CHAPTER 7

INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS
CHAPTER 7

INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS

7.1 Introduction

Since wireless sensor network has been used for many surveillance applications [204], [205] and military applications operating in hostile environments, it is necessary to provide certain level of protection or fault tolerance to the sensor network so that it can resist the attacks from outsiders. In WSNs, sensors can be put in non-active status to save energy, and only active sensors perform the sensing tasks. Obviously, the denser and more active the sensors are, the better the protection for the objects or the better fault tolerance for the network. Many research activities on sensor networks are focused on how to balance the quality of protection [205]–[209] or fault-tolerance [210]–[212] or both [213]–[216] with energy consumption of the sensors. Security and privacy are rapidly replacing performance as the first and foremost concern in many sensor networking scenarios. While security prevention is important, it cannot guarantee that attacks will not be launched and that, once launched, they will not be successful. Not all types of attacks are known, and new ones appear constantly. Therefore, detection of malicious intrusions forms an important part of an integrated approach to network security.

However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network security. First, unlike traditional networks, sensor nodes are often deployed in large accessible areas, presenting the added risk of physical attack. Second, sensor networks interact closely with their physical environments and with people, posing new security problems. And third, most of the early proposed network techniques assumed that all nodes are cooperative and trustworthy.
7.2 Issues in Sensor Network Security Research

Security architecture for sensor networks must integrate a number of security measures and techniques in order to protect the network and satisfy the desirable requirements we have outlined.

To achieve a secure system, security must be integrated into every component, since components designed without security can become a point of attack. Consequently, security must pervade every aspect of the underlying system design.

In what follows here we describe the most important components that are currently under research in this type of distributed networking. Some of these research issues are similar to those faced in traditional networks, only with some additional constraints; others are unique to sensor networks.

- **Self-Organization:** A WSN is a typical ad hoc network, which requires every sensor node to be independent and flexible enough to use self-organizing and self-healing properties according to the application demands. There is no fixed infrastructure available for the purpose of network management in a sensor network. In the same way that nodes can organize their routes for supporting multi-hop communication, they must also self-organize to conduct key management [217] [218] and build trust relations among sensors. If self-organization is lacking, the damage resulting from an attack or even the surrounding hostile environment can be destructive.

- **Key Establishment:** In the setup of wireless sensor network, the primary requirement is the initiation of security keys for the later use. Many researchers have proposed a range of methods in last few decades for this highly over-rated problem. The main reason behind this is that same protocols cannot be implemented in networks serving diverse fields. The up gradations in the technology of wireless sensor networks render the old techniques vestigial. Many sensor devices in present employment are energy constrained and specific computational algorithm. Thus the public-key cryptography is too expensive in terms of system overhead. Key-establishment techniques are required in the networks with hundreds and thousands of nodes.

- Moreover, having each node sharing a separate key with every other node in the network is not possible due to memory constraints.
Intrusion Detection in Wireless Sensor Networks

- **Time Synchronization**: Most sensor network applications rely on some form of time synchronization [219] between communicating nodes for: (i) energy conservation by turning on and off their radio in predefined time slots, and (ii) computation of a packet's end-to-end delay. Explicit defenses against attacks assume a loose synchronization between cooperating nodes such as μ TESLA [220]. However, secure time synchronization is considered to be a very important but challenging task that has not yet been addressed effectively.

- **Secure Localization**: Some of the most important utilities of sensor networks, e.g. tracking, rely on their ability to accurately locate each node in the network. For example, a protocol designed to locate faults will need accurate location information in order to pinpoint the location of a fault. A number of attempts have been made towards this direction [221] [222]. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc.

- **Secure Data Aggregation**: As WSNs continue to grow in size, so does the amount of data that nodes are capable of sensing. Because of this, a query made by the base station is likely to return a great deal of traffic, much of which is not of interest to intermediate individuals that act as routers. Therefore, it is advantageous to have aggregators for collecting primitive data from a subset of nodes and then process them into more useful sets before actually transmitting them. Secure information aggregation techniques are needed because, as we noted earlier, not all nodes can be considered trustworthy; aggregators can easily alter the received content. A number of attempts have been made towards this direction [223-226] but much more investigation is needed.

- **Secure Routing**: Data forwarding and self routing to enable the communication is essential in wireless sensor networks. However the security algorithms suffer some vulnerability (Chapter 4, 5, 6). An attacker may attempt to launch denial-of-sleep attacks on routing protocol just to expanse the energy of nodes that would result in inconsistent routing. Simple authentication techniques may prevent the network against injection attacks yet some protocols are susceptible to replay attacks or other
attacks of similar category. Securing such protocols is very important, since even a single compromised node could completely paralyze communication in the network.

Autonomic computing provides alternative design paradigms and management techniques to deal with complexity, dynamism, heterogeneity and uncertainty. It aims at realizing computing systems and applications that are capable of managing themselves with minimal human intervention. There have been several efforts [228, 229] to characterize the main features that make a computing system or an application autonomic. In general, an autonomic system must at least support the following four features: self-protecting, self-optimizing, self-healing, and self-configuring. In this autonomic computing paradigm, a component (e.g., hardware resource or a software module) can be used to build into a larger autonomic system where each (compound) component can be configured dynamically to support the required combination of the four properties.

7.3 Motivation
Since the sensors are themselves critical and important objects of the network, a natural query about their protection are always been the consideration in research works. To resist the attacks targeting them in straightforward manner another subject of concern is how and who will secure the network. The above problem falls under self-protection because the sensors themselves are the best solution that can eradicate the problem.

A very less attention is seen in this domain because of the diverseness in the field. However in the works of Dan Wang et al. [230] key element for autonomic computing was witnessed as formal study of the subject. In this thesis the focus is concentrated on the simple mechanisms that can work efficiently for the enhancement in quality of work or object covering, as the sensors if not are self-protected could be the self-destructive in nature.

Another author Yu Wang et al. [231] developed an Efficient Self-Protection Algorithms for Static Wireless Sensor Networks, which is more efficient as compare with existing approaches. He also extends his experiment to simple wireless sensor network [232].

Most of the existing geographic routing protocols have not been designed to work effectively in scenarios with malicious nodes. Some protocols use cryptographic schemes, reputation schemes and other sorts of complex and costly (especially for a wireless sensor network)
solutions to provide security to the routing protocols. Moreover, these schemes are not able to deal with attacks from legitimate nodes compromised (insider attacks). Author [233] analyse in detail the effects of insider attacks (Sybil and Sinkhole) in beaconless geographic routing protocols and propose a Self-Protected Beaconless Geographic Routing protocol. Here we review that just enhancing the forwarding logic of our routing protocol to make additional transmissions when suspicious traffic is detected, we can deal with these insider attacks without the extra cost and overhead of deploying complex reputation systems. Some other Efficient Self-protection algorithms we found are [234] [235], [236], and [237]. They consider that, due to their open nature of the wireless medium an adversary can easily eavesdrop and replay or inject fabricated messages. Authors explained that Different cryptographic methods can be used to defend against some of such attacks. But here we analyse that for node compromised those methods can do little, which is another major problem of WSN security as it allows an adversary to enter inside the security perimeter of the network, which raised a serious challenge for WSNs.

7.4 Attacks on Wireless Sensor Networks

Self-organized sensor networks once deployed provides the applications in almost all domains autonomously or without manual interference. Some of the popular attacks are briefed in this segment.

7.4.1 Jamming

The interference in the radio frequencies of the network is caused by jamming. Only few nodes are enough to launch the attack with considerable amount of destruction. The adversary can restrict the entire network.

7.4.2 Tampering

This attack may damage the sensor node and replace its segment or the complete node to gain the access of sensitive information. The nodes tempered are easy source of shared cryptographic keys and access of higher layers.

7.4.3 Spoofed, Altered or Replayed Routing information

Also known as one of the most direct attack the spoofing, replaying or altering the information of routing leads the attacker to create complications in protocols and generate
loops for attraction and repulsion of traffic, generating false error messages, partitioning of network, false error messages or extending source routes or shortening of source.

7.4.4 Selective Forwarding
Selective forwarding attack enables the adversary to present itself as the active candidate of the path. Thus the attacker decides to drop or forward the packets causing black hole.

7.4.5 The Sybil Attack
A malicious node with multiple identities is termed as Sybil attack in the network. The attack is designed to confuse the routing protocols as the node advertises itself as the active route path to multiple locations of the network.

7.4.6 Wormholes
Wormhole attacks are the intelligent attacks as the intended nodes tracks the information from one side of network and replay the same with lower latency link to other side of system. Convincing the nodes about the identity as their neighbour is not challenging and the quick dispense of energy is sustained by attack. An attacker that is placed near to the base station are most vulnerable as the wormholes created disrupt the network completely by convincing nodes about the wormhole that they are couple of hops away against wormhole.

7.4.7 Hello Flood Attacks
A hello message is the common initiation in WSN for the announcement of presence in network to the neighbours. Such messages are considered as the active senders within range and the neighbouring nodes awake for transmission. The attacker with high power antenna convinces the nodes as active transmitter and dissipates the nodes energy.

7.4.8 Selective Forwarding Attack and its Variants
Karl and Wagner [239] in their work studied the selective forwarding attack. The attack sometimes is also referred as Grey Hole attack as the dark nodes simply does not generate voids in active path and allow few packets to pass in network.

The selective forwarding is of different forms. In one form of the attack the selective forwarding states about the malicious nodes that selectively drops the packets coming from
the x location or a cluster of nodes. This behaviour leads to DoS attack for that particular node or cluster of nodes.

The nodes also behave as the blackhole that refuses the forward transmission of packets. The malicious nodes act as illiterate candidates responsible for anonymous behaviour in node forwarding and the packets against the routing protocols are dispatched to random nodes. Another form of selective forwarding attack is Neglect and Greed. In these attacks, the subverted nodes arbitrarily drop the route of some packets [238]. The nodes however participate in the protocols of lower level and even may acknowledge data reception to sender but actually drops random messages. Such nodes are neglectful. When the nodes facilitate the highest priority to its own messages they are termed as greedy. Moreover, another variance of selective forwarding attack is the time delay in packet transmission inserted via nodes to create confusion among sensor nodes about routing protocols.

Fig. 7.2 below shows how the selective forwarding attack works through a simple example. The selective forwarding attack may be happened in the link from node S to node A in several ways. In the path to the sink, node S forward or send the packets to its neighbour node A but node A stop forwarding the packets from node S. Otherwise, node A may forward the packet to an unknown malicious node through a high-quality route for eavesdropping [239].
7.4.9 Black Hole Attack
Black hole attacks are severe vulnerabilities for the routing protocols in the sensor network. The attack counterfeits the presence of other nodes by advertising itself as the shortest active route to the destination. The node attracts the traffic and drops the packets consecutively [243]. Black hole is categorized under denial of service attack series. The source node looks forward to transmit data and signals Route Request (RREQ) messages in environment. Malicious node receives the signal and corresponds with the Route Reply (RREP) message as soon as possible. Thus the sending node entertains the request as the shortest distance to the destination.

7.5 Related Work for Black Hole Node Detection
There are number of mechanisms proposed for the detection of malicious nodes proposed by various researchers in their work. A sequential study of the works provide base for understanding the black-hole node problem and the constraints in detection schemes further evaluated by performance parameters.

Wu Yuanming et al. in [244] discussed about the vulnerabilities in security of watchdog mechanisms [245] and trust mechanism. The authors examined the potential of exploitation carried about by attackers. Their work can be illustrated in a three step mechanism: 1) Monitoring of node behaviour, 2) management of trust, 3) detection of insider attack.

Marti Guili et al. in [245] proposed about the mechanism for watchdog that works on eavesdropping concept. The node overhears the transmissions within the radial range of transmission.
The watchdog mechanism is not so popular mechanism due to certain limitation like overhearing method. This mechanism was modified in the works of A. Forootaninia [246] who fixed the cluster head node and the packets received were stored in buffers.

S. Banerjee in [247] proposed algorithm to mitigate the grey hole and black hole attacks. The algorithm divides the complete data set into small blocks and relies on network for finding and uncovering the malicious nodes. The nodes that are adjacent cooperate in delivery of packets from source destination to the end destination. The acknowledgment signal from the end destination is the key element in the detection of malicious nodes.

Jian yin et al. in [248] stated about the hierarchical routing protocol for security against the black-hole node attack. The scheme is base on symmetric key cryptography for discovery of secure routing against the attacks. In this routing the network of secure routing protocol is divided in various groups that are organized as tree where the root is the group leader. After key establishment of inter-group and intra-group, the detection of black hole is carried out locally. For cooperative black-hole detection a randomized scheme for data acknowledgement is proposed.

In [247], Karakehayov proposed a technique in which transmitting SN performs power control to transmit a packet to more than one SNs in the direction of the BS. If an SN that is on the forwarding path does not forward a packet, then its next hop neighbour on the forwarding path will identify this event and report the SN as a black hole. This scheme is very expensive – for a network with $n$ black hole nodes, for each original message, $O(n)$ extra messages are required, which is very expensive.

In [250], the proposed an extension for WSNs, which addressed the combined objectives of security and reliability. In [251], Shu et al. proposed enhanced techniques based on the multi-path routing design proposed by Lou et al. in [250] and [249] to mitigate black hole attacks in the network. They consider the black hole region as illustrated by us in Section I. The best technique was called the Multicast Tree Assisted Random Propagation (MTRP). In MTRP, instead of using deterministic multi-path routes to the BS to transmit data from the SNs, Shu et al. proposed the use of randomized routes. A share is routed in the direction of the BS on a randomized path until it traverses a pre-specified number of hops to a forwarding node. Subsequently, the share is routed deterministically to the BS from the forwarding node.
Intrusion Detection in Wireless Sensor Networks

Nitesh Gondwal et al. [252] propose a technique that uses routing through multiple base stations only when there is a chance of occurrence of black-holes in the network. Otherwise routing through nearest base station is done to reduce extra use of messages in the network. Hence, it reduces the consumption of energy in the network by the node which is a major factor which is limited and is to be considered carefully in the sensor networks. Check agent plays a major role in the detection of black-holes in the network and also reduces extra overhead from the network. The data delivery is ensured as there is a provision of using multiple base stations in the network. But the work can be done further to handle the message complexity and to use less number of base stations in the network for better delivery results in the wireless sensor networks.

7.6 Proposed work for black hole detection

After formulating the problem in different way, the proposed methodology is expressed as below.

- Simulate the Traditional AODV protocol, Without Malicious Nodes.
- Calculate the network efficiency parameters for AODV routing protocol without attack.
- After that we are adding some malicious nodes which co-operates each other in dropping packets coming from source node which originate for the destination.
- Calculate the network efficiency parameters for AODV routing protocol with Cooperative Black Hole attack in order to check how much the efficiency was degraded by the co-operative black holes in the network of normal nodes.
- After that we have to add a mechanism to the current AODV protocol which suffers from Cooperative Black Hole attack, as described in the section below.

Since, some of the mobile devices are malicious in the group of nodes selected, so a detection scheme must be used in order to manage a good routing efficiency.

To analyze the effects of Cooperative black holes, we simulated the wireless ad-hoc network with and without a black hole node present in the network. To do that, we have to innovate a new protocol from traditional AODV protocol, which we called “Modified AODV”. This new protocol, modified AODV is inherited from the existing AODV routing protocol, it contains a watch mechanism to detect the behavior of device that it is malicious or not, it also
Intrusion Detection in Wireless Sensor Networks

contains a mechanism in which source monitors devices that a device in its communication path is co-operates a malicious node or not.

In Watch mechanism, each node keeps two extra tables, one is known as pending packet table and another one is known as node rating table. There are four fields in pending packet table, Packet ID, Next Hop, Expiry Time and Packet Destination.

I. Pending packet table

<table>
<thead>
<tr>
<th>Packet ID</th>
<th>Next Hop</th>
<th>Expiry Time</th>
<th>Packet Destination</th>
</tr>
</thead>
</table>

- Packet ID: ID of packet sent.
- Next Hop: Address of next hop node
- Expiry Time: Time-to-live of packet
- Packet Destination: Address of destination node.

There are also four fields in node rating table, Node Address, Packet drops, Packet forwards and Misbehave. This table updated corresponding to pending packet.

Table. I. Node rating table

<table>
<thead>
<tr>
<th>Current Node Address</th>
<th>Packet Drops</th>
<th>Packet Forwards</th>
<th>Misbehave</th>
</tr>
</thead>
</table>

- Node Address: Address of next hop node.
- Packet Drops: Counter for counting the dropped packet.
- Packet Forwards: Counter for counting the forwarded packet.
- Misbehave: It has two values 0 and 1, 0 for well behaving node, 1 for misbehaving node.

We use Internal Black hole attack from cooperative malicious nodes, This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node. Firstly we have introduced some normal nodes in the network, after that
Intrusion Detection in Wireless Sensor Networks

we introduce a group of nodes which are cooperative and oppose the current behaviour of the network. It is difficult to route data when there are number of malicious nodes in our network.

![Diagram](image)

**Figure 7.3: Different node configuration for black hole detection**

7.6.1 **Used Watch Mechanism for cooperative black hole detection:**

In pending packet table, each node maintains track of the packets, it sent. It contains a unique packet ID, the address of the next hop to which the packet was forwarded, address of the destination node, and an expiry time after which a still-existing packet in the buffer is considered not forwarder by the next hop.

In node rating table, each node maintains rating of nodes, which are next to it (means nodes are within its communication range). This table includes the node address, a counter of dropped packets noticed at this node and a counter of successfully forwarded packets by this node.

The fourth field of the above node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node misbehave value will be 1 (means it is interpreted as a misbehaving node), otherwise it is deliberated as a legitimate node. An expired packet in the pending packet table causes the packet drops counter to increase for the next hop correlated with the pending packet table entry. Each node listens to packets that are inside its communication range, and only to packets associated to its domain. Then, it checks each packet and prevent forged packet. If it
Intrusion Detection in Wireless Sensor Networks

notices a data packet in its pending packet table, then it deletes this data packet from pending packet table after authenticating the packet. If it notices a data packet that exits in its pending packet table with source address different from the forwarding node address, then it increases the packet forwarding value in node rating table.

For determining whether a node is misbehaving or act as a legitimate one, rest on the selection of threshold value. For example if we assume a threshold value of 0.5. This means that as long as a misbehaving node is transmitting twice packets as it drops it will not be distinguish. If we assume a lower value of threshold then it will increase the percentages of false positives.

After finding a misbehaving node, a node will attempt to do local repair for all routes passing through this misbehaving node. If local repair process fails, then it will not transmit any RERR packet upstream in the network. This process attempts to prevent a misbehaving node from dropping packets, and also prevent blackmailing of legitimate nodes. To avoid constructing routes, which traverse misbehaving nodes, nodes drop all RREP messages arriving from nodes currently marked as misbehaving. To stop misbehaving node to act actively in a network, the all packet starting from this node has been dropped as a form of punishment.

*Introduced mechanism proposed an algorithm is as follows:*

1. Data packet forwarded or sent.

2. Copy and keep the data packet in pending packet table until it is expired or forwarded

3. If (data packet forwarded)

   
   Increment the corresponding forwarded packet in the node-rating table and remove the data packet from pending packet table.
   Update the current Node number which routes the data, and also update the previous routing node number from which the current node receives the packet.

4. If (data packet expires in the pending packet table)
Increment the corresponding dropped packet in the node-rating table and removes the data packet from pending packet table.

If (dropped packet > threshold (th1)) then
{
  If ((dropped packet / forwarded packet) > threshold (th1))
  {
    Node is misbehaving, update the misbehaving node counter.
    Promiscuous node locally tells all the node of its wireless range from node rating table that particular node (misbehaving node 2) and the previous node (misbehaving node 1) which route the data packets to that particular node are misbehaving node.
    Discard RREP message coming from the misbehaving node 1
  }
}

Figure 7.4: The Concept of Monitoring a Node from a Source

In our mechanism, if a source broadcast a RREQ to nodes, corresponding nodes reply back with the RREP, this RREP also contains address of next hop node (NHN). If node A replies to the RREQ and lists node B1 as its NHN in the RREP message. Source does not trust node A and sends an FREQ (forward request) to Node B1 which sends back the FREP (forward reply). In similar manner, if node B1 replies to the FREQ and lists node B2 as its NHN in the
Intrusion Detection in Wireless Sensor Networks

RREP message. Source does not trust node B1 and sends an FREQ to Node B2 which sends back the FREP. If Node B2 is cooperating with B1 Node, no black hole is identified here. But now if Node B1 is the intermediate node and the situation is similar to the one black hole problem.

The difference in case of multiple malicious nodes is that after a node is identified malicious (node B2) all the nodes on the path from this black hole to the node which acted as the first Intermediate node (node B1) would be identified as black holes as the Node B1 cooperates Node B2 to drop the packet, and their identities broadcasted over the network.

7.7 Results

![Figure 7.5: Distribution of Normal, malicious and sink nodes on 100*100 meter](image)

Figure 7.5: Distribution of Normal, malicious and sink nodes on 100*100 meter

![Figure 7.6: End to End delay for Routing protocol without attack depends, upon the number of rounds delay factor increases, as we moves for more number of round then delay increases accordingly.](image)

Figure 7.6: End to End delay for Routing protocol without attack depends, upon the number of rounds delay factor increases, as we moves for more number of round then delay increases accordingly.
Figure 7.7: Throughput calculation of Normal routing protocol

Figure 7.8: comparative analysis of end to end delay with or without black hole attack

Figure 7.9: Through put is better under normal operation, but once under attack it reduces drastically with respect to number of round.
7.7.1 Simulation results

Black hole detection:

- Node 46 sends FREP to Source Node
- Packet Dropped By Node 46
- Hence, Node 46 is a Malicious Node
- Since Node 38 Cooperates Node 46
- Hence, Node 38 is also a Malicious Node

7.8 Conclusion

The requirement of security has always been the parallel issue along with the evolution of Wireless Sensor Networks. The chapter first describes the critics of security requirements followed by the threat models that surfaced with power to bypass the security parameters. Also, in vulnerable environment of operation, the attacks are still unknown and broad in classifications are required to be mitigated. The focus of this section was to create a WSN with self-Protection features. Generally speaking the motive is to design the system that mitigates any ridiculous method prone to attack the system. Considering the Black Hole node attack model, the solution we seek is available in Autonomic Computing. The simulation results prove the efficiency of our system managing the constraints of energy resources of the system.