Abstract

In most of the applications, wireless sensor networks (WSNs) are deployed in an unattended environment. Thus, sensor nodes can be physically captured by the adversaries, and the adversaries can then extract the stored information in those nodes using the power analysis attacks. Using the extracted information they can manufacture new sensor nodes. These newly manufactured sensor nodes can also have additional functionalities, which can be used to launch different attacks. After that these new sensor nodes can be deployed by the adversaries in the network. These nodes can launch different attacks in the network, which can cause information loss along with high energy expenditure. Furthermore, WSN is prone to various attacks, such as blackhole attack, wormhole attack, sinkhole attack, etc.

In a blackhole attack, an attacker can physically capture and re-program a set of nodes in the network to block the packets they receive instead of forwarding them towards the BS. Any information that enter in the blackhole region is then compromised, and the information does not reach to the destination. This produces high end-to-end delay, and decrease in packet delivery ratio and network throughput. As a result, the information cannot reach to the destination node within the required time period.

In a sinkhole attack, an attacker node first advertises a best possible route (with less hop-distance route) to the destination (BS) to attract its neighbors so that they may fall into this attraction to utilize the advertised route more frequently. The neighbors can then forward their traffic through the efficient advertised route declared by the sinkhole attacker node. The route can also captivate other nodes apart from the neighbor nodes of the sinkhole attacker node, which are closer to the sinkhole than the BS. So, the attacker node has an opportunity to tamper with the data, damage the regular network operations or conduct other serious threats.

Sometimes multiple attacks can also be launched in the network using the hybrid anomaly. Hybrid anomaly degrades the network performance rapidly and also trouble the attack specific detection mechanisms. In this situation, it is very crucial to find out what kind of anomaly is activated in the network.

In the presence of blackhole attack, sinkhole attack and hybrid anomaly, the confidential information can be delayed, leaked, altered or even can not reach to the destination. Therefore, it becomes essential to provide robust and efficient solutions for the detection and prevention of blackhole attack, sinkhole attack and hybrid
anomaly in HWSN. This motivates us to propose new detection and prevention protocols for these types of attacks in HWSN.

In this thesis, we propose several intrusion detection and prevention schemes in hierarchical wireless sensor networks (HWSNs). The first contribution is on designing a new efficient group-based scheme for the detection and prevention of multiple blackhole attacker nodes in HWSNs. In our scheme, the entire WSN is divided into several clusters, and each cluster has a resource-rich cluster head (CH) node. Each CH is responsible for the detection and prevention of blackhole attack in the network. For the detection purpose, each CH uses the proposed detection algorithm by which it sends status-cum-data query messages to all its cluster members (sensor nodes). CH then waits for the reply to those messages from its members. Node status messages (e.g. sleeping, working, idle) are merged with data query messages in order to further reduce the total communication cost of the proposed scheme. After the detection of blackhole nodes, CH nodes use the proposed responsibility reassignment algorithm in order to reassign the responsibilities of the blacklisted nodes (blackhole attacker nodes) to the normal nodes. Our scheme is secure against blackhole attacker nodes, which is shown through the analytical and simulation results using the widely-accepted NS2 simulator. The proposed scheme achieves about 90% detection rate and 3.75% false positive rate, which are significantly better than the existing related schemes. Furthermore, our scheme is efficient, and thus, it is very appropriate for practical applications in HWSNs.

In the second contribution, we propose a new detection scheme for the detection of different types of sinkhole nodes in HWSNs. To the best of our knowledge, this is the first attempt to design such a detection scheme in HWSNs which can detect sinkhole message modification nodes (SMD), sinkhole message dropping nodes (SDP) and sinkhole message delay nodes (SDL) nodes. In our approach, the entire HWSN is divided into several disjoint clusters, and each cluster has a resource-rich high-end sensor node (called a cluster head), which is responsible for the detection of different sinkhole attacker nodes if present in that cluster. Our scheme is secure against sinkhole attacker nodes, which is shown through the analytical and simulation results using the widely-accepted NS2 simulator. The proposed scheme achieves around 95% detection rate and 1.25% false positive rate. These factors are significantly better than the previous related schemes. Furthermore, the computation and communication efficiency is achieved in our scheme. As a result, our scheme is also
suitable for the sensitive critical applications, such as military applications.

In the last contribution, we propose a new intrusion detection technique for hybrid anomaly in HWSNs, which uses the existing data mining algorithm, called $K$-means clustering. For detection purpose, patterns of intrusions are built automatically by the $K$-means clustering algorithm over training data. After that intrusions are detected by matching network activities against these detection patterns. We evaluate our approach over a HWSN dataset that is created using Opnet modeler, which contains various attributes, such as end-to-end delay, traffic sent and traffic received. The training dataset contains the normal values of the network parameters. The testing dataset is created in actual working mode consists of normal and abnormal values of the network parameters. The proposed technique has the ability to detect two types of malicious nodes: blackhole and misdirection attacker nodes. The proposed scheme is useful, especially for those scenarios where the chances of occurrence of hybrid attacks are high and attack specific detection mechanisms fail. It can automatically detect the hybrid anomaly. Our scheme achieves 98.6% detection rate and 1.2% false positive rate, which are significantly better than the existing related schemes.

**Keywords:** Wireless sensor networks, intrusion detection and prevention, blackhole attack, sinkhole attack, hybrid anomaly, security, simulation.