Chapter 3

Review of Related Works

In this chapter, we first provide a taxonomy of various security protocols proposed in wireless sensor networks (WSNs). We then provide brief literature survey on user authentication, access control and user access control in WSNs. Finally, we give the detailed review on the existing schemes of intrusion detection and prevention in WSN as it is our main focus in this thesis work.

The security protocols proposed in WSNs can be categorized in various kinds, which are shown in a taxonomy form in Figure 3.1. The key management, user authentication, access control, user access control, and intrusion detection and prevention are the main security issues in WSNs.

![Figure 3.1: Taxonomy of security protocols in WSNs](image-url)
3.1 Key distribution in WSNs

The key distribution in WSNs is achieved through the bootstrapping protocol, which establishes cryptographically secure communication links among the communicating sensor nodes. This protocol must not only enable a newly deployed sensor node to initiate a secure infrastructure, but it must also allow sensor nodes deployed at a later time to join the network securely. However, it is a challenging area due to resource limitations of sensor nodes as well as vulnerable to physical capture of nodes by an adversary in a sensor network.

A bootstrapping protocol involves the following three phases [19], [29].

- **Key predistribution:** This phase is executed prior to deployment of the sensor nodes in a particular target field or deployment area. A key set-up server (usually, it is the base station) pre-loads a set $K_{SN_i}$ of keying information (for example, symmetric keys) to each deployed sensor node $SN_i$ in a sensor network. Note that $K_{SN_i}$ is called the key ring of $SN_i$.

- **Direct key establishment:** This phase is executed by each sensor node once the sensor nodes are deployed in the target field. Each sensor node first locates all other sensor nodes with which it can communicate directly and secretly. We call two sensor nodes $SN_i$ and $SN_j$ as physical neighbors if they are within the communication ranges of one another. $SN_i$ and $SN_j$ are then key neighbors if they share one or more key(s) in their key rings $K_{SN_i}$ and $K_{SN_j}$. Now, $SN_i$ and $SN_j$ can secretly and directly communicate with each other if and only if they are both physical neighbors and key neighbors, and they are called as direct neighbors. In this phase, each sensor node $SN_i$ locates its direct neighbors. For this purpose, $SN_i$ can broadcast its own ID and the IDs of the keys from its key ring in order to establish pairwise keys with its neighbor nodes.

- **Path key establishment:** This is not a mandatory phase. Thus, if this phase is executed, it adds to the secure network connectivity of the network. Assume that two physical neighbors $SN_i$ and $SN_j$ fail to establish a direct key between them in the direct key establishment phase. $SN_i$ and $SN_j$ can then discover a secure path between them. Once the path is discovered, a new secret pairwise key is transmitted securely along that path. However, the main difficulty in this phase is the discovery of a secure path between $SN_i$ and $SN_v$. Also,
3.1 Key distribution in WSNs

the communication and computation overheads increase significantly with the number of hops of the discovered path.

A bootstrapping protocol for sensor networks needs to satisfy the following requirements [18]:

- Deployed sensor nodes must be able to establish secure node-to-node communication.

- Illegal sensor nodes should not be able to gain access into the network, either through packet injection or masquerading as a legitimate sensor node.

- One can always deploy new sensor nodes dynamically at any time after the initial deployment and these additional deployed nodes can form secure connections with the already deployed nodes in the network. Hence, the bootstrapping information must always be present and can not be simply erased after deployment to prevent compromise in the event of sensor nodes capture by an adversary.

A bootstrapping protocol also needs to satisfy the following evaluation metrics [18]:

- It should support a large-scale sensor network and must be flexible against substantial increase in the size of the network even after initial deployment of the sensor nodes in a sensor network.

- The amount of memory required to store security credentials must be minimum.

- The number of messages exchanged during a key establishment procedure must be less.

- The amount of processor cycles required to establish a secret key between two communicating sensor nodes should be minimum due to resource limitations of sensor nodes.

- The network connectivity is the probability that two sensor nodes can establish a secret key. Enough network connectivity must be provided for a WSN to perform its intended functionality.
• The resilience against node capture attack of a key distribution scheme is measured by estimating the fraction of total secure communications that are compromised by a capture of \( c \) nodes *not including* the communication in which the compromised nodes are directly involved. In other words, we want to find out the effect of \( c \) sensor nodes being compromised on the rest of the network. For example, for any two non-compromised sensor nodes \( SN_i \) and \( SN_j \), we have to find out what is the probability that the adversary can decrypt the secret communications between \( SN_i \) and \( SN_j \) when \( c \) sensor nodes are already compromised? Let \( P_e(c) \) denote the fraction of total secure communications compromised after capturing \( c \) sensor nodes by an attacker in a sensor network. If \( P_e(c) = 0 \), we call a key establishment scheme as *unconditionally secure against node capture* or *perfectly resilience against node capture*.

According to the probability of key sharing between a pair of sensor nodes, the key management schemes in WSNs can be divided into probabilistic and deterministic in nature. Pietro et al. [106] proposed a deterministic key management protocol, which is based on the Logical Key Hierarchy (LKH). In their scheme, the base station is treated as a key distribution center (KDC), and all keys are logically distributed in a tree rooted at the base station.

Zhu et al. [155] proposed a deterministic key management protocol for sensor networks, called the Localized Encryption and Authentication Protocol (LEAP). Lai et al. [82] further proposed a deterministic scheme, which establishes the pairwise session keys between any two neighboring nodes. It is scalable and also energy efficient.

Eschenauer and Gligor [49] introduced a random key predistribution scheme for sensor networks, which relies on probabilistic key sharing among the nodes of a random graph. Chan et al. [18] proposed the \( q \)-composite scheme, where at least \( q \) common keys are needed to be shared between the key rings of nodes during the key setup phase in order to build a secure link between any two neighboring nodes.

Liu and Ning [89] proposed a polynomial pool-based key distribution scheme. Two neighbor nodes can establish a secret key if they have at least one common symmetric bivariate polynomial \( f(x, y) \) of degree \( t \). The main drawback of this scheme is that if more than \( t \) nodes in the network are compromised by an adversary, he/she can easily reconstruct the original polynomial using the *Lagrange interpolation* [62].
As a result, all the pairwise keys shared between the non-compromised nodes using this polynomial will also be compromised. Thus, this scheme is unconditionally secure and \( t \)-collusion resistant. Although increasing the value of \( t \) can improve the security property of this scheme, it is not feasible for wireless sensor networks due to the limited memory in sensors. Du et al. [46] also presented another pairwise probabilistic key predistribution scheme, which is similar to Liu-Ning’s scheme [89]. However, the schemes presented in [30], [32], [34], [39], [40] provide better security and network performances as compared to other existing key distribution schemes in WSNs.

### 3.2 User authentication in WSNs

User authentication is another important security aspect needed for secure communication in WSN. In user authentication, a legal user can query and collect the real-time data at any time from a sensor node or cluster head in the sensor network as and when he/she demands for it. Since most of the critical applications in WSNs (for example, battlefield scenario, healthcare, etc.) are real-time based, users are generally interested in accessing real-time data from the sensor nodes. Therefore, the users (also called the external parties) can be allowed to access the real-time data directly from the sensor nodes inside WSN directly instead of accessing data from the base station. This is because the information from the sensor nodes are collected periodically by the base station, which may not be always real-time data. Thus, the user authentication problem becomes a very important topic in research of WSN security, which makes a significant attention in the research community in recent years.

The existing user authentications protocols proposed in the literature for WSNs usually fall into two categories: (i) password-based user authentication schemes and (ii) biometric-based user authentication schemes. According to the authentication type and factor, the protocols can be further divided into three categories: single-factor, two-factor and three-factor. In single-factor authentication schemes, the user’s smart card can be only used. In two-factor authentication schemes, the user’s smart card and password can be used. Finally, in three-factor authentication schemes, the user’s smart card, password and biometrics can be used.

The user authentication schemes proposed by Watro et al. [138], Wong et al.
Tseng et al. [128], Tsern et al. [85], Ko [77] and Liu et al. [93] come under single-factor password based authentication. The user authentication schemes proposed by M. L. Das [43], Nyang et al. [102], Huang et al. [66] and Khan et al. [75] fall under two-factor password based authentication. The schemes proposed by Yuan et al. [145], and Das and Bruhadeswar [38] fall under biometric-based user authentication. Yuan et al.’s scheme [145] uses very similar concept as in M. L. Das’s scheme and it cannot resist denial-of-service attack and sensor node compromise attack. However, it supports freely changing password locally without contacting the base station in the network as compared to other password-based user authentication schemes.

3.3 Access control and user access control in WSNs

In an access control scheme, there are two tasks [67], [153]: node authentication and key establishment. In node authentication phase, a deployed sensor node needs to prove its identity to its neighbor sensor nodes and also to prove that it has the right to access the existing sensor network. After node authentication, in key establishment phase, the shared secret keys are established between a deployed node and its neighbor nodes to protect secure communications among them.

Depending on the authentication type, the access control protocols are divided into two broad categories: (i) certificate-based access control and (ii) certificate-less access control. The certificate-based access control schemes can be further subdivided into hash-chain based and hash-chain less access control schemes. Huang-Liu [67] proposed a certificate-less access control scheme based on the one-way hash function. Huang [64] and Kim-Lee [76] proposed ECC-based access control schemes using the hash-chain. Zhou et al. [153] and Huang [65] proposed the certificate-based hash-chain less access control schemes.

User access control mechanism is used to provide the access rights for the correct information and resources for different services in WSNs. Using user access control, an authorized user can access only those information for which he/she is permitted to access them. Some of the user access control schemes proposed in WSNs include Wang et al.’s scheme [131], Mahmud-Morogan’s scheme [94] and Le et al.’s scheme [83], which are based on ECC.
3.4 Intrusion detection in WSNs

The intrusion detection protocols detect any suspicious activity occurring in the network. The following intrusion detection protocols have been proposed in the literature.

Guechari et al. [56] proposed an efficient approach for detection of DoS attacks in HWSNs. Their method is based on the election of controller nodes, called cNodes, which observe and report DoS attack activities. The role of cNode is to analyze traffic and then send back a warning to the cluster head, if any abnormal traffic is detected. Their proposed dynamic solution further improves the network lifetime by minimizing the energy consumption for each sensor node.

In WSN, an intruder can be a moving object deployed by the enemy in the battlefield. With uniformly deployed sensor nodes, the detection probability is same at any point. But the detection probability is application specific and can also vary as per the location. The sensor nodes deployed using the Gaussian distribution can provide the differentiated detection capabilities at different locations. Wang et al. [136] analyzed the problem of intrusion detection in a Gaussian-distributed WSN by characterizing the detection probability with respect to the requirements of applications. They considered the single sensing detection and multiple-sensing detection scenarios. The performance of Gaussian-distributed WSNs is compared with the performance of uniformly distributed WSNs.

In WSN, intrusion detection is a mechanism to detect the existence of static or moving attackers. Wang et al. [137] discussed this issue to characterize WSN parameters, such as node density, sensing range, etc. in terms of a desirable detection probability. They considered the issue according to homogeneous and heterogeneous WSN models. They computed the detection probability by considering single-sensing detection and multiple-sensing detection. The simulation results validate the analytical values for both homogeneous and heterogeneous WSN models.

Yu et al. [144] discussed various types of attacks and countermeasures related to trust schemes. An extensive literature survey was presented by summarizing state-of-the-art trust mechanisms in two categories, namely, secure routing and secure data.

Shin et al. [120] discussed the various intrusion detection systems for wireless industrial sensor networks. They provided the classification of various methodologies
against intrusions. They further proposed a hierarchical framework for intrusion detection and data processing. Their main focus was on one-hop clustering, which was not addressed in the previous schemes. They implemented some logical protocols in the hierarchical framework of intrusion detection and prevention.

Rajasegarar et al. [110] proposed two techniques for anomalies detection in WSN. The first technique is called the centered hyperellipsoidal support vector machine (CESVM), which is based on linear programming-based hyperellipsoidal formulation. But CESVM approach has limited scope for distributed implementation in WSNs. The second approach was the distributed anomaly detection algorithm that used a one-class quarter-sphere support vector machine (QSSVM). Both CESVM and QSSVM techniques achieved high detection accuracies on various data sets.

Tiwari et al. [126] proposed a specification based IDS for WSNs. Their proposed scheme optimizes the local information into global information in order to compensate the communication pattern in the network.

Zhang et al. [150] proposed a new method for traffic classification, which can improve the classification performance effectively by incorporating correlated information into the classification process. Their method was analyzed from both theoretical and empirical perspectives. Various experimentations were also performed on two real-world traffic data sets to validate the proposed method. However, the detection accuracy of their scheme is 90%, which is less than that for other existing schemes.

Heinzelman et al. [61] discussed the communication protocols, which can have significant impact on the overall energy dissipation of the networks. The traditional protocols of direct transmission, multihop routing, and static clustering are not optimal for WSNs. So, they proposed LEACH (Low-Energy Adaptive Clustering Hierarchy), an energy efficient clustering-based protocol for WSNs, that further distributes the energy load among the sensor nodes in the network.

Xie et al. [142] then proposed a K-nearest neighbor (KNN) based anomaly detection technique, in which a hyper grid intuition based approach is applied. The computational complexity is reduced by redefining anomalies from hypersphere detection region to hypercube detection region. The detection accuracy of their scheme is about 96%. However, the false positive rate is 8%, which is very high.

Abduvaliyev et al. [6] provided a survey on various intrusion detection system (IDS) in WSNs. A classification of different IDS schemes according to the em-
ployed detection techniques is done. They further discussed three categories such as anomaly detection, misuse detection and specification-based detection protocols. They also explained various WSN attacks and corresponding intrusion detection systems to tackle those attacks. Modares et al. [98] also discussed the security aspects of WSN.

Su [125] proposed a technique to detect flooding attacks in real-time based on genetic weighted $KNN$ classifiers. This scheme uses the genetic algorithm to train an optimal weight vector for features, and unsupervised clustering algorithm is used to reduce the number of instances in the dataset, which further shortens training and execution time and provides improved accuracy. The proposed system can identify DoS attacks from the network traffic within a very short duration of time. The proposed system also achieves 95.86% overall accuracy.

Wang et al. [130] presented a survey on recent advances in WSN research. They summarized the special features of sensor data collection in WSNs by comparing with both wired sensor data collection network and other WSN applications.

Xie et al. [141] discussed the key design principles for anomaly detection techniques in WSNs. They presented the analysis and comparison of the approaches belonging to a similar technique category.

Li et al. [86] proposed an intrusion detection system based on $KNN$. The classification is done to separate the abnormal and normal nodes. They analyzed the parameter selection and error rate of their proposed model. They have shown that the proposed model has a high detection rate ($DR$) and speed. However, their scheme has a high false positive rate ($FPR$).

### 3.4.1 Blackhole attack detection in WSNs

Wazid et al. [139] measured the affect of blackhole attack on the performance of WSN, and then a technique for detection and prevention of blackhole attack was proposed. Their technique has some limitations, such as it is not applicable for multiple blackhole attacker nodes and it has high communication cost.

Prathapani et al. [107] discussed the vulnerability of a wireless mesh network (WMN) to blackhole attack. The intelligent agents, called honeypots, are used to detect these attacks. The honeypots generate dummy Route Request (RREQ) packets to lure and trap blackhole attackers. They demonstrated that honeypot based detection model aids in the increase of throughput in a WMN. Though their
technique has a high detection rate, it has high false positive rate.

Misra et al. [97] proposed an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission. However, their scheme achieved good packet delivery ratio but it has high FPR.

Gao et al. [51] proposed a technique to detect and defend blackhole attacks by improving the AODV (Ad-hoc On-Demand Distance Vector) routing protocol by combining flow analysis. Their results were evaluated for SAODV (secure AODV) and mAODV-TA (modified AODV protocol and Traffic Analysis) protocols with varying number of attackers. However, their technique has low DR and high FPR.

Table 3.1 summarizes the technique used and limitations/drawbacks of the existing protocols for detection and prevention of blackhole nodes.

Table 3.1: Summary of techniques used and limitations/drawbacks of the existing protocols for blackhole attack detection

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Technique used</th>
<th>Limitations/drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wang et al. [137]</td>
<td>single and multi sensing detection</td>
<td>low DR</td>
</tr>
<tr>
<td>(2008)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tiwari et al. [126]</td>
<td>packet dropping rule</td>
<td>deployment of watch dog produces overhead and consumes network resources</td>
</tr>
<tr>
<td>(2009)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shin et al. [120]</td>
<td>hierarchical intrusion detection</td>
<td>low DR with high hop counts</td>
</tr>
<tr>
<td>(2010)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Misra et al. [97]</td>
<td>BAMBi (multiple base stations based detection)</td>
<td>high FPR, PDR with one base station, and high computation cost</td>
</tr>
<tr>
<td>(2011)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wazid et al. [139]</td>
<td>blackhole attack detection and prevention</td>
<td>high communication cost</td>
</tr>
<tr>
<td>(2013)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wang et al. [136]</td>
<td>Gaussian and uniform distributed WSN</td>
<td>low DR with less number of nodes</td>
</tr>
<tr>
<td>(2013)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gao et al. [51]</td>
<td>AODV</td>
<td>low DR and high FPR</td>
</tr>
<tr>
<td>(2014)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Li et al. [86]</td>
<td>$KNN$ classification based IDS</td>
<td>high computation cost</td>
</tr>
<tr>
<td>(2014)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: $DR$: detection rate; $FPR$: false positive rate; $PDR$: packet delivery ratio
3.4.2 Sinkhole attack detection in WSNs

Ngai et al. [101] proposed a lightweight technique for detecting sinkhole attack. In their technique, the attackers are detected by observing the network flow information. A many-to-one communication model is used in which the routes are established based on received route advertisements. The scheme has less communication and computation overheads. But the success rate of the scheme is less in case of high drop rate.

Wang et al. [135] proposed an integrated intrusion detection system (IIDS) for a cluster based WSN. The proposed system is capable to resist the attacks by doing the real-time analysis of network data. The proposed system consists of three types of IDSs, such as intelligent hybrid intrusion detection system (IHIDS), hybrid intrusion detection system (HIDS) and misuse intrusion detection system. The detection is performed using anomaly and misuse detection modules, which gives high detection rate with low false positive rate.

Hamedheidari et al. [58] proposed a mobile agent based defense mechanism against sinkhole attack. They used mobile agents to aware all sensor nodes from its neighbors through a three-step negotiation, which makes them not to listen the traffics generated by the malicious sinkhole attacker nodes. In the performance evaluation, the scheme is evaluated in terms of mobile agent energy consumption, packet loss rate and throughput. The use of mobile agents produces the network overhead, which is a drawback for WSN.

Fessant et al. [50] proposed a technique to describe the impact of selective-forwarding attacks in tree-based routing protocols. Their proposed protocol is effective and improves the resilience of WSN against sinkhole attacks.

Zhu et al. [156] proposed a technique to detect node replication attack in which adversaries prepare their own low-cost sensor nodes and then deploy them in the deployment field that causes the network to accept them as legitimate nodes. To prepare the clone of a sensor node, an adversary can physically capture a sensor node and extract all its confidential information, such as keys, used for the communication, its identification number (ID), etc., and then reproduce their own nodes by using the extracted information and deploy them in the network at some strategic positions.

Shafiei et al. [117] proposed a method to identify energy holes (sinkholes). Sinkhole attacker nodes are detected using a centralized model. A lightweight mitigation
method is also provided to eliminate sinkhole attacker nodes.

Rajasegarar et al. [111] proposed a distributed hyperspherical cluster based algorithm to identify anomalies in WSN. The implementation of their proposed scheme on a real WSN testbed is also performed. The distributed hyperspherical cluster-based scheme has better detection accuracy with less communication overhead as compared to the centralized scheme in which all sensor nodes communicate to a central node for processing.

Zhang et al. [148] proposed a redundancy mechanism to prevent sinkhole attack. In this technique, messages are sent to the suspicious nodes through multiple paths. The sinkhole attacker nodes are identified on the basis of replied messages received from the suspicious nodes. However, their proposed scheme has low detection rate.

Sreelaja et al. [121] proposed an ant colony optimization attack detection (ACO-AD) algorithm to detect sinkhole attacker nodes. In this scheme, nodes generate an alert if they identify any sinkhole in the network. A voting based method is used to identify sinkhole attacker nodes. Their proposed technique identifies the anomalous connections without generating false positives and with minimum storage memory use of sensor nodes.

Nahas et al. [100] proposed a routing approach to protect WSN against the wormhole and sinkhole attacks, which is called the Secure-Path Routing (SPR). Their method uses expected path risk as a parameter in routing to reduce the traffic flow over the nodes, which are vulnerable to holes attacks. But the problem with the selection of low risk routes may lead to the choice of routes which can consume large energy. Thus, they implemented an algorithm that balances the risk with other path selection parameter, such as energy consumption. They also evaluated the trade-off between security and energy consumption. During the experimentation, it has been observed that the proposed technique is quite effective as it increases the traffic flow over legitimate routes, and its impact on the network lifetime is also negligible.

Krontiris et al. [80] proposed an intrusion detection system to protect WSN against sinkhole attack. Some rules are designed and embedded in the IDS system for the successful detection of sinkhole attack. However, their proposed scheme has low detection rate.

Garofalo et al. [52] proposed a decision tree classification based technique for the detection of sinkhole attack. There is a trade-off between high detection rate and energy used in detection process. So, a light weight detection technique is
implemented on motes in order to save energy. Sinkhole attack dataset has been created and utilized to evaluate the effectiveness of the proposed scheme.

Giruka et al. [55] surveyed the state of art approaches in securing WSNs. Several security techniques of WSN were reviewed. They mainly focused on authentication, key management and distribution and secure routing techniques available for intrusion detection in WSNs.

Hai et al. [57] proposed a lightweight IDS for cluster-based WSN. An algorithm was proposed to minimize the triggered intrusion modules in the network by using an over-hearing technique to reduce the sending alert packets. Their proposed technique is capable to detect most of the routing attacks in WSN. During the experimentation, it has been observed that their technique requires less energy consumption as compared to the other techniques. However, their technique has high false positive rate up to 10% in some cases.

Du et al. [47] proposed a secure and efficient routing protocol for heterogeneous sensor networks. Their scheme specifically utilizes the powerful high-end sensors. During the experimentation, it has been observed that their secure routing protocol achieves better routing performance than the existing directed diffusion technique. The delivery ratio of their scheme decreases with increase in failure nodes. The delivery ratio is good with more number of L-sensors which decreases drastically in case of less number of L-sensors.

Dallas et al. [27] proposed a method for the detection of sinkhole attack. They monitored the hop-count parameter in order to detect sinkhole attack. Their scheme is computationally efficient for detecting the abnormal route advertisements that are used to perform sinkhole attack.

Roy et al. [112] implemented a dynamic trust management system (DTMS) that counters two severe attacks (sinkhole and blackhole attacks) in WSN. Their technique ensures that network architectures do not require redefinition for every specific attack. It can handle both attacks at the same time. The drawback with such schemes is that they require high computation cost which creates energy consumption issues in low powered sensing devices.

Papadimitriou et al. [104] introduced two cryptographic techniques to secure WSN against sinkhole attack. The objective of their technique is to provide continuous protection against the sinkhole attacker nodes rather than its detection. Their proposed cryptographic protocols are effective against the sinkhole attack as they
can successfully protect the network against sinkhole attacker nodes.

Chen et al. [22] proposed a technique to protect the large scale wireless sensor networks against sinkhole attack. The detection problem is formulated as a change-point detection problem in which they monitor the CPU usage of each sensor node and predict the normal or abnormal behavior on the basis of CPU usage. Their proposed technique is capable to differentiate among normal and abnormal sensor nodes (attacker nodes). However, CPU usage is also more in case of other attacker nodes e.g. blackhole, wormhole nodes or in some other attacks. Therefore, it is very difficult to confirm that the suspicious node is sinkhole attacker node by using the proposed scheme.

Traditional cryptographic schemes used in the development of trust-aware routing protocols do not effectively address the problems associated with multihop routing. The sybil, sinkhole and wormhole attacks are possible in WSN. So, to secure WSNs against adversaries misdirecting the multihop routing, Zhan et al. [146] proposed a trust-aware routing framework (TARF) for dynamic WSNs. TARF is efficient as it provides trustworthy and energy-efficient routes without requiring time synchronization and geographic information of sensor nodes. The TARF module is implemented and demonstrated on TinyOS platform. Simulation results prove its effectiveness against the various routing attacks.

Qi et al. [109] used MultiHopLQI routing protocols to protect the WSN against sinkhole attack. The MultiHopLQI routing protocol adopts LQI (link quality indicator) that indicates the last packet as the criterion for parent selection. The aim of MultiHopLQI mechanism is to ensure that a message reaches to the BS within time and in an accurate form.

Salehi et al. [115] proposed a detection mechanism for sinkhole attack. Their suggested algorithm first identifies a group of suspected nodes, and then the sinkhole attacker nodes are confirmed on the basis of network flow information. Their technique has low detection rate and high false positive rate.

Sharmila et al. [118] proposed a message digest algorithm based technique to detect sinkhole attack in WSNs. The proposed technique ensures the integrity of the transferred messages using a trustable path.

Finally, the summary of the techniques used and limitations/drawbacks of the existing state-of-art protocols for sinkhole attack detection is provided in Table 3.2.
3.4 Intrusion detection in WSNs

Table 3.2: Summary of techniques used and limitations/drawbacks of the existing protocols for sinkhole attack detection

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Technique used</th>
<th>Limitations/drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Du et al. [47] (2007)</td>
<td>Two Tier Secure Routing (TTSR)</td>
<td>very low PDR with less number of L-sensors</td>
</tr>
<tr>
<td>Wang et al. [137] (2008)</td>
<td>Single and multi sensing detection</td>
<td>low DR</td>
</tr>
<tr>
<td>Krontiris et al. [80] (2008)</td>
<td>Cooperative detection by using intersection of neighbor lists</td>
<td>low DR</td>
</tr>
<tr>
<td>Wang et al. [135] (2011)</td>
<td>IHIDS for the sink, HIDS for CH and misuse IDS approaches</td>
<td>low DR and high computational cost</td>
</tr>
<tr>
<td>Wang et al. [136] (2013)</td>
<td>Gaussian and uniformly distributed WSN</td>
<td>low DR with less number of nodes</td>
</tr>
<tr>
<td>Salehi et al. [115] (2013)</td>
<td>Grouping of suspected nodes and network information flow based detection</td>
<td>high FPR</td>
</tr>
<tr>
<td>Hamedheidari et al. [58] (2013)</td>
<td>Mobile agent based detection</td>
<td>high network overhead</td>
</tr>
<tr>
<td>Shafiei et al. [117] (2014)</td>
<td>Energy holes estimation using geostatistical hazard model</td>
<td>energy expenditure maps can create problem in network congestion areas that further affects DR and FPR</td>
</tr>
<tr>
<td>Zhang et al. [148] (2014)</td>
<td>Redundancy mechanism</td>
<td>low DR</td>
</tr>
</tbody>
</table>

Note: DR : detection rate; FPR : false positive rate; PDR : packet delivery ratio

3.4.3 Hybrid anamoly detection in WSNs

Zhang et al. [149] presented a classification scheme for the network traffic. Their scheme improves the performance of classification with a few training samples. The F-measure of their scheme can be increased, if the number of classifiers can be added and tested.

Zhang et al. [151] presented a random forests classification based intrusion de-
tection framework. The random forests algorithm is used for misuse detection and analyzing the patterns of intrusions. Their framework improves the performance of detection by combining anomaly and misuse detection approaches. Their scheme achieves 94.7% $DR$ and 2% $FPR$, which is high as compared to other existing schemes. However, intrusions with high degree of similarity can not be detected by their scheme.

Hwang et al. [70] presented a hybrid intrusion detection system. This hybrid system has the advantages of low false-positive rate of signature-based intrusion detection system, and it has also the ability to detect unknown attacks. Their scheme has low false alarm rate, but it has also low detection rate.

Sachan et al. [114] performed a topological analysis of WSN in the presence of misdirection attack. Further, they proposed an algorithm for the prediction of delay and throughput. However, their scheme proposed for delay and throughput prediction considers only a single attack scenario.

Qazanfari et al. [108] presented a hybrid anomaly-based intrusion detection method that combines two different methods. These methods are trained in a supervised way. They used the following additional techniques in order to improve the performance of their approach. In the first technique, a feature selection method using the entropy of features is used for extracting optimized information from KDD data set. In the second technique, a method is proposed to combine the results of these two learning based methods. Their scheme is applicable for network intrusion detection, which is based on the support vector machine (SVM) and multilayer perceptron (MLP) based hybrid detection technique.

Chitrakar et al. [24] applied the hybrid learning approach that combines K-medoids based clustering technique followed by the Naive Bayes classification technique. The detection rate of their scheme is low and also has high false positive rate. Furthermore, the computational cost is high as their scheme is based on both K-medoids and SVM.

Aneetha et al. [11] then proposed an intrusion detection framework for known and unknown attacks. Their framework has the ability to detect intrusion in real time environment from the link layer. However, they considered only the flooding and packet dropping.

Agarwal et al. [7] presented an anomaly detection system based on the entropy of network features and SVM. Their scheme has 97.25% detection rate and 2.75%
3.5 Summary

false positive rate, which can be further improved. Arya et al. [12] presented a hybrid intrusion detection system that uses the signature and anomaly information together. The detection rate of their scheme is less (around 83%). In addition, their scheme needs high computational overhead. Chakraborty and Nagwani [17] presented an extended partitioning based K-means clustering technique. Their scheme performs clustering when the number of clusters and number of objects are also increased.

Elbasiony et al. [48] presented a classification and clustering-based hybrid anomaly detection framework. The random forests algorithms is used in their approach in order to detect the misuse by building intrusion patterns from the training dataset. These patterns are then matched with the network connections to detect network intrusions. The K-means clustering algorithm is used to detect the intrusions by clustering the network connections for anomaly detection. In addition, their technique has high false positive rate.

Muda et al. [99] also presented an intrusion detection system with moderate accuracy and detection rate. They gave a hybrid learning approach through the combination of K-means clustering and Naive Bayes classification. Their approach is used to cluster all data into the corresponding group before applying a classifier for classification purpose.

3.5 Summary

In this chapter, we have first discussed a taxonomy of various security protocols in WSNs, such as key distribution, user authentication, access control and user access control. In addition, we have reviewed the intrusion detection techniques used in WSNs. More specifically, we have discussed the existing methods for blackhole and sinkhole attacks detection, and also the hybrid anomaly detection techniques in WSNs. However, it is noted that most intrusion detection schemes proposed in the literature are either inefficient or have low detection rates/high false positive rates.