Intrusion Detection Systems

Ashwini V. Jatti, V. J. K. Kishor Sonti

Abstract: Intrusion Detection System is competent to detect the intrusions and alerting the administrator of system about the signs of possible intrusions. This paper presents a detailed review of the intrusion detection techniques used in WSNs. More specifically, the existing methods for blackhole and sinkhole attacks detection are reviewed. 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. This survey also highlights the research gap in this domain and provides better scope for the advanced work.

Keywords: Intrusion detection; Blackhole; Sinkhole; Detection Rate; Wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks (WSNs), nowadays have came out as a most capable platform for many applications such as Surveillance of battlefield, monitoring of traffic, monitoring of healthcare and environment. Sensor nodes with limited resources have many different features, like sensing, processing and communication for fulfilment of many different application requirements. Sensors in WSNs are mostly deployed in areas, where there is restriction for human accessibility and where they use unguarded wireless medium for communication. Computational power and communication channel are the factors for resource-constrains in nodes in WSNs. Hence while designing security systems for sensor networks guideline for designing should confirm for resources of nodes and their limitation. General security requirements for WSN are as follows:

i. Authentication: WSNs before granting permission for revealing information must authenticate base stations, cluster heads and sensor nodes.

ii. Reliability: Entity or message to be considered must not be changed in WSN. It should be reliable.

iii. Confidentiality: In WSNs privacy of wireless communication medium must be provided for prevention of false reports injection.

iv. Availability: WSNs must ensure availability of desired network services despite of denial of service attacks.

v. Non-repudiation: Malicious nodes will not able to hide their actions.

vi. Authorization: WSNs must ensure that sensors nodes having authority can only provide information to network services.

vii. Novelty: WSNs must ensure that data must be updated and latest, and no old messages should be replayed by adversary.

Limitations of sensor nodes of the WSN which are challenging task for providing the security WSNs requirements are as follows:

i. Restricted resources: Every sensor node comprises of a processor with low computational power and small memory for programmes.

ii. Limitation of life time: Every sensor node operates on power battery. So, after several weeks or months of operation, some nodes in the network may exhaust their power and therefore the protocols for security must be energy efficient.

iii. Limitation of communication ability: Every sensor node is capable for communication between each other and the base stations (BSs) at low bandwidth by using short range wireless radio transmission.

iv. Insufficient knowledge for deployment configuration: Earlier post deployment network configuration cannot be decided in many applications. Hence, it may not be always possible to use algorithms having strong dependence on locations in a sensor network of sensor nodes for security.

Further the manuscript is divided into sections describing the literature review on intrusion detection system, black hole and sink hole.

II. INTRUSION DETECTION SYSTEM

Systems that are able for detection of intruder and provide an alert about node which tried make disturbances into a system or a network is called as Intrusion detection system (IDS). IDS are a collection of activities that are discovered, analyzed, reported as unauthorized and damaging actions. Detection of any kind of breach in confidentiality and integrity, resources availability is the aim of IDS. Traditional IDS have following primary components: 1) To monitor and analyze action sensors or agents are used, 2) Information collected by the sensors or agents is centralized by management server and manage them, 3) All data created by the IDS is stored in database server. 4) A console is used for many following functions where it provides connection between users and administrators to check the updated data of the system monitored, collect alert messages, inspect events and constitute the system.

Figure 1 Basic IDS block diagram [1]
Intrusion Detection Systems

Based on six criteria IDS techniques are classified as follows:

1. Target system: The proposed surroundings for the IDS are described in this criterion.
2. Detection technique: IDSs in this criterion are distinguished for analysis on basis of their basic approach.
3. Assembly method: Behaviour and traffic based are the two IDS in this criterion.
4. Trust model: IDS in this criterion classify from standalone IDSs from raw data or analysis results.
5. Scrutiny method: IDS in this part, various from sophisticated data mining approaches to simple pattern matching.

Figure 2 Intrusion detection techniques for wireless networks [2]

Krontiris et al. (2007) [3]: Distributed Intrusion detection system which used a plenty of independent but localized and cooperating agents for detecting a node introducing a sinkhole attack model was described by krontiris. They demonstrated, in the overall case of random topologies for confirmation of effectiveness and algorithm’s accuracy, simulation was illustrated by deploying sensor network.

Farooqi and Khan (2009) [4], classified IDS as purely distributed, purely centralized and distributed centralized. The whole performance of wireless sensor networks is affected because the networks are exposed to a many attack which are inside the network. Erroneous analysis of this sensor field is resulted due to these attacks. So, use of IDS with energy-efficiency arises which would work in scattered way and for identification of abnormal behaviour of nodes, they must cooperate with other nodes.

Zhijie and Ruchuang (2012) [5] by using Markov model for sensor nodes they proposed an traffic prediction algorithm which is efficient. Authors have design an IDS for detecting selective forwarding attacks, DOS attacks based on traffic prediction algorithm. For achieving detection mechanisms and the simulations include reported malicious attacks, NS2 as a simulation tool was used. Based on the results it can be observed that less computation cost and less communication cost with high detection ratio is obtained by the proposed scheme of authors.

Rassam et al. (2013) [6], presented online anomaly detection model which can measure the sensor variations in principal component space. Authors conducted experiments based on real world dataset using Sensorscope system and compared their model results with earlier model results. They found their model is giving high detection rate along with few false positive rates.

Maleh et al. (2015) [7], used support vector machine (SVM) algorithm for IDS which included a learning algorithm and for detecting malicious behaviours and lightweight IDS, which is based on attack signatures. Simulation results showed lower false alarm, high detection rate and can efficiently detect abnormal events.

Sajjad et al. (2015) [8], presented an evaluation-based anomaly IDS with low weight neighbour node with reliable computation. Using MATLAB, proposed intrusion detection system was implemented with random node deployment and a simulation area of 200 x 200 sq. m. Simulations were performed with size of 60, 80, 100, 120,140, 160, 180, and 200 nodes. By analysis of the network statistics and malicious node behavior selective forwarding attack, Hello flood attack, jamming attacks are detected successfully by this proposed scheme. Simulation results prove that network is performing better with anomaly-based IDS and neighbour node trust management.

Butun et al. (2015) [9], presented an outline of IDS for hierarchical WSNs, based on multi-level clustering. This IDS provides two frameworks namely “downwards-IDS” and “upwards-IDS”. Member nodes intrusion is identified by Downwards IDS and cluster heads intrusion is identified by upward IDS. Result showed that as the intrusion detection probability of system decreases with increase in maximum hop count and vice versa.

Guechari et al. (2012) [10] had presented an effective method for spotting DoS attacks. This technique uses cNodes which are nodes used for controlling, which are elected to detect and give information of activities of DoS attack. cNode evaluate any traffic and cluster head receives an
alert message, if any abnormal traffic is detected. Network lifetime is improved by minimum energy consumption.

Wang et al. (2013) [11] Intrusion detection problem was analyzed in a Gaussian-distributed WSN, according to application requirement by characterizing the probability of detection.

Detection by single sensing and multiple-sensing scenarios were measured. Uniformly distributed WSNs with Gaussian-distributed WSNs performances were compared. Wang et al. (2008) [12] presented an issue to distinguish WSN parameters, in relation to node density, sensing range, required detection probability by considering single and multiple sensing were discussed. Homogeneous and heterogeneous WSN models were considered for issues. The values analytically heterogeneous and homogeneous WSN models were validated by simulation results.

Yu et al. (2012) [13] did a review on secure routing and secure data related to trust schemes, different kinds of countermeasures and attacks were discussed.

Shin et al. (2010) [14] for wireless industrial sensor networks, the various intrusion detection systems were discussed. For intrusion detection and data processing, authors additional implemented a hierarchical outline. Main aim was to emphasis on one-hop clustering, which in the earlier systems were not addressed.

Rajasegarar et al. (2010) [15] for anomalies detection in WSN two techniques were presented. The first technique namely Centred hyperellipsoidal support vector machine (CESVM) which is based on linear programming. Then for distributed implementation in WSNs, CESVM has limited scope approach. Another technique viz., Quarter-Sphere Support Vector Machine (QSSVM) which is based on distributed anomaly detection algorithm.

Tiwari et al. (2009) [16] presented IDS for WSNs based on specification where local data was combined with global data to pay off the communication pattern in the network.

Zhang et al. (2013) [17] proposed a technique which improve the classification performance by including correlated information into the classification process. Both theoretical and empirical perspectives were used for analysis of their method. For validation of the presented method, various experiments on two real-world traffic data sets were performed.

Heinzelman et al. (2000) [18] proposed the communication protocols, in which total energy dissipation of the networks had a large effect. For WSNs, static clustering, the traditional protocols of direct transmission and multihop routing were less favourable. An energy effective clustering-based and more in the network, it also allocates the energy load between the sensor nodes namely Low Energy Adaptive Clustering Hierarchy (LEACH) protocol was used.

Xie et al. (2013) [19] presented a K-nearest neighbour (KNN) where method based on a hyper grid intuition is applied and it is based on anomaly detection technique. By defining differences between hypersphere and hypercube detection region the computational complexity can be reduced. Their scheme has accuracy of detection around 96%. Still, the FPR is very high which is nearly 8%.

Abduvaliyev et al. (2013) [20] in WSNs, a review on different intrusion detection system (IDS) was provided. Based on the active detection methods, categorization of various IDS schemes was done. Three classes were further discussed namely, specification-based detection, anomaly detection and misuse detection protocols. Different attacks in WSN and related IDS (intrusion detection systems) which would handle those attacks were also explained by them.

Su (2011) [21] proposed a technique viz., KNN classifiers for detection of flooding attacks in real-time. For training an optimal weight vector for features, this scheme uses the genetic algorithm and unsupervised clustering algorithm was used for reducing the number of instances in the dataset. Overall accuracy of 95.86% also can be achieved by this proposed system.

Wang et al. (2011) [22] presented a review on current advances in WSNs and compared with wired sensor network. Xie et al. (2011) [23] discussed the key design principles required in WSNs for anomaly detection. Li et al. (2014) [24] presented KNN based IDS. For separation of abnormal nodes from normal nodes, classification was done. They obtained higher detection ratio. Still high false positive rate (FPR) was drawback of their scheme.

3. Black Hole Attack

In WSNs confidential data can be leaked or altered as WSNs are prone to many various kinds of attacks. The attacker in blackhole attack can physically capture and for blocking the packets, in the network they change the data of nodes, which is received instead of transmitting them towards the base station (BS). Attacker compromise information which is entered in blackhole and does not allow them to reach the destination. This increases end-to-end delay, and it decreases network throughput and packet delivery ratio. Therefore, within the required time period, destination node does not receive the appropriate information.

Wazid et al. (2013) [25] the impact on the performance of WSN of blackhole attack was measured, after that a method to detect and also prevent blackhole attack was implemented. This method was not applicable for multiple blackhole attacker nodes, which was the limitation to method and communication cost is very high.

Prathapani et al. (2009) [26] the wireless mesh network (WMN) weakness to blackhole attack was discussed. These attacks were detected by, the intelligent agents, called honeypots. To trap and trick blackhole attackers, dummy Route Request (RREQ) packets are generated by honeypots. There was increase in throughput in a WMN was proved by this method. Even it had high false positive rate, this technique had a high detection rate.

Misra et al. (2011) [27] introduced an efficient technique that uses several base stations installed in the...
network to counter the effect of black holes on data transmission. This method has drawback of high FPR but packet delivery ratio is good. Gao et al. (2014) [28] by improving the AODV routing protocol, they presented a method for detection and defending blackhole attacks by merging analysis of flow. Results for mAODV-TA and SAODV protocols were evaluated by changing number of attackers. Yet, their mechanism has high FPR and low DR.

Simulation results depicted improved use of bandwidth, better PDR, less end to end delay and good throughput. Sarathe and Shrivastava (2018) [59] reviewed techniques and methodologies which were used for detection and prevention of blackhole attack in MANET with AODV routing protocol. Authors considered three cases for the simulation, SAODV with and without black hole attack and extended SAODV algorithm. These methods have merit such as higher packet delivery and demerits namely, higher overhead, higher packet loss and increased end to end delay.

### III. SINK HOLE ATTACK

In this attack, an attacker node which is sinkhole node promotes a greatest probable path to the BS, due to this, neighbour nodes are misguided for frequently usage of this path. Attacker node then receive a chance to interfere with the information, regular process of the network is damaged or further serious threats are conducted. Then the malicious node to misguide its neighbours, exploits a compromised node to introduce the attack where path with a smaller number of hops distance is promoted. The neighbours are assured to transmit all the traffic through this promoted route. The path fascinates the sinkhole neighbours and other nodes which are far from BS than sinkhole.

Ngai et al. (2007) [29] for detecting sinkhole attack, presented a lightweight mechanism. In this method, by observing the network flow data, the attacker nodes are detected. They use many-to-one communication model where the routes are created based on received route advertisements. Even in case if drop rate is high, scheme success rate is low, the method has less communication and computation overheads.

Wang et al. (2011) [30] implemented an integraded IDS for a cluster based WSN. Author demonstrated three categories of such systems namely, misuse IDS, hybrid IDS and Intelligent IDS which resulted in low false positive rate with high detection rate.

Hamedheidari and Rafieh (2013) [31] presented defense technique for sinkhole attack based on mobile agent. In this mechanism there are three step negotiation, where mobile agents are used to aware all sensor from its neighbours, due to this sensor nodes are not able to pay attention to the traffics created by the attacker nodes. Mobile agent, packet loss rate, energy consumption and throughput, are the terms considered by the technique for estimation. Drawback for WSN is the network overhead which is created due to use of mobile agents.

Fessant et al. (2012) [32] presented an algorithm in tree-based routing protocols for detecting the effect of selective forwarding attacks. Flexibility of WSN against sinkhole attacks is improved and also effectiveness is obtained by this method.

Zhu et al. (2012) [33] they presented an algorithm for detection of node replication attack, where low-cost sensor nodes are created by enemies by their own and further

### Table 1 Blackhole attack detection techniques and its limitations

<table>
<thead>
<tr>
<th>Technique used</th>
<th>Limitations/drawbacks</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensing detection: single sensing</td>
<td>Lower detection rate</td>
<td>Wang et al.</td>
</tr>
<tr>
<td>and multi sensing</td>
<td></td>
<td>(2008)</td>
</tr>
<tr>
<td>Packet dropping</td>
<td>Watch dog produces overhead and network</td>
<td>Tiwari et al.</td>
</tr>
<tr>
<td></td>
<td>consumption resources</td>
<td>(2009)</td>
</tr>
<tr>
<td>Hierarchical detection of abnormal</td>
<td>High hop count with lower detection rate</td>
<td>Shin et al.</td>
</tr>
<tr>
<td>abnormality</td>
<td></td>
<td>(2010)</td>
</tr>
<tr>
<td>Multiple base-station detection</td>
<td>Cost of computation is high</td>
<td>Misra et al.</td>
</tr>
<tr>
<td></td>
<td>For a smaller number of nodes detection rate lower</td>
<td>(2011)</td>
</tr>
<tr>
<td>Detection and prevention</td>
<td>Cost of communication is high</td>
<td>Wazid et al.</td>
</tr>
<tr>
<td>of blackhole</td>
<td></td>
<td>(2013)</td>
</tr>
<tr>
<td>WSNs distribution: Gaussian and</td>
<td>For a smaller number of nodes detection rate lower</td>
<td>Wang et al.</td>
</tr>
<tr>
<td>Uniform</td>
<td></td>
<td>(2013)</td>
</tr>
<tr>
<td>KNN classification-based IDS</td>
<td>high computation cost</td>
<td>Li et al.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2014)</td>
</tr>
<tr>
<td>Secure Knowledge Algorithm</td>
<td>Low PDR</td>
<td>Siddiqua et al.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2015)</td>
</tr>
<tr>
<td>Knowledge Based Learning</td>
<td>Packet loss, Delay and throughput</td>
<td>Kaur and Singh</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2016)</td>
</tr>
<tr>
<td>AoDMDV routing protocol</td>
<td>Increased routing overheads</td>
<td>Bendale and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shrivastava</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2016)</td>
</tr>
</tbody>
</table>
arrange those sensor nodes in the deployment field which makes the system to admit them as valid nodes. An attacker node for prepares the replica of a sensor node, which can actually capture a sensor node and take whole data which is confidential and further replicate by using the taken data their own nodes and at some planned positions, in the network install them.

Shafiei et al. (2014) [34] for detection of sinkhole (energy holes), they presented an algorithm. Centralized model is being used to detect sinkhole attacker node. To remove sinkhole attacker nodes, a lightweight mitigation technique is used.

Rajasegarar et al. (2014) [35] to detect an abnormal node in WSN, they presented an distributed hyperspherical cluster based algorithm. They had also preformed this algorithm on a real WSN testbed.

This technique had a good accuracy of detection with fewer communication overhead when comparing to the centralized methods where for processing, to a central node every sensor node has to communicate.

Zhang et al. (2014) [36] for prevention from sinkhole attack, they implemented an redundancy technique. In this method, multiple paths are used for sending the messages to suspicious nodes. Reacted messages which the doubtful nodes transmit are used for detecting attacker nodes. Low detection rate was the drawback of this technique.

Sreelaja et al. (2014) [37] for detection of sinkhole attacker nodes, they presented an ant colony optimization attack detection (ACO-AD) algorithm. In network nodes creates warning message if any sinkhole attacker node is detected, in this mechanism. Sinkhole attacker nodes were detected by voting based algorithm. This method recognizes the abnormal connections without creating false positives and make the use of smallest storage memory of the sensor node. Nahas et al. (2009) [38] introduced an the Secure-Path Routing (SPR) protocol for protection of WSN from wormhole and sinkhole attacks. In this technique, for reduction of the traffic flow over the nodes, a parameter in routing they used a predictable path risk, that was exposed to attacker nodes. Then the choice of small menace paths was the problem because chosen routes would consume more energy. Therefore, a method which could make balance between another parameter for path selection, like consumption of energy was proposed. It could also a balance between security and consumption of energy. This method is very effective as traffic flow over the routes was increased.

Krontiris et al. (2008) [39] for protection of WSN from sinkhole attack, they presented an IDS and few rules are designed and embedded. Drawback was low detection rate.

Garofalo et al. (2013) [40] for sinkhole attack detection they presented a decision tree classification-based technique. Drawback of this method was making the balance between energy used in detection process and high detection rate. Therefore, for saving the energy a light weight detection algorithm was performed on motes. They had created a dataset of sinkhole attack and the effectiveness of the proposed system was used for evaluating.

Giruka et al. (2008) [41] reviewed number of security procedures of WSN based on authentication, key management and distribution and secure routing algorithm. Hai et al. (2010) [42] for cluster-based WSN they presented an light weight IDS. The method was designed for minimizing the activated intrusion parts in the network by using an over-hearing method for reduction of the sending alert packets. Most of the routing attacks in WSN were able to detect by this proposed method. Technique needed less energy consumption as compared to other methods was observed during the experiments. But in some cases, up to 10% this method has high false positive rate.

Du et al. (2007) [43] for heterogeneous sensor networks, they presented a secure and efficient routing protocol. They precisely use the powerful high-end sensors. Results of the experiments, proved that this technique resulted in performance better than others algorithms. In this algorithm the delivery ratio decreases as failure nodes increases. With a greater number of L-sensors the delivery ratio increases and delivery ratio decreases with less number of L-sensors.

Dallas et al. (2007) [44] they presented the technique for sinkhole attack detection. For detecting attack, they supervised the hop-count parameter. This technique was computationally efficient for detection of the abnormal route advertisements which were used by attacker nodes.

Roy et al. (2008) [45] proposed a hybrid dynamic IDS which can detect both blackhole and sinkhole in WSN. This method confirms that for every specific attack, network designs do not require redefinition. At the same time, it can deal with both attacks. Disadvantage of this method is high computation cost for low powered sensing devices which causes issues in energy consumption.

Papadimitriou et al. (2009) [46] to protect WSN against sinkhole attack they proposed two cryptographic methods. The main aim of this method is to protect continuously sensor network against sinkhole attack instead of only detection. They introduced cryptographic protocols for sinkhole attack was successful as it secured the network effectively.

Chen et al. (2010) [47] presented a mechanism for sinkhole attack for protection of largescale wireless sensor networks. The mechanism is expressed as a change-point detection technique in which they keep the data of the CPU usage of every sensor node and on the basis of CPU usage, forecast whether the behavioural is normal or abnormal.

Zhan et al. (2012) [48] presented a trust-aware routing framework (TARF) for dynamic WSNs. Without need of time management and geographic data of sensor nodes, it provides trustworthy and energy-efficient routes for nodes in network. TinyOS platform is used for implementation and establishment of TARF module. Efficiency against the various routing attacks is proved in results by simulation.

Qi et al. (2012) [49] for protection of WSN from sinkhole attack, they proposed Multi Hop Link Quality Indicator routing protocols. LQI which specifies that the last packet as the criterion for parent selection is used by MultiHopLQI routing protocol. The objective of this technique is to confirm that base station receives the message in an exact form at given time.

Salehi et al. (2013) [50] for sinkhole attack presented a detection technique. Their proposed process firstly
recognizes a group of distrusted nodes, and then on the basis of network flow data the nodes are confirmed as a sinkhole attacker node. Drawback of this mechanism is high false positive rate and low detection rate.

Sharmila et al. (2011) [51] for detection of sinkhole attack in WSNs they presented a message digest algorithm-based mechanism. The presented method by using a trustable path confirms the honesty of the transferred messages.

Table 2 Sinkhole attack detection techniques and its limitations

<table>
<thead>
<tr>
<th>Technique used</th>
<th>Limitations/drawbacks</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two Tier Secure Routing</td>
<td>very low PDR</td>
<td>Du et al. (2007)</td>
</tr>
<tr>
<td>Sensing abnormality: Single &amp; multi sensing</td>
<td>Lower detection rate</td>
<td>Wang et al. (2008)</td>
</tr>
<tr>
<td>Cooperative abnormality</td>
<td>low DR</td>
<td>Krontiris et al. (2008)</td>
</tr>
<tr>
<td>Intelligent hybrid IDS for the sink, hybrid IDS for CH and misuse IDS approaches</td>
<td>Cost of computation is high with lower detection rate</td>
<td>Wang et al. (2011)</td>
</tr>
<tr>
<td>WSN Distribution: Gaussian and Uniformly</td>
<td>low DR with less number of nodes</td>
<td>Wang et al. (2013)</td>
</tr>
<tr>
<td>Attacker node grouping and flow-based identification of network information</td>
<td>high FPR</td>
<td>Salehi et al. (2013)</td>
</tr>
<tr>
<td>Detection based on Mobile agent</td>
<td>Network overhead is high</td>
<td>Hamedheidari et al. (2013)</td>
</tr>
<tr>
<td>Energy holes estimation by using geostatistical hazard model</td>
<td>energy expenditure maps can create problem in network congestion areas that further affects DR and FPR</td>
<td>Shafiei et al. (2014)</td>
</tr>
<tr>
<td>Redundancy mechanism</td>
<td>Lower detection rate</td>
<td>Zhang et al. (2014) &amp; Patel et al. (2016)</td>
</tr>
<tr>
<td>Hop counting</td>
<td>When malicious node position is near to base station (one or two hop distance), algorithm can not accurately detect sinkhole nodes</td>
<td>Abdullah et al. (2015)</td>
</tr>
<tr>
<td>Mobile Agent Based Detection, Hop Count Based Detection, Sequence Number Based Detection, Cryptography Based Detection and Energy Consumption Based</td>
<td>Security issues, Low Detection Rate, High Detection Overheads and Communication Cost</td>
<td>Mathew et al. (2017)</td>
</tr>
<tr>
<td>Ad-hoc on demand distance vector routing protocol</td>
<td>Low throughput, increase in packet drop, increase in RREP messages with increase in malicious nodes</td>
<td>Sehrawat et al. (2018)</td>
</tr>
</tbody>
</table>

Abdullah et al. (2015) [52] proposed sinkhole detection using hop counting technique. The proposed technique can detect successfully when the malicious nodes are situated at distant from base station where it reports with less accurately when malicious node are located near the base station.

Patel et al. (2016) [53] detected sinkhole attack based on the analysis of routing behaviour in a wireless sensor network. The proposed algorithm consists of three phases namely, topology generation & data transmission, sinkhole implementation and detection phase. By analysing the forward and reverse routes this scheme detects the sinkholes. Mathew et al. (2017) [54] discovered and examined the existing solutions which are employed for detection of sinkhole attack in wireless sensor network. They focused on techniques viz., cryptography, sequence number, hop count and mobile agent. They found that mainly techniques have security issues, high communication cost, low detection rate and high detection overheads.

Sehrawat et al. (2018) [55] analyzed the impact of Sinkhole attack on AODV protocol with varying number of attacker nodes. Simulated the proposed methodology in Qualnet 7.3.1 software using 50 nodes in an area of 1500 m x 1500 m with no mobility. Result showed low throughput, increase in packet drop, increase in RREP messages with increase in malicious nodes.

IV. CONCLUSION

This survey paper reviewed the intrusion detection techniques used in WSNs. More specifically, the existing methods for blackhole and sinkhole attacks detection are reviewed. Based on literature review the parameters used for evaluating performance of IDS are identified as detection rate, false alarm rate, true positive, true negative, false positive, false negative and noise. Majority of the methods have failed in security issues such as low detection rate, high detection overheads and high communication cost. Thus, there is scope for future work which may focus on reducing the network overheads and increase the security concerns along with higher detection rates. Designing an efficient hybrid mechanism to detect black hole and sink hole attack simultaneously could be another future direction in WSNs.

REFERENCES


