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 areas 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 WSN 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.

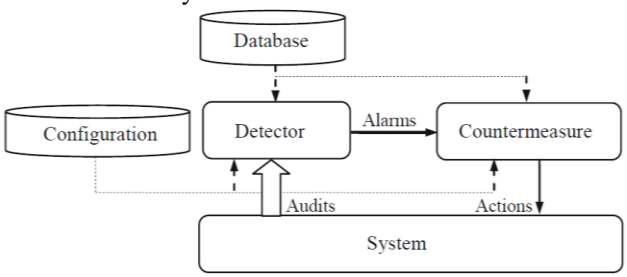

Figure .1 Basic IDS block diagram [1]

Revised Version Manuscript Received on 16 September, 2019.

S Ashwini V. Jatti , Research Scholar, Department of ECE, Sathyabama Institute of Science and Technology, Chennai - 600 119, India.
koti.ashwini@gmail.com

Dr. V. J. K. Kishor Sonti, Associate Professor, Department of ECE, Sathyabama Institute of Science and Technology, Chennai - 600 119, India.
kishoresonti.ece@sathyabama.ac.in

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 is 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.
6. Response Tactic: IDS in this part, differentiates between active and passive response strategies.

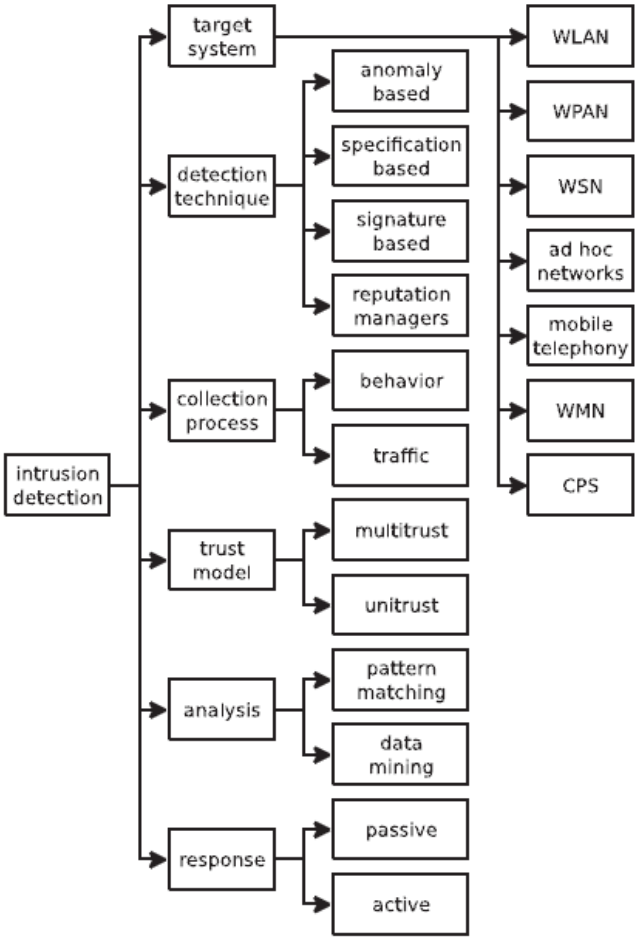

Figure. 2 Intrusion detection techniques for wireless networks [2]

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 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 uesd.

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.

Table 1 Blackhole attack detection techniques and its limitations

Technique used	Limitations/drawbacks	Reference
Sensing detection: single sensing and multi sensing	Lower detection rate	Wang et al. (2008)
Packet dropping	Watch dog produces overhead and network consumption resources.	Tiwari et al. (2009)
Hierarchical detection of abnormality	High hop count with lower detection rate	Shin et al. (2010)
Multiple base-station detection	Cost of computation is and high FPR & PDR for one base station	Misra et al. (2011)
Detection and prevention of blackhole	Cost of communication is high	Wazid et al. (2013)
WSNs distribution: Gaussian and Uniform	For a smaller number of nodes detection rate is lower	Wang et al. (2013)
KNN classification-based IDS	high computation cost	Li et al. (2014)
Secure Knowledge Algorithm	Low PDR	Siddiqua et al. (2015)
Knowledge Based Learning	Packet loss, Delay and throughput	Kaur and Singh (2016)
AoDMDV routing protocol	Increased routing overheads	Bendale and Shrivastava (2016)

Siddiqua et al. (2015) [56] for black hole detection in AODV protocol, they developed a secure knowledge algorithm. This method observe packet drop reason before declaring the node as black hole node.

Kaur and Singh (2016) [57] proposed knowledge-based learning technique which detect and mitigate the black hole node which is responsible for activating the attack from the network. Results of simulation showed that the proposed technique drops less packets, delay output is 56000 and 98% throughput in comparison to existing techniques.

Bendale and Shrivastava (2016) [58] proposed AODV protocol for detection of blackhole in the networks. 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 integrated 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 Rafeh (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 defining 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

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

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

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

[1] Amrita Ghosal and Subir Halder, "Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches", Wireless Networks and Security (2013): 329-367.

[2] Robert Mitchell and Ing-Ray Chen, "A survey of intrusion detection in wireless network applications", Computer Communications 42 (2014): 1-23.

[3] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos , "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks", ALGOSENSORS (2007):150-16.

[4] Ashfaq Hussain Farooqi and Farrukh Aslam Khan, "Intrusion Detection Systems for Wireless Sensor Networks: A Survey", FGCN/ACN 56 (2009): 234-241.

[5] Han Zhijie, Wang Ruchuang, "Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model", Physics Procedia 25 (2012): 2072-2080.
[6] Murad A. Rassam, Anazida Zainal, Mohd Aizaini Maarof, "An Efficient Distributed Anomaly Detection Model for Wireless Sensor Networks", AASRI Procedia 5 (2013): 9-14.
[7] Yassine Maleh, Abdellah Ezzati, Youssef Qasmaoui, Mohamed Mbid, "A Global Hybrid Intrusion Detection System for Wireless Sensor Networks", Procedia Computer Science 52 (2015): 1047-1052.
[8] Syed Muhammad Sajjad, Safdar Hussain Bouk, Muhammad Yousaf, "Neighbor Node Trust Based Intrusion Detection System for WSN", Procedia Computer Science 63 (2015): 183-188.
[9] Ismail Butun, In-Ho Ra and Ravi Sankar, "An Intrusion Detection System Based on Multi-Level Clustering for Hierarchical Wireless Sensor Networks," Sensors 15 (2015): 28960-28978.
[10] M. Guechari, L. Mokdad, and S. Tan. Dynamic solution for detecting Denial of Service attacks. In IEEE International Conference on Communications, pages 173-177, Ottawa, Canada, 2012.
[11] Y. Wang, W. Fu, and D. P. Agrawal. Gaussian versus uniform distribution for intrusion detection in wireless sensor networks. IEEE Transactions on Parallel and Distributed Systems, 24(2):342–355, 2013.
[12] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal. Intrusion detection in homogeneous and heterogeneous wireless sensor networks. IEEE Transactions on Mobile Computing, 7(6):698–711, 2008.
[13] Y. Yu, K. Li, W. Zhou, and P. Li. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. Journal of Network and Computer Applications, 35(3):867–880, 2012.
[14] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, and H. Rhy. An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks. IEEE Transactions on Industrial Informatics, 6(4):744–757, 2010.
[15] S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami. Centered Hyper-spherical and Hyperellipsoidal One-Class Support Vector Machines for Anomaly Detection in Sensor Networks. IEEE Transactions on Information Forensics and Security, 5(3):518–533, 2010.
[16] M. Tiwari, K. V. Arya, R. Choudhari, and S. K. Choudhary. Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information. In 4th IEEE International Conference on Computer Sciences and Convergence Information Technology, pages 824–828, Seoul, South Korea, 2009.
[17] J. Zhang, Y. Xiang, Y. Wang, W. Zhou, Y. Xiang, and Y. Guan. Network traffic classification using correlation information. IEEE Transactions on Parallel and Distributed Systems, 24(1):104–117, 2013.
[18] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy Efficient Communication Protocol for Wireless Microsensor Networks. In 33rd Hawaii International Conference on System Sciences, pages 1–10, Hawaii, USA, 2000.
[19] M. Xie, J. Hu, S. Han, and H.-H. Chen. Scalable Hyper grid k-NN-Based Online Anomaly Detection in Wireless Sensor Networks. IEEE Transactions on Parallel and Distributed Systems, 24(8):1661–1670, 2013.
[20] A. Abduvaliyev, A. S. K. Pathan, J. Zhou, R. Roman, and W. C. Wong. On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks. IEEE Communications Surveys & Tutorials, 15(3):1223–1237, 2013.
[21] M.-Y. Su. Using clustering to improve the KNN-based classifiers for online anomaly network traffic identification. Journal of Network and Computer Applications, 34(2):722–730, 2011.
[22] F. Wang and J. Liu. Networked Wireless Sensor Data Collection: Issues, Challenges, and Approaches. IEEE Communications Surveys & Tutorials, 13(4):673–687, 2011.
[23] M. Xie, S. Han, B. Tian, and S. Parvin. Anomaly detection in wireless sensor networks: A survey. Journal of Network and Computer Applications, 34(4):1302-1325, 2011.
[24] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li. A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network. Electrical and Computer Engineering, 2014:1–8, 2014. Article ID 240217.
[25] M. Wazid, A. Katal, R. S. Sachan, R. H. Goudar, and D. P. Singh. Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network. In IEEE International Conference on Communication and Signal Processing (ICCSP), pages 576–581, Melmaruvathur, India, 2013.
[26] A. Prathapani, L. Santhanam, and D. P. Agrawal. Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks. In 6th IEEE International Conference on Mobile Adhoc and Sensor System, pages 753–758, Macau, China, 2009.
[27] S. Misra, K. Bhattarai, and G. Xue. BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. In IEEE International Conference on Communications (ICC), pages 1–5, Kyoto, Japan, 2011.
[28] H. Gao, R. Wu, M. Cao, and C. Zhang. Detection and Defense Technology of Blackhole Attacks in Wireless Sensor Network. In International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP), Lecture Notes in Computer Science (LNCS), pages 601–610, Dalian, China, 2014. Springer.
[29] E. C. H. Ngai, J. Liu, and M. R. Lyu. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer Communications, 30(11-12):2353–2364, 2007.
[30] S.-S. Wang, K.-Q. Yan, S.-C. Wang, and C.-W. Liu. An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks. Expert Systems with Applications, 38(12):15234–15243, 2011.
[31] S. Hamedheidari and R. Rafeh. A novel agent-based approach to detect sinkhole attacks in wireless sensor networks. Computers & Security, 37:1–14, 2013.
[32] F. L. Fessant, A. Papadimitriou, A. C. Viana, C. Sengul, and E. Palomar. A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis. Computer Communications, 35(2):234–248, 2012.
[33] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao. Detecting node replication attacks in wireless sensor networks: A survey. Journal of Network and Computer Applications, 35(3):1022–1034, 2012.
[34] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi. Detection and mitigation of sinkhole attacks in wireless sensor networks. Journal of Computer and System Sciences, 80(3):644–653, 2014.
[35] S. Rajasegarar, C. Leckie, and M. Palaniswami. Hyperspherical cluster based distributed anomaly detection in wireless sensor networks. Journal of Parallel and Distributed Computing, 74(1):1833–1847, 2014.
[36] F.-J. Zhang, L.-D. Zhai, J.-C. Yang, and X. Cui. Sinkhole Attack Detection based on Redundancy Mechanism in Wireless Sensor Networks. Procedia Computer Science, 31:711–720, 2014.
[37] N. K. Sreelaja and G. A. V. Pai. Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks. Applied Soft Computing, 19:68–79, 2014.
[38] H. A. Nahas, J. S. Deogun, and E. D. Manley. Proactive mitigation of impact of wormholes and sinkholes on routing security in energy-efficient wireless sensor networks. Wireless Networks, 15(4):431–441, 2009.
[39] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos. Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks. In 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (ALGOSENSORS), volume 4837 of Lecture Notes in Computer Science, pages 150–161, Wroclaw, Poland, 2008. Springer.
[40] A. Garofalo, C. D. Sarno, and V. Formicola. Enhancing Intrusion Detection in Wireless Sensor Networks through Decision Trees. In 14th European Workshop on Dependable Computing (EWDC), Lecture Notes in Computer Science (LNCS), volume 7869, pages 1–15, Coimbra, Portugal, 2013. Springer Berlin Heidelberg.
[41] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi. Security in wireless sensor networks. Wireless Communications and Mobile Computing, 8(1):1–24, 2008.
[42] T. H. Hai, E. N. Huh, and M. Jo. A lightweight intrusion detection framework for wireless sensor networks. Wireless Communications and Mobile Computing, 10(4):559–572, 2010.
[43] X. Du, M. Guizani, Y. Xiao, and H. H. Chen. Two Tier Secure Routing Protocol for Heterogeneous Sensor Networks. IEEE Transactions on Wireless Communications, 6(9):3395–3401, 2007.
[44] D. Dallas, C. Leckie, and K. Ramamohanarao. Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks. In 15th IEEE International Conference on Networks (ICON), pages 176–181, Adelaide, Australia, 2007.
[45] S. D. Roy, S. A. Singh, S. Choudhury, and N. C. Debnath. Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management. In Symposium on Computers and Communications (ISCC), pages 537–542, Morocco, 2008.
[46] A. Papadimitriou, F. L. Fessant, A. C. Viana, and C. Sengul. Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks. In 5th Workshop on Secure Network Protocols (NPSec), pages 43–48, Princeton, USA, 2009.
[47] C. Chen, M. Song, and G. Hsieh. Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. In IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), pages 711–716, Beijing, China, 2010.
[48] G. Zhan, W. Shi, and J. Deng. Design and Implementation of TARF: A Trust- Aware Routing Framework for WSNs. IEEE Transactions on Dependable and Secure Computing, 9(2):184–197, 2012.
[49] J. Qi, T. Hong, K. Xiaohui, and L. Qiang. Detection and Defence of Sinkhole attack in Wireless Sensor Network. In 14th IEEE International Conference on Communication Technology (ICCT), pages 809–813, Chengdu, China, 2012.
[50] S. A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala. Detection of sinkhole attack in wireless sensor networks. In International Conference on

Space Science and Communication (IconSpace), pages 361–365, Melaka, Malaysia, 2013.
[51] S. Sharmila and G. Umamaheswari. Detection of Sinkhole Attack inWireless Sensor Networks Using Message Digest Algorithms. In International Conference on Process Automation, Control and Computing (PACC), pages 1–6, Coimbatore, India, 2011.
[52] M. Abdullah, M. M. Rahman and M. C. Roy. Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count, I. J. Computer Network and Information Security, 3, pages 50-56, 2015.
[53] M. Patel, M. B. Ahmed. Sinkhole attack detection based on redundancy mechanism in wireless sensor network, International Journal of Scientific Development and Research, pages 302-305, 2016.
[54] A. Mathew and J. S. Terence. A Survey on Various Detection Techniques of Sinkhole Attacks in WSN, IEEE International Conference on Communication and Signal Processing, April 6-8, India, pages 1115-1119, 2017.
[55] H. Sehrawat, Y. Singh, V. Siwach. Analysis of AODV Routing Protocol under Sinkhole Attack in Wireless Sensor Network, International Journal of Engineering & Technology, 7 (2.4), pages 153-156, 2018.
[56] A. Siddiqua, K. Sridevi, A. A. K. Mohammed, Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm, SPACES-2015, Dept of ECE, K L University, pages 421-425, 2015.
[57] H. Kaur and A. Singh. Identification and Mitigation of Black Hole Attack in Wireless Sensor Networks, IEEE International Conference on Micro-Electronics and Telecommunication Engineering, pages 616-619, 2016.
[58] G. Bendale and S. Shrivastava. An Improved Blackhole Attack Detection and Prevention Method for Wireless Ad-hoc Network, IEEE International Conference, pages 1-7, 2016.
[59] P. Sarathe and N. Shrivastava. A Review on Different Methods to Prevent Black Hole Attack in MANET, International Journal of Computer Sciences and Engineering, Vol. 6, Issue-6, pages-1149-1156, 2018.