations of these nodes are requirement of higher energy, computing ability and memory. These limitations provide enormous research challenges (Hu et al 2003) such as energy awareness, localization, tiny operating system, architecture design, routing and security.

1.1 FUNDAMENTALS OF WIRELESS SENSOR NETWORKS

Wireless Sensor Network (WSN) (Akyildiz et al 2002) is an interconnection of autonomous sensor nodes that are capable of transmitting the sensed information to a base station/sink node. WSN consists of fundamental components namely, (i) Wireless Node (ii) Base Station / Sink Node and (iii) Wireless Link. The communication between the nodes and the nodes to the base station is done by using radio transceiver with an internal antenna or connection with an external antenna.
The RF transceiver consumes 1.97mA in receiving mode, 20mA in idle mode. The device is powered by two AA batteries which provide 2.7-3.3V. The RF transmitter and receiver sensitivity is -90dBm (min) to -94dBm (typ); 24 dBm to 0dBm and receiver sensitivity is -90dBm (min) to -94dBm (typ). The RF module and up to 13mA in sleep mode. Its radio frequency power ratio between deep sleep mode and power mode is 8mA. The current drawn by this unit is small in active mode.

The current draw is 1.43mA (typ) and 3.4mA (max) at 3.3V. The RF transceiver consists of ATmega128L, a low power microcontroller, and ER EEPROM. The power consumption of ATmega128L, a low power microcontroller, and the EEPROM, is 0.093mA (typ) and 0.34mA (max). The low power consumption of the RF transceiver makes it suitable for battery-powered devices.

When more than one sensor unit consists of a central processing unit, management and reduces the overall power consumption. The last three planes help the node to coordinate for sensing, task power aware and collision resistant and transmission of data responsible for sensing. The first three planes, the data, maintenance and routing of the data, are responsible for sensing the data. The first five layers are data link layer, physical layer, power management layer, mobility and link layer. The protocol stack consists of application layer, transport layer, network layer, transport layer, network layer, application layer, and physical layer.
and 1 µA in sleep mode. Its operating frequency band is from 2400MHz to 2483.5MHz.

1.1.2 WSN Standards

Institute of Electrical Electronics Engineers (IEEE) concentrates on physical and media access control layer, Internet Engineering task force gives attention to layer 3 and above and there is also other non standards. The most commonly used standards that are currently either ratified or unapproved are listed in Table 1.1.

Table 1.1 WSN Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Highway Addressable Remote Transducer protocol (HART)</td>
<td>Based on WSN Technology</td>
<td>Operated in 2.4 GHz ISM band using IEEE 802.15.4 time synchronized, self organizing and self-healing mesh architecture. <strong>Advantages:</strong> Fair level of interoperability and standardized data model</td>
</tr>
<tr>
<td>IEEE 1451</td>
<td>Smart transducer for open, common, network independent communication interface for connecting transducer</td>
<td>Developed by IEEE. Transducers are connected to systems or networks via a wired or wireless means.</td>
</tr>
</tbody>
</table>
## Table 1.1 WSN Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 802.15.4</td>
<td>Focused on Physical and MAC Layer</td>
<td>10 meter communication with a maximum transfer rate of 250k bits. <strong>Physical layer:</strong> It manages channel, energy and signal management functions. 868/915 direct sequence spread spectrum technique. Employs Binary Phase Shift Keying (BPSK), Offset (O-BPSK) and Amplitude Shift Keying <strong>Advantages:</strong> Wireless, low cost, flexibility and mobility <strong>MAC Layer</strong> Responsible for point-point delivery.</td>
</tr>
<tr>
<td>Zigbee</td>
<td>High level Communication Protocols</td>
<td>Maximum transfer rate of 250k bits. Low cost low power wireless mesh network standard. Network layer supports star, tree and mesh networks. Physical and MAC layers builds up on IEEE 802.15.4 Zigbee – Device Objects (ZDOs) layer responsible for device rolls, management of requests, device discovery and security. <strong>Advantage:</strong> Low latency (3s) Sleep to active mode (30ms or less), power consumption is low and long battery life. <strong>Disadvantages:</strong> Not secure, replacement with appliances can be costly.</td>
</tr>
</tbody>
</table>
Table 1.1 WSN Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>6LoWPAN</td>
<td>IPV6 low power wireless personal area networks</td>
<td>Internet protocol could be applied for low power computing devices.</td>
</tr>
</tbody>
</table>

**Advantage**
- It can handle data and management

**Disadvantage**
- Not a standard for sensor data, actual data covered by other standards

1.1.3 WSN Security Challenges

Since the transmission medium is exposed to any node surrounded by the geographical limit of the network, it is more difficult to secure the network from the malicious node. The following are the security challenges (Chong and Kumar 2003, Zia Zomaya 2006, Wang et al 2006, Sabbah and Kang et al 2009) present in the WSN along with its limitations.

- **Adhoc systems**: WSN is used in adhoc networks (Yu and Liu 2005, Shila et al 2010) in which a specific design is required to protect the network. Hence, data security is accomplished by using encryption and authentication algorithms at an increased cost. This decreases the performance of the system.

- **Intrusion Detection System (IDS)**: With the resource constraints of WSN, nodes are not capable of dealing with strong malicious attack. An IDS (Amitabh et al 2004) detects the possible insecurities and warns the malicious node. Designing an IDS is a unique challenge to overcome all type of attacks.
- Secured architecture: In the existing sensor network, the nodes require protection against packet drop, and injection or modification of packets. Since the nodes have limited power, recharging or replacement is not feasible. Hence, it is necessary to design a secured architecture (Shi and Perrig et al 2006) with the security primitives to prevent the network from attacks.

- Design of secure routing protocols: The routing attacks are more vulnerable in the WSN. The conventional routing protocols are designed without the security aspect. The protection of network plays a vital role. Enormous research challenges (Walters et al 2007) are there in designing secure routing protocols (Lee and Choi 2006) (Perrig et al 2002) or to modify the existing routing protocols in order to detect the malicious nodes.

- Physical security: Sensors are deployed in situations to collect data without human intervention. Nodes are thus insecure, unmonitored and subject to capture by attackers. Sensor network requires physical security, robustness, and resistance to tampering (both physically and wirelessly).

- Mobile nodes: In the dynamic topology, the threats and attacks of WSN are more due to mobile nodes (Xing and Hui 2007). The network performance varies based on the mobility and transmission range. Hence, the design of secure protocols, algorithms, and operating systems based on their mobility provides more challenges (Hao and Luo 2004).
Secure Services: Currently, research on security solutions for WSN is focused on secure localization (Binwei Deng et al 2012, Kui et al 2008, Zia and Zomaya 2007), routing, aggregation, software, transmission, and synchronization.

1.2 NEED FOR DETECTION SCHEMES

The WSN responsible for processing sensitive data face the risk of data manipulations, packet drop, modification in the routes of the packets, etc (Carman et al 2002). Hence, intrusion detection schemes are necessary in order to protect the network. Detection schemes are able to detect the malicious node as they transfer the message in a secured manner (Zia and Zomaya 2007). It has the ability to provide guaranteed message transmission from source to destination. The performance of the detection schemes is based on the network performance and its parameters such as throughput, packet delivery, energy consumption, detection accuracy (success rate, false positive rate, and false negative rate), byte overhead, and computation overhead. Without these detection schemes, packets on the network travels in an insecure manner resulting in retransmission of packets, packet dropping, and modification of routing path and thus deteriorates the performance of the network. Since the existing routing protocols are designed without considering the security issues, detection schemes are needed to secure the network from the malicious nodes. The following points indicate the necessity of detection schemes in the network.

- Certain applications of WSN includes real time applications such as health care monitoring, Body Area Networks (BAN), military applications, etc that need secure data transmission.
Constraints of WSN such as high energy and memory, less computational ability make the network more susceptible to attacks.

Detection schemes are required to improve the performance of the network otherwise malicious nodes makes the network lifeless.

Attacks in all the layers of WSN are fundamental. It is found that network routing attacks causes more damages in the network after analysis. Hence it is required to propose detection schemes to secure the network.

The widely used routing protocols such as Dynamic Source Routing (DSR), AODV, etc are not designed with security aspects. Since the network needs secure data transmission, certain detection schemes need to be incorporated either by modifying the routing protocol or redesigning the routing protocol.

The presence of malicious node causes packet loss, modification of the routing path, injection of malicious messages, creation of fake identities; etc, which degrade the performance of the network.

The possible potential threats based on the application is depicted in Table 1.2 (Y W Law 2005), Detection schemes are to be applied besides the other techniques to secure the network to quarantine those causes.
Hence, the incorporation of detection schemes in the network to provide secure data transmission, to increase the network throughput, packet delivery and to decrease the packet loss becomes a mandatory measure.

Table 1.2 Potential Security Threats, grouped according to the application domains

SA=Service Availability, C=Confidentiality, I=Integrity, A=Authenticity.

x = Possible violations

<table>
<thead>
<tr>
<th>Application domain</th>
<th>Potential Security threats</th>
<th>Properties violated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Military</td>
<td>• Denial-of-service attacks by means of jamming and/or confusing the networking protocols.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Eavesdropping of classified information</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>• Supply of misleading information, e.g. enemy movements in the east where in fact they are in</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Disaster detection and relief</td>
<td>• Supply of misleading information, e.g. bogus disaster warning by pranksters, causing huge financial loss as a result of unnecessary large-scale evacuation and deployment of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Application domain</td>
<td>Potential Security threats</td>
<td>Properties violated</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Industry</td>
<td>● Eavesdropping of commercial secrets by business rivals.</td>
<td>SA</td>
</tr>
<tr>
<td></td>
<td>● Intentional disruption of manufacturing processes as a result of misleading sensor</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>readings caused by disgruntled employees or business spies.</td>
<td></td>
</tr>
<tr>
<td>Agriculture</td>
<td>● The agricultural department might want to deploy WSNs to ensure that farmers do not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>overuse pesticides or other hazardous chemicals on their crops, but unscrupulous</td>
<td></td>
</tr>
<tr>
<td></td>
<td>farmers might tamper with the sensor</td>
<td>x</td>
</tr>
<tr>
<td>Environmental monitoring</td>
<td>● Government-endorsed environmental sensors are installed near a factory to monitor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>air/water quality to make sure the factory’s emission lies beneath the pollution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>threshold. However by feeding the sensors with wrong information, the factory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>allows itself to escape detection and let its</td>
<td></td>
</tr>
<tr>
<td>Application domain</td>
<td>Potential Security threats</td>
<td>Properties violated</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| Intelligent buildings   | ● Biometrics-based access control mechanisms can compromise if the biometric sensors can be bypassed or footed.  
                             ● Token-based access control mechanisms can compromise if the token authentication protocol | x       | x | x |
| Health/medical          | ● Providing wrong physiological measurements of a patient to the care or doctor, a miscreant may cause potentially fatal diagnosis and treatment | x       | x |
| Law enforcement         | ● If criminals are able to eaves drop the databases of the police departments, or to misguide the detection of gunshots, or to disrupt the network, public safety will be | x       | x | x | x |
| Transportation          | ● There is no order in the city when traffic information can no longer be trusted          | x       | x |
Table 1.2 (Continued)

| Space exploration | ● Space agencies invest billions into space exploration projects, it is logical that they want to ensure all commands executed on their space probes are authorized, and all their collected data are encrypted and | x | x | x | x |

1.2.1 Security Goals

The security goals ensure the assured message transmission in a network in the presence of malicious nodes. They prevent the network from external attacks and it is achieved by modifying the existing routing protocol.

Authenticity

Authenticity verifies the identity of communicating nodes. Authentication of these nodes is necessary for data processing and for sensor node administration. Adversary can easily inject malicious messages in the network and the receiver nodes must be tuned to frame to receive the data from the exact source before making any decision. Authentication prevents unauthorized access and even legitimate nodes must be able to detect the messages from unauthorized nodes. It can be achieved by sharing the secret key between the sender and receiver to compute a Message Authentication Code (MAC). When the message with correct MAC arrives, the receiver knows that it must have been sent by the sender. Public key digital signatures are too expensive, symmetric key mechanisms are commonly used.
Confidentiality

Confidentiality aims to preserve the secrecy of packets from unauthenticated parties. A sensor network should not deliberately give out sensed data in network. This can be achieved by using cryptographic mechanisms. In most of the existing protocols, symmetric key encryption is preferred since it consumes less node energy.

Integrity

Data integrity ensures the receiver that the data received is not modified by the malicious nodes. WSN are intrinsically unreliable. Malicious node can tamper messages. For example, malicious node may add or manipulate the data in the packet and it may alter the routing path. Message digest algorithms are used to ensure the integrity of such network.

Availability

It is ensuring that the desired service is available whenever required in the network. Nodes have the intelligence to monitor its functionality and make sink/ base stations to be available in the network.

Data Freshness

Data freshness suggests that the data is recent and it ensures that no old messages have been replayed. A key establishment mechanism and receiving time of the packet ensures the freshness of the data between the two nodes.

Flexibility

The primary goal of the flexibility is to allow changes in the architecture of network with enough room for scalability and to provide uninterrupted functionality. Sensor networks will be used in dynamic
battlefield scenarios where sensor may change rapidly. In few applications, sensors may be required to remove additional sensors or to be included into an established sensor network. Furthermore, two or more sensor nodes may be fused into one or a single network may be split into many networks. Protocols that require knowledge of what other nodes will be co-deployed are discouraged whereas protocols with minimal preconceptions are encouraged.

1.2.2 Network Layer Attacks

In WSN, the main attack model is in the network layer. The attacks have been classified into ten types and listed below with their attack methodologies (Karaloff and Wagner 2008, Wang and Tseng 2007, Tran et al 2006).

Spoofed, altered, or replayed routing information

The goal of the malicious node is to exchange the routing information between the nodes. This attack causes the malicious node to create routing loops, attract network traffic, extend or shorten source routes, generate false error messages, make partitions of the network, increase end-to-end latency, etc.

Selective Forwarding Attack

Multihop networks are often based on the assumption of forwarding the received messages to another node. In this type of attack, a node will refuse to forward the messages and simply drop them. It ensures itself that it cannot propagate the message further. Attacker concludes that node has been failed and decides to seek some other route (Sun et al 2007, shila et al 2010).
Sinkhole attack

In a sinkhole attack, malicious node attracts the entire traffic from the surrounding nodes. It creates a figurative sinkhole with the malicious node at the centre. For instance, malicious node advertises a very high quality route to a base station. Using this imaginary route, each neighboring nodes of the malicious node forwards the packets to the base station though the malicious node. It propagates the magnetism of the route to its neighbors. Malicious node creates the large field of influence, successfully by attracting the entire traffic that is destined for a base station.

Wormhole attack

In wormhole attack, the malicious node creates a low latency link between the nodes. This can be done by a variety of means, e.g., by using an Ethernet cable, a long-range wireless transmission or an optical link. The malicious node captures the link on end, transmits the packets through the link and replays them on another end. The malicious node listens the messages at one of the end of the link called as origin point, channelizes them using the wormhole, link and replays them at the other end of the link, called as destination point.

HELLO Flood attack

Many routing protocols requires node to broadcast HELLO packets for identifying the node location. This makes the laptop-class attacker to easily convince every malicious node in the network as its neighbor.

Sybil attack

In sybil attack (Douceur 2002), the malicious node illegally claims that it has multiple identities. It causes false routing in routing algorithms,
data aggregation, voting, fair resource allocation, and foiling misbehavior detection.

**Acknowledge spoofing**

The malicious node can spoof link layer acknowledgements. Its goal is to encourage the source node that weak link has a stronger link and further it conveys that dead node is active. It encourages the destination node to transmit the packet on that link.

**Denial of service (DoS) attacks**

In DoS attack (Aad et al 2008), the malicious node jams the entire network. It makes the node incapable of sending the message or receives. The attack is activated in link layer. The malicious node may intentionally violate the communication protocol. It transmits the messages continuously to generate collisions and thereby reduces the node’s power supply.

**Physical Attacks**

Physical attacks demolish the nodes permanently. The attacker can extract cryptographic secrets, associated circuitry, alter the programs in the sensors or replace them with malicious nodes under the control of attacker.

**Node Replication Attacks**

In the node replication attacks, malicious node adds a node in the existing network by replicating the node ID. It causes the network disconnection, false sensor readings etc. If the malicious node gains the physical access, it copies the cryptographic keys to the replicated node and
inserts the nodes into intentional points in the network for manipulating the network and disconnects the network altogether.

1.3 LITERATURE SURVEY

The primary objective of this dissertation is to provide the detecting schemes in order to improve the performance of the network and ensure secure data transmission. The existing routing attacks and their issues have been addressed to a limited extent. With respect to the issues, the relative literature survey on existing detection schemes of network routing attacks such as selective forwarding attack, wormhole attack, sinkhole attack, sybil attack are carried out and presented.

1.3.1 Selective Forwarding Attack (SFA)

SFA may corrupt some mission critical applications. In these attacks, malicious nodes behave like normal nodes most of the times but selectively drop sensitive packets, such as a packet reporting, the movement of the opposing forces, etc. Such selective dropping is hard to detect. Counter measures cannot detect the malicious nods. If malicious node is present on a route through which packets are forwarded, attackers can simply dropping the packets. Specific detection schemes are required to overcome the SFA.

SFA can cause serious threats on many applications. Attacker can launch the SFA and drop a portion of packets for which it needs to store the layout while forwarding the rest. SFA is hard to detect (Jeremy Brown et al 2008), since packet drops in sensor networks may be caused by unreliable wireless communications or node failures.
1.3.1.1 Multihop Acknowledgement

Multi-hop acknowledgement scheme (Yu and Xiao et al 2006) identifies the malicious nodes in the network by launching alarms based on the acknowledgement received from the intermediate nodes. It has downstream process and upstream process. In the downstream process, packets are transmitted from source to base station whereas in the upstream process, packets are transmitted from base station to source. In this scheme, each intermediate node which lies in the forward path is responsible for detecting malicious nodes. If the intermediate node detects any misbehavior of its downstream (upstream) nodes, it generates the alarm packet and delivers to the source node (base station).

During the initialization process, key server loads unique secret key. The symmetric bivariate polynomial is used to establish the pair wise key between the nodes. The base station is used to encrypt the sensor reports and generate message authentication codes. In the deployment phase, upstream and downstream nodes are identified using the neighbor ID in upstream detection process; report packet, acknowledgement packet, and alarm packet which are used to detect the malicious nodes. When a special event is identified by the source node, it generates the report packet and sends to its neighbor node and it waits for acknowledgement packet. If any intermediate node fails to send the acknowledgement within the predetermined time, then the node suspects from the previous report packet which might have been dropped and an alarm packet is forwarded to the source node.

In the downstream detection process, if any intermediate node receives a report packet which has discontinuous packet ID for a specific source, the node generates an alarm packet and forwards to the base station.
The alarm packet contains the suspicious node ID’s. The packet may also be dropped due to outside jammer or change in routing topology. Since base station receives all the report packets, it is easy to identify and remove the false alarms.

**Advantages**

- Scheme lets both the base station and the source nodes to have the capability of detecting the attacks.
- Even when the base station is temporarily deafened by adversaries, attacks can still be detected.
- Schemes should quickly detect any malicious packet dropping.
- Detection accuracy should be guaranteed even when radio conditions are poor.

**Disadvantages**

- The nodes surrounding the base station are malicious nodes. Then, SFA is still applicable because multiple paths ultimately join the base station.
- It is difficult to distinguish the cause of packet loss either due to compromised nodes or outside jammers.
- Lack of efficiency: nodes take more attempts to detect forwarding attack.
- Security problem: This accuracy of the detection scheme is less attack in some particular condition.
The scheme causes communication overheads due to increase number of paths.

1.3.1.2 CHEckpoint-based Multi-hop Acknowledgement Scheme (CHEMAS)

A lightweight security scheme is used to detect selective forwarding attacks using check point based acknowledgement technique (Bin Xiao et al 2007).

Features:

- The proposed scheme increases the system resilience by preventing sensor nodes to become a malicious node.
- The source node detection mechanism is advantageous. It is capable of making decisions and responding to other nodes even when the base station is defended by surrounding malicious nodes.

Detection Process

The defensive process consists of three phases, a deployment phase, an intrusion detection phase, and decision and response phase. In the deployment phase, each node identifies its neighbor nodes and exchanges the first key. It is required by the Timed Efficient Stream Loss-tolerant Authentication (µTESLA) protocol.

In the detection phase, the random selection of check-point selection strategy is used to detect the malicious node. When a special event is identified by the source node, it generates the event packet and sends to its
neighbor node and it will wait for acknowledgement packet. The check point which lies in the forward path receives the event packet and generates the acknowledgement packet. Then it forwards the packet to the upstream nodes. An alert packet is generated at intermediate nodes that suspects the node as malicious node. Further, the scheme uses MAC for acknowledgement packets to avoid the fabrication/ modification of the alert packets.

In the decision and response phase, malicious node is isolated from the network. By using the statistical techniques or complicated IDS algorithm, the nodes are confirmed as malicious node. Then, an alarm packet is generated and broadcasted to exclude the malicious node from the network.

**Advantages:**

The possibility of either being selected as a checkpoint or being compromised is the same for every node.

- As the selection for each event packet is independent and randomized, it is difficult for an adversary to know the list of checkpoints for the next event packet.

- Detection based approach.

- Allows the base station to collect alert information from the intermediate nodes.

**Disadvantage**

This scheme could be used to transfer ordinary packets, but when the source node generates a very important packet, it should be delivered to
the base station through multiple paths. Prioritizing is not possible and all the packets are treated as equal.

1.3.1.3 Multi Dataflow Topologies (MDT)

The main idea in the MDT scheme (Hung-Min Sun et al 2007) is to detect the selective forward attack using dataflow topologies. Due to packet drop in the network, base station fails to receive the dropped packets from the source. However, the base station can recover the lost information through other data flow topologies. Constructing more than one topology makes the malicious node useless to perform selective forward attack.

Advantages

- Even though packet drop occurs due to malicious sensor nodes the base station can still receive the information through other topologies.

- MDT scheme is lightweight and simple. Sensor nodes do not need to take much effort to detect and identify the malicious sensor nodes.

- The sensor nodes do not need to obtain other routing paths to resend the packets when detecting malicious sensor nodes. Hence, the base station reacts immediately.

- This scheme can also defend against jamming attack and sinkhole attack.
Disadvantages

- Network cost is high.
- Network lifetime will be low due to multi data transmission.
- If attack occurs in all topologies then there will not be any solution to defend the attack.

1.3.1.4 Cumulative Acknowledgement based DEtection (CADE)

Cumulative acknowledgement based detection overcomes the limitations of CHEMAS of SFA (Young Ki Kim, et al 2008). The detection process consists of four phases: Topology construction and route selection phase, data transmission phase, detection phase and analysis phase.

In topology construction and route selection phase, Secure and Energy Efficient Multipath (SEEM) routing protocol is adopted to construct the topology and to identify the routes between the base station and nodes. In the data transmission phase, the base station broadcasts the data-enquiry message to the whole network. Corresponding nodes respond to the data reply packet through multipath. Based on the data reply packets, base station selects the route path and sends the route to the source node. Then, the data transmission starts through the opted routing path. In the detection phase, malicious node is detected by using the following process.

- Timer is set before the transmission phase. The network connectivity parameters Request–ack packets, sequence number and hop counts are noted.
- Each node sets the timer with $2\delta \times \text{hop count} \text{ seconds}$. Where $\delta$ is the maximum transmission delay between two neighboring nodes.

- The node initiates a response packet, acknowledgement packet, route -negative acknowledgement, and the MAC is computed.

- After receiving the response packet, base station runs a decision process.

- If the base station fails to receive a response packet within a predetermined time, it concludes that its neighboring node as a malicious node.

In the analysis phase, the efficiency of the detection scheme is analyzed. The detection scheme detects the malicious node even if the malicious node drops only data packets, route packets, request-acknowledgement packets, false acknowledgements and response packets. It also detects the malicious node if there are any deletions or modifications of acknowledgement and MACs is added by other nodes.

**Advantages**

- The detection scheme detects multiple malicious nodes.

- It also detects the sinkhole attack.

- It does not require time synchronization.
Disadvantages

- Duplicate data-reply packets are generated
- It incurs communication overhead by generation acknowledgement packets when the packet is dropped.

1.3.1.5 Game Theory Model

A different approach based on game theory is used to detect the selective forward attack (Yenumula and Srivathsan et al 2009). This scheme formulated the attack-defense game as a 2-player, nonzero-sum, non-cooperative game, and showed that it achieves Nash equilibrium, thus leading to a defense strategy for network attacks, and significantly increasing the chance of detecting intrusions. In an attack model, two players act as intruders and detectors. The Intrusion detection system stores drop rate, selection of routing path, security levels and calculates the payoff before the packet transmission. If the payoff function bends towards the attacker, it means that the node is a malicious node.

**Advantage:**

Malicious node was found irrespective of the dropping rate.

**Disadvantage:**

The accuracy of the detection will severely suffer due to congestion and other causes of packet dropping.
1.3.2 Wormhole Attack

A wormhole attack (Khabbazian et al 2009) requires two or more malicious nodes that have better communication link than the regular nodes. It is immune to cryptographic technique. It can be launched in the physical layer or to bit level. In physical layer, the replay is done bit by bit even before the entire packet is received. In bit level, the actual physical signal is replayed and is hard to detect.

1.3.2.1 Packet leashed technique

The packet leashed technique (Hu et al 2003, Perrig et al 2006) prevents the packet from traveling farther than radio transmission range. The wormhole attack can be detected by an unalterable and independent physical metric such as time delay or geographical location. The leash is any information added to the packet for restricting the packet maximum. It has two types: geographical leash and temporal leash. The geographical leash ensures that the receiver is located within the certain distance from the sender. The temporal leash ensures the packet has upper bound life time and it restricts the maximum travel distance.

A TELSA with Instant Key (TIK) disclosure protocol is implemented with temporal leash in order to detect the wormhole. It is based on message authentication code. The different stages of TIK protocol are sender setup, receiver boot strapping and sending, and verifying authenticated packets. In sender setup stage, pseudo random function is used to generate the keys. In order to authenticate any packet from the sender, both the sender and receiver are synchronized with each other and the receiver knows the sender hash tree in the boot strapping stage. Secure broadcast authentication is
achieved using hash MAC and it avoids the receiver to forge the authentication information of the packet. Due to delay in retransmission of packets, wormhole attack is prevented from the malicious node.

**Advantages**

- Prevents the wormhole attack.
- Enables the authentication for the messages using MAC.

**Disadvantage:**

- It needs synchronization between the sender and the receiver.

1.3.2.2 **Location–Aware Guard Nodes (LAGNs)**

The LAGNs (Laos et al. 2005) are used to prevent the wormhole attack on wireless ad hoc networks. It is based on graph theoretical approach. It uses the guard node to detect the message flow between nodes. The messages are encrypted using the local broadcast key algorithm. The guard nodes transmit the different hash value of the messages. If any node receives identical messages more than one time, then it is due to the presence of malicious node in the network. The wormhole link is detected by the communication constraint property. In the absence of location or distance bounding probabilistic techniques are used to detect the wormhole link.

**Advantages:**

- This technique uses an analytical model to detect the wormhole link.
- This technique produces a connected sub graph for a geographical model of the networks.
- the accuracy of the detection is improved by using cryptographic protocols.

**Disadvantage**

The drawback of this technique is that the guard nodes are required to know their location and it is suitable for dense stationary sensor node networks.

**1.3.2.3 Anti jamming techniques**

Anti jamming techniques (Cagalj et al 2007) are used to detect the wormhole. In this technique, three approaches: wired pairs of sensor nodes, coordinated frequency-hopping pairs and uncoordinated channel-hopping pairs of nodes are analyzed using probabilistic wormholes. In wired pair of nodes, let $d$ be the length of the wire that connects the pair of nodes. $R_t$ is the transmission time range of transceivers. The attacker jams the region with a jamming range $R_j$. The exposure region is a region which surrounds the jamming region in order to detect the presence of wormhole attack. The drawback of this approach is the requirement of wires in the deployment field.

In frequency via hopping pairs, nodes are connected using wireless to resist jamming. It has two types of nodes. The first type is regular node with single channel radio and the second type is a node with regular radio and frequency shop radio. Frequency hopping pairs with high probability forms at least one wormhole link in the event of a jamming attack. In channel hopping, probabilistic wormholes are created between two channels with large frequency band. The effect of channel interferences is not focused.
1.3.2.4 Statistical Analysis

The statistical analysis (Zhibin Zhao 2010) used to detect the wormhole for multipath routing. Since the nodes are available with the existing routing data, wormhole is created with routing metrics and unnaturally high frequency. An intrusion detection system is designed to detect the wormhole. This method identifies the wormhole link, with the help of drastic change in statistics of routing information stored in the base station or sink node. The statistical analysis includes determination of suspected link and validates the wormhole with time constraint. Wormhole is detected based on the hypothesis.

Advantages:

- This method does not require any time synchronization.
- It does not require any special hardware.

Disadvantages:

- This method works only for on-demand and multipath routing protocols.
- Hidden wormhole link cannot be detected.
- It fails to detect the attack because the affected link appears like normal link from its frequency value.

1.3.2.5 Detection based on topology

The distributed detection (Dezun Dong et al 2011) relies solely on network connectivity information. It detects the wormhole based on topology. It is suitable for continuous geometric surface where each node locally
communicates with neighboring ones and homogenous nodes. This detection scheme has four types of wormholes. Class-I wormhole is the malicious nodes that are located inside the surface. Class-II wormhole has one end point inside the surface and the other end lies on the boundary of the surface. In Class –III type two end points lies on different boundary. Class-IV wormhole has two end points lying in the same boundary. The detection scheme detects single wormhole and multiple wormholes are detected as it is analyzed for various scenarios and it characterizes the final topology. In distributed environment, wormhole design has three components. They are candidate loop selection, finding independent nonseparating loops and seeking knit nonseparating loop pairs. In candidate loop selection, shortest-path tree is established. Loop is constructed from two shortest paths and a threshold value is assigned for the loop. In finding independent nonseparating loop, when the candidate loops passes through the wormhole link, then the link is detected and locates two endpoints of the class-I wormhole and one end point of the class-II wormhole. In seeking Knit nonseparating loop pair, Class III or Class-IV wormholes are detected by topological indistinguishable from a bridge across the candidate loop.

Advantages

- Detects the exact single and multiples wormhole link.
- Based on topology, wormhole is detected in distributed environment.

Disadvantage

- Complex detection scheme.

1.3.3 Sinkhole Attack

Many to one communication is highly vulnerable to sinkhole attack
and causes serious threats in sensor network (Ioannis et al 2008). The existing detections schemes with their merits and demerits are discussed further.

1.3.3.1 Intrusion detection scheme

The detection of sinkhole attacks is based on Intrusion detection (Nagai et al 2006). Base station detects the sinkhole by using data inconsistency of the network using the statistical technique. Let $X_j = X_1, ..., X_n$ be the sensing data collected in a sliding window, $X_j$ is the sensed data collected for the jth node and $\bar{X}$ be their mean. $f(X_j)$ is defined as shown in Equation (1.1).

$$f(X_j) = \sqrt{\frac{(X_j - \bar{X})^2}{\bar{X}}}$$

If $(X_j)$ is greater than the threshold, then the respective node is suspected to be a malicious node.

The base station floods the request message in the network IDs of all the affected nodes. The affected nodes reply to the base station with a message containing their IDs that is ID of the next hop and associated cost. Based on the routing pattern of the nodes, base station realizes that network traffic flows towards the same destination. Further, this technique is enhanced by encryption and path redundancy. Multiple malicious nodes are detected based on the hop count.
Advantages

- Less computation overhead and communication overhead.

- The algorithm is robust to deal with cooperative nodes that attempt to hide the real intruder.

Disadvantages

- Needs improvement in statistical algorithm to find the exact suspected nodes in sinkhole attack.

- Success rate is decreased due to misleading of information in network flow from the colluding nodes.

- Detection is based on selective forwarding attack in the network.

1.3.3.2 Received Signal Strength Indicator (RSSI) based detection

Sinkhole is detected by using Received Signal Strength Indicator (RSSI), (Tumrongwittayapak et al 2009). Initially, nodes are localized with power of the signal at the receiver. The distance between the transmitter and receiver are calculated by using the transmitting power. This method adopts lognormal shadowing model to estimate the loss of the distance and RSSI values to locate the nodes. This method has four Extra Monitoring (EM) nodes and sinkhole detector. The sinkhole detector creates the Visual Graphic Map (VGM) depending on data from the four EM nodes. When a node transmits the message in the network, EM nodes receive the message and RSSI values of the nodes. If the destination node of the received message is a base station, then four EM nodes sends RSSI value to the RSSI based sinkhole detector. The position of the sender is identified and VGM is
updated. If the flow of the received message does not match with the normal flow of VGM, sinkhole is detected.

**Advantages**

- Light weight and robust.

**Disadvantages**

- Depends on extra monitoring nodes.
- Needs improvement in protocol to detect other attacks.
- The position of the base station is fixed.

1.3.3.3 **Link Quality Indicator (LQI)**

The detection scheme using Link Quality Indicator scheme (Choi et al 2009) stores the link cost and calculates the path cost. The LQI is calculated using receiver energy detection, signal to noise ratio estimation or combination of two. The detection scheme consists of network initialization phase and attack detection phase. In network initialization phase, the minimum link cost table is constructed by calculating the LQI value of the communication between the neighbor nodes. The minimum link cost table is used to detect attack when the malicious node tries to change the routing path. The detector node searches the surrounding detector node and computes its optimal path cost between the detector nodes.

In the detection phase, two detection methods are used to detect the sinkhole attack. In method 1, malicious nodes forge and send the routing information to other nodes. The node constructs the minimum link cost table and examines the strength of the table. According to the malicious nodes
action, if the Equation (1.2) is true, neighbor node can suspect that the message is forged.

\[
\text{LinkCost}_{\text{cur}} < \text{LinkCost}_{\text{min}} \times C 
\]  \quad (1.2)

Where

- \text{LinkCost}_{\text{cur}} - \text{cost of the current link}
- \text{LinkCost}_{\text{min}} - \text{cost of the minimum link}
- \text{C} - \text{Tolerance extent of the received signal.}

In method 2, the detector node monitors the route reply messages for detecting the sinkhole attack. It computes the incremental link cost, path cost, and link cost. The incremental link cost is defined as the increment of accumulated link cost in route reply message. The path cost is the minimum cost between the detector nodes and link cost of the detector nodes is the link cost between the detector nodes and the nodes that send route reply message.

\[
\text{IncrementofLinkCost} < \text{PathCost}_{DD} - \text{LinkCost}_{DN} \quad (1.3)
\]

\text{IncrementofLinkCost} :: \text{Increment of accumulated link cost in route reply message}

\text{PathCost}_{DD} : \text{Minimum path cost between detector nodes}
\text{LinkCost}_{DN} : \text{Link cost between detector node and node that sends Routing reply message}

The sinkhole is detected, if the condition stated in Equation (1.3) is true.
This method detects abnormally strong signal by referring to minimum neighbor link cost table. Malicious node voluntarily sends the minimum link cost and examines the strength of the signal.

**Advantage**

- Light weight detection scheme.

**Disadvantages**

- The value of C is based on the applications and surrounding environmental such as radio noise, etc.

- Detection scheme has to be improved.

### 1.3.3.4 Hop Count Monitoring

This method is a novel intrusion detection system (Dallas et al 2007) for sinkhole detection. It has an intrusion detection scheme that imposes thresholds on hop-count variation when the routing path is updated. Hop counts below the lower threshold values suspect the attack and hop count above the upper threshold value identifies the failure of multiple nodes. The detection scheme has training data and it is collected when the base station initializes the network and the routing table is constructed and updated. The training data helps to construct the profile of expected hop counts and thresholds limits are derived. The thresholds values differentiate the normal updates, original updates and network failure updates. The distribution of hop count is modeled using lognormal distribution.
Advantages:

- No false alarms in a simulated network.
- Applicable to any routing protocol.

Disadvantages:

- It needs sinkhole detector.
- It needs to generate forged message containing hop count, broadcast ID, and high sequence number.
- It introduces communication overhead in the network.

1.3.4 Sybil Attack

Sybil node is launched by an external attacker and forms the neighborhood. It joins together to bias the data from the neighborhood. It seriously affects the WSNs in routing, majority voting, congestion, misbehavior detection, data aggregation, etc.

1.3.4.1 Radio Resource Testing

Radio resource testing (Newsome et al 2004) is a technique used to detect the sybil attack in direct communication using probability test. It allocates the different channel for the neighbor nodes to broadcast and to transmit the messages. The node listens to the channel and chooses a random channel for transmission. Let s be sybil node, n are verifier nodes. The probability of not detecting the sybil node for r rounds is defined as 

\[ \left( \frac{n-s}{n} \right)^r \]  

In the difficult case, when there are not enough channels to assign each
neighbour node, the probability test can be done for the subset of the nodes. This is a defensive mechanism for detecting simultaneous sybil attack in direct communication method. This method is suitable for radio communication.

**Advantages:**

- It has the potential to support the protocols that does not require any pre configuration of pre shared secrets.
- It improves the scalability of the network.

**Disadvantages:**

- The radio is not capable of simultaneous sending and receiving of more than one channel. This reduces the usage of channel bandwidth.

### 1.3.4.2 Secure LEACH Protocol

Secure Low Energy Adaptive Clustering Hierarchy (LEACH) protocol against sybil attack improves the security of the network. (Yang Chen et al 2010). It focuses the problem of low energy consumption and high security of WSN. It is based on position and distance of the nodes. Positions of the nodes are calculated using RSSI. When the malicious node changes ID each time, it will broadcast to neighbor nodes and claims itself as cluster head. Using the LEACH protocol, the numbers of cluster heads are continuously collected and the cluster head number selected per round is stable relatively under normal condition. The sybil node is detected based on RSSI when the cluster head number in WSN is over a threshold.
Advantages

- Resistant to sybil attack.
- Consumes less energy.
- Improves the security.

Disadvantages

- The method works only for LEACH protocol.

1.3.4.3 Received Signal Strength Indicator

Received signal strength indicator (Demirbas and Song 2006, Murat and Youngwhan 2006, Satyajayant Misra and Sowmya 2010, Wang et al 2007) is a technique based on signal strength. Let four monitoring nodes have ID D1, D2, D3 and D4 and sybil node forge it’s ID as S1, S2. The node D1 computes the RSSI ratio at time t1, and time t2. If the distance between the two ratios is zero, then the node is confirmed as sybil node.

Advantages:

- Light weight scheme.
- Guarantees less false positives.
- Low overheads.

Disadvantages:

- The nodes are time varying.
- Need collaboration of nodes.
1.3.4.4 Node cooperation method

It is based on node cooperation (Shaohe et al). It uses RSSI technique to infer the distance between the nodes and further determines the positional relation from multiple neighbor nodes. It detects the nodes by observing the nodes identities and distances. It detects the sybil node accurately using node cooperation. The detection process contains three phases: Periodic detection, sybil reorganization, and sybil relaxation. In the periodic detection phase, it observes the overheard packet at time and computes the average RSSI value for overheard ID’s. It groups the node with similar ID and then broadcasts the result if the result is distinct with the previous one. After receiving the group results, it decides to do either sybil reorganization or relaxation. In sybil reorganization phase, Computes the intersection of groups, if all the intersections are empty, it is confirmed that there is no sybil node in the group. If there is a large intersection, the new group is identified as sybil group. In the sybil relaxation phase it computes the intersection of the groups and largest intersection group is chosen. The ratio of the largest intersection to the suspect group is less than the suspect coefficient then the suspect group is isolated from the sybil group.

Advantages

- Detects the sybil node in time.
- Protects the system throughput.

Disadvantages

- It does not detect the multiple nodes.
1.3.4.5 Localization technique

One time localization technique (Abbas et al 2009), detects the sybil node by periodic dissemination of location information. In cluster based scenario sybil nodes are identified by comparing the location of the newcomer with its one-hop neighbors. If the location of any neighbor matches the location of the newcomer’s location, the new identity is detected as sybil identity of that neighbor. If the newcomer is not a sybil node, then cluster head registers the new identity and broadcasts the updated Registered Identity List (RIL) to its member nodes in the cluster and the newcomer provides for further services. In distributed scenario, based on the timer of the updated message, Sybil identity is detected.

Advantages:

- It reduces the communication overhead.

Disadvantages:

- It increases the overheads when node mobility is high.

1.3.5 Performance Metrics

The following metrics are used to evaluate the performance of the network and to find out the effectiveness of the detection schemes.

Packet delivery ratio (PDR): It is defined as the ratio of data packets received by the destinations to those generated by the sources.

Throughput (bits per second): It is the average rate of successful messages is delivered over the communication channel.
**Communication Overhead:** It is the ratio of overheads with and without the detection scheme.

**Average Latency:** It is the mean time in seconds taken by the packets to reach their respective destination.

**Mobility:** It is the speed in which the node moves in the network. Its unit is m/s.

**Detection accuracy:** It is defined in terms of success rate, false positive rate and negative rate. The success rate represents the percentage of detection of malicious nodes correctly. False positive rate represents the percentage of detection of malicious node falsely. False negative rate represents the percentage of undetected malicious node that exists in the network.

**Detection Complexity:**

The complexity of the detection includes the overheads such as memory, computation and energy in the detection scheme. These overheads degrade the life time of the node and deteriorate the network.

**Memory overhead:** It is defined as the amount of memory consumed by the detection scheme.

**Computation Overhead:** It defines that the node consumes excess of computation time due to detection scheme.

**Energy consumption:** It is defined as the amount of node energy consumed by the detection scheme in the network.
Byte Overhead: It is defined as the ratio of the total number of control bytes generated to the total number of data bytes received during the simulation.

1.4 JUSTIFICATION OF RESEARCH

The next generation adhoc networks are targeted for various real-time applications such as health care and medical applications. In these networks the information is to be transmitted in a secured manner and the network must be protected from the intruder. Hence, providing detection schemes (Rajasegarar et al 2008) for various routing attacks is an important objective in designing the forthcoming WSN. The layer based attacks such as physical layer attack, Media Access Control layer attacks, Network layer attacks and Application layer attacks are encountered in WSN (Li and Gong 2008). The most vulnerable attack is network layer that can fail the communication in WSN. It affects the network by sending false information by modified routing table, modified packets, drops the packets, creates fake identities and has an objective to degrade the performance of the network. From the literature survey it is found that, existing detection schemes need improvement in detection accuracy and overheads is to be reduced.

Hence, this dissertation, proposes the following

- CHEAD and EBD based detection scheme for selective forward attack.
- Time and Hop based detection scheme for wormhole attack.
- Digest based detection scheme with hardware simulation for sinkhole attack.
• Node ID based and EH based detection scheme for sybil attack.

• Hardware models Secure AODV and Secure Signaling scheme.

The proposed schemes are simulated in NS-2, Glomosim and Xilinx with constraints to test for the detection of accuracy and network performance.

1.5 THESIS CONTRIBUTIONS AND REPORT ORGANIZATION

Detection of malicious node avoids abnormal event progression, misinterpretation of network routing path and data hacking from the attackers. Detection can be achieved by modifying the existing routing protocol or by designing a secure routing protocol for the specific attack. The detection schemes are based on software approach and hardware approach (Junajo and Rosa 2002). In software approach, the detection scheme consists of six phases. They are as follows.

• Formation of Nodes and its identification.

• Topology identification

• Route selection

• Data transmission

• Detection process and Detection Analysis.

In the first phase of the detection, nodes to be monitored are framed and its exact location is to be identified. In topology identification phase, neighbor list is constructed. In route selection phase, the actual routing path is
selected from the source to destination using the existing routing protocol like DSR protocol, AODV, etc. In data transmission phase, messages are transmitted in the opted routing path. In hardware approach, the proposed detection schemes are based on routing protocol and signal level security (Li and Dai 2007). The implementation of secure routing procedure in hardware level (Hwang et al 2006) provides unique solution in network layer attack. Since the complexity of detection is less, it improves the node’s life and reduces communication and routing overhead. The outline of the research work is shown in Figure 1.2.

**Figure 1.2 Outline of the research work**
In the detection process, malicious nodes are detected by using connectivity measurements like transmission time, link utilization, received signal strength indicator, network traffic, etc. The proposed detection schemes are based on acknowledgment mechanism, energy, round trip time, hash function, node identification, and hop count. In the final phase, malicious nodes are isolated and the detection scheme is analyzed by comparing the performance indicators of the network before and after the application of the detection scheme.

In chapter –I, the literature survey of selective forward attack, wormhole attack, sinkhole attack, sybil attack have been discussed to the required proximity.

Chapter –II explains the detection schemes named CHEAD and EBD for selective forwarding attack that are proposed. The detection schemes are based on cumulative acknowledgement and energy based detection that improves the detection accuracy and energy consumption of the node. Depending on the dynamic topology and mobility of the nodes, detection accuracy of the network varies. Since the network traffic like congestion causes packet drop in the network, cumulative acknowledgement packets and control packets are also vulnerable to threats and attacks, the proposed scheme is simulated in NS-2 Simulator and Glomosim. The simulation results and its analysis with the existing schemes are also presented in this chapter.

Though the detection schemes for wormhole attack are appreciable in static environment, it requires adequate improvement in mobile nodes scenario. The performance degradation is mainly because of its inability of detection, to distinguish the actual routing path and detection time. Hence, a
time and hop based detection scheme is proposed to address the issue of wormhole detection in chapter III. It is based on the round trip time, acknowledgement and cumulative acknowledgement packets. It is incorporated to improve the detection time.

In chapter IV, a deterministic approach towards digest based detection scheme for sinkhole attack is proposed. Since the collision resistance of the digest dictates the message integrity, and it is mandatory to provide improved collision resistant scheme namely modified double devis mayer scheme to detect the sinkhole attack. The functionality test of the proposed scheme is presented with the accuracy of the network. This chapter also incorporates a hardware model of the proposed scheme and features the model such as memory, collision resistant, speed, and power consumption are obtained. This model is simulated in Xilinx and the results are obtained for various target devices.

In chapter V, Node ID based and EH based detection of sybil attack is proposed. The multiple identities in WSN suffer from the problem of sybil attack and it is difficult to detect in mobile environment. The detection accuracy along with various mobility and network traffic are presented. Cryptographic measures, localization schemes are not suitable to detect the sybil attack. Hence identification based scheme and Energy - Hop based scheme are proposed and are analyzed with network throughput and packet delivery ratio of the network.

In chapter VI, the software solutions for the detection of routing attacks in WSN depends on either modifying the routing protocol and network connectivity indicators such as round trip time, received signal
strength indicator, hop count, etc and so on. A unique detection scheme is needed for specific routing attack. To overcome this, a hardware model is proposed based on AODV routing protocol. This chapter also includes a modified direct spread spectrum technique (Ipatov 2005) with rabbit stream cipher in order to achieve the signal level security. Bit error rate and synchronization is improved and it is compared with Elliptic curve cryptography.

The results from each chapter are consolidated and discussed in chapter VII. The scope for future research and the directions in which the future work can be carried out is also discussed in this chapter.