Indian Journal of Data Communication and Networking (IJDCN)
ISSN: 2582-760X (Online), Volume-1 Issue-4 August 2021

Challenges in Sinkhole Attack Detection in Wireless Sensor Network

Akhilesh A. Waoo, Virendra Tiwari

***Abstract:** Wireless sensor networks (WSN's) comprise limited energy small sensor nodes having the ability to monitor the physical conditions and communicate information among the various nodes without requiring any physical medium. Over the last few years, with the rapid advancements in information technology, there has been an increasing interest of various organizations in making the use of wireless sensor networks (WSN's). The sensor nodes in WSN having limited energy detects an event, collect data and forward this collected data to the base node, called sink node, for further processing and assessment. Few attributes of WSN's like the energy consumption and lifetime can be impacted by the design and placement of the Sink node. Despite various useful characteristics WSN's is being considered vulnerable and unprotected. There is a large class of various security attacks that may affect the performance of the system among which sinkhole an adversary attack puts dreadful threats to the security of such networks. Out of various attacks, a sinkhole attack is one of the detrimental types of attacks that brings a compromised node or fabricated node in the network which keeps trying to lures network traffic by advertising its wrong and fake routing update. Sinkhole attacks may have some other serious harmful impacts to exploit the network by launching few other attacks. Some of these attacks are forwarding attacks, selective acknowledge spoofing attacks, and they may drop or modify routing information too. It can also be used to send fake or false information to the base station. This study is analyzing the challenges with sinkhole attacks and exploring the existing available solutions by surveying comparatively which used to detect and mitigate sinkhole attacks in the wireless sensor network.*

***Keywords:** Wireless sensor network (WSN), compromised node, sinkhole attack, detection, and mitigation of sinkhole attack.*

I. INTRODUCTION

A wireless sensor network refers to a group of the number of small nodes capable to perform sensing and send data to the base station [1]. Wireless sensor network technology is prominently being used in different and variety of applications example is in military activities, where it works to track the movement of suspected and unauthenticated persons. It is also very useful in fire detection mechanisms and healthcare services like wearable items for monitoring heart rate [2] and so. Unfortunately, it is found that most of the wireless networks are actually deployed and working in not-friendly and not secured areas and normally left open unattended in an unsecured environment. Also, most of their frequent use routing protocols don't consider or attend the security aspect due to resource constraints and limitations which contain low memory, low computational power, storage capacity low power supply, and low communication range [3]. All these constraints create possibilities for many vicious attackers to create trouble by attacking established networks easily. One of the examples of such attacks is the sinkhole attack [4]. A simple impersonation-like attack, which leads to a sinkhole attack, can compromise the entire network. In a network layer state, an adversary makes an effort to lure over traffic to prevent the network base station from implementing a Sinkhole attack so from receiving complete sensing data from nodes [5]. By doing so the adversary normally fabricates and compromises the node and that compromised node will be used to initiate the launch of an attack. This introduced fabricated node will keep trying to send fake information to all connected neighboring nodes about the network link quality which is used in routing metrics to select the best route during data transmission [6]. So, all the packets from neighbors of that node pass through it before reaching the base station. A sinkhole attack tries to prevent the network base station from receiving complete and precise sensing data from nodes. The purpose of this survey is to analytically study all existing solutions used to detect sinkhole attacks in the current scenario [7]. Various given solutions which are being applied to detect and identified dangerous sinkhole attack in different ways are suggested by many researchers.

II. WIRELESS SENSOR NETWORKS (WSN)

Wireless Sensor Networks (WSN) refers to an infrastructure-less network that refers to a group of interconnected small embedded, inexpensive and elegant computing devices called sensors, which nowadays are being used in all advanced sectors; for developing and deploying smart sensors [7]. These smart sensors get geographically distributed in the network in such a way and embedded by the process to ecological devices with various purposes like measuring and monitor environment effectively like temperature, sound, humidity, pollution levels, wind, and so on [8]. The sensor nodes of the network using radio signals can interact and exchange information among themselves [9].

Manuscript received on 11 June 2021 | Revised Manuscript received on 29 July 2021 | Manuscript Accepted on 15 August 2021 | Manuscript published on 30 August 2021.

* Correspondence Author

Dr. Akhilesh A. Waoo*, Associate Professor and Head, Department of Computer Science & Engineering, AKS University, SATNA, M.P., India.

Mr. Virendra Tiwari*, Research Scholar, Department of Computer Science & Engineering, AKS University, SATNA, M.P., India.

A wireless sensor node is consisting of massive, tiny sensing devices and computing devices, radio transceivers, which are shown in Figure, and power components such as a location finding system, a power generator with minimum power, less processing, and interaction abilities. The sensor network is highly required for the proper administration and useful application of WSN needs an established protocol and scheduled algorithm due to the undesirable task of maximum sensors in sundry and diverse fields as it is prone to vicious sinkhole attacks since it is composed of specialized interacting patterns [11][12].

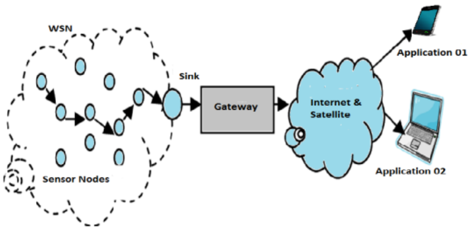

Fig. 1. Wireless sensor network architecture

III. SINKHOLE ATTACK

A sinkhole attack is one of the forms of insider detrimental attack where an intruder compromises a network's node by advertising its fake routing update within the established network and does an attack launching. After that, the compromised node tries to attract all the possible traffic from neighbor-connected nodes which are based on the available routing metric(path for transferring data/traffic) that is used in the routing protocol [13]. When it is capable to manage to achieve that, will be launching an attack. Due to the reason of many to one communication pattern of wireless sensor network of where every connected node transmit data to the base station, making this WSN possibly vulnerable to sinkhole attack [14], and it can reduce and spoil the overall performance of the network by causing improper and potentially dangerous responses based on false measurements [15].

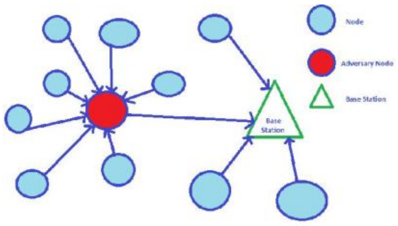

Fig. 2. Two illustrations of sinkhole attack in WSN

The sinkhole attack in the WSN's can be launched on different routing protocols by fabricating the routing metric. There are following discussed subsections are the techniques used in MintRoute protocol and AODV protocol in launching sinkhole attacks.

A. Sinkhole Attack in MintRoute Protocol

MintRoute routing protocol is one of the protocols which is usually used in wireless sensor network technology [16]. It is designed and configured purposely for the wireless sensor network, this protocol is light, usable, and very effective for sensor nodes that have in general minimum storage capacity, low consumption of computation power, and short power supply [17]. MintRoute protocol in the process of routing uses link quality as a metric in a way to select the optimal and best route to send the packet to the network base station [18].

B. Sinkhole Attack in TinyAODV Protocol

This is one of the other types of sinkhole attacks due to the dynamic nature of the WSN which comes under TinyAODV (Ad-hoc On-Demand Vector) routing protocol. Routing protocols play a very crucial role in setting up structured routes among pairs of nodes in the network. Functionally, the TinyAODV is a routing protocol similar to AODV in MANET but the difference is that one is slightly lighter compared to AODV and got modified and updated purposely for the technology of the established network [19]. The number of hops towards the network base station is the routing metric that will be used properly in this protocol. Generally, when one of the nodes sends a request then the route from source to destination is created, the source node of the network sends an RREQ (Route Request) packet to the neighbor's node when wants to send a packet. The next neighbor would be close to the destination replying by sending back RREP (Route Reply) packet if the packet is not forwarded to other nodes, close to the destination. Eventually, the source receives RREP packets from all the neighbors then selects one of the nodes having fewer hops to the destination. The fabricated node or compromised node launches an attack by sending back the RREP packet. In the RREP packet, it shows a small number of hops which indicates proximity to the base station. After this, the source node decides to forward the packet to the sinkhole node. Then compromised node performs the same process to its entire neighbors and tries to attract as much traffic as possible [20].

IV. CHALLENGES IN THE DETECTION OF SINKHOLE ATTACK IN WSNS

Following are some of the main challenges in determining sinkhole attacks in wireless sensor networks after reviewing some of the renowned works of literature:

A. Communication Pattern in WSN

In a WSN, the entire sensor nodes message is destined to the base station of the network. This procedure creates an opportunity and possibility for the sinkhole to bring an attack in the network. Sinkhole attacks usually become part of the network when fabricated nodes send fake and false routing-related information to other neighboring nodes in the network with aiming of attracting as much traffic as manageable [21]. Based on this mechanism of communication the intruder will only be trying to make compromised that node that is closest to the base station rather than targeting the entire network's node. This is found one of the dangerous challenges since the communication pattern itself creating some possibilities for attack in the network.

B. Unpredictable Nature of Sinkhole Attack

In wireless networks, the execution of packet transmission is based on prepared routing metrics apply by different protocols of routing [22]. Routing metrics used by the compromised node that routing protocol uses in the network to lie to its neighbors may launch sinkhole attacks. It makes it possible that all the data and information from its neighbors to the base station will be passing through the occurred compromised node. Processes and techniques used by a compromised node in a network may differ means that used in TinyAODV routing protocol is different from the one used by another routing protocol like MintRoute protocol. In the process of MintRoute, link quality gets to use as a route metric while in the TinyAODV they use the mechanism of counting many hops to the base station of the network as a routing metric [23]. Therefore, the techniques of sinkhole attacks get changed. It depends on the routing metric which is created in the preferred routing protocol.

C. Insider Attack

There are two different categories of attacks in a wireless sensor network; these are insider attacks and outsider attacks. The outside attack of the network is considered when an intruder is not part of the network means does not belong to a WSN whereas in the case of an inside attack of network the intruder tries to compromise and fabricate one of the legitimate nodes behave in unintended or unauthorized ways of the network through tempering of the node or maybe through some other vulnerabilities of the system software then fabricated node injects wrong information in the established network after getting valuable secret information [24]. The connected network can be disrupted by modifying the routing packet in the process of an inside attack. The fabricated node possesses sufficient access privilege in the existing network and has valuable information and important procedures about the network topology. This creates it more challenging in exposing and detecting. Based on this concept it is found that even cryptography is unable to secure against insider attacks in the network although it can provide some other attributes like authentication integrity, and confidentiality [25]. Therefore, can be said that the internal attack brings a more serious and dangerous impact on the victim system compared to outsider attacks [26].

D. Resource restriction

Resource restriction is one of the major challenges in WSNs. The low communication range, limited processing speed, limited power supply, low computational power, and low memory capacity are the main inherently constrained of any wireless sensor network that makes it difficult to implement a strong security mechanism [27]. Suppose if the Robust cryptographic method is being used in some networks effectively and efficiently cannot be implemented similarly in another working network due to some practical challenges like low computational power and low storage capacity. Therefore, a less strong key might be considered which is suitable and compatible with the network available resources.

E. Physical Attack

A wireless sensor network is usually installed and set up in a hostile and unfriendly environment and left unattended or neglected in an unsecured environment [28]. It affects the performance of the entire network and it is the primary obstacle that must be solved and fixed in network application [29]. As it makes possibilities for an intruder to attack a network's node of the network physically and get illegitimate access to all valuable and very important information [30].

V. EXISTING APPROACHES

Many analyzers and researchers are engaged in developing the technologies needed to have proper security mechanisms which suit the occurred resource various constrained due to expanding demand of network's applications in very sensitive areas [31]. This survey and study reviews and analyzes related work on Sinkhole attack exposition or detection, various prevention strategies, procedures, and multiple attack techniques and it is also trying to highlight the list of open challenges in the network dealing with such attacks. There are some following identified mechanisms and approaches that were used by different experts and researchers to detect Sinkhole and exposing sinkhole attacks by identifying in a wireless sensor network. Major approaches and techniques are categorized into the rules-based, anomaly-based, statistical method, key management, and hybrid-based [32].

A. Rule-based

Rules can be designed based on some crucial points like the behavior or technique used to launch a sinkhole either one can be chosen. Then these designed rules are embedding in intrusion spotting and detection system which runs on network's sensor nodes. Now, these processed rules are applied to the transmitted packet down the working network nodes. If any node of the network violates or breaches the created rules will be considered as an adversary and going to be isolated and separated from the network [33]. In the mechanism of the rule-based method of detecting sinkhole attacks, two rules get embedded or implanted in the procedure of intrusion [34]. When any of the embedded rules are violated by any of the network's nodes, the intrusion detection mechanism instantly triggered an alarm system but it does not give the ID of the fabricated node. There are two rules, the first rule is "ID of the sender node for each overhead route packet must belong to the ID in its neighbors" and the second rule is "Sender ID in the network for each overhead route update packet must differ your node ID means must not be same[35].

B. Anomaly-based Detection

In the procedure of anomaly-based detection, initially, the normal user behavior is properly defined and the basis on that intrusion detection gets searched for anything which is suspected or anomalous in the working network [36].

Published By:
Lattice Science Publication (LSP)

This mechanism considers an intrusion an anomalous activity since it seems unrepresentative and abnormal compare to the normal behavior of the node. In the anomaly-based detection approach, some other approaches are also included like the rule-based and statistical [37].

C. Statistical Method

In the procedure of statistical, the nodes associated data and information of various activities in the network is observed on different parameters and recorded by the experts or researchers. Such as, monitoring the normal passing on packets among the network nodes or could be monitoring of resources consumption of the nodes such as the use of CPU [38]. So, adversary or fabricated node gets detected by referencing the threshold value and comparing with actual behavior if any nodes beyond a limit or exceed the established value that will be considered as an intruder [39].

D. Hybrid based Intrusion Detection

The combination of both the above-discussed methods anomaly and signature-based are used in this approach. The false and wrong positive rate which is produced by anomaly-based gets reduced in this approach due to the use of both methods of detection [40]. Moreover the advantage of this approach it enables to catch of any suspicious nodes if their signature is not included in the detection database [41].

E. Key Management

In the procedure of key management, the authenticity and integrity of traveling packets inside the working network are secured and shielded by using an encryption key and decryption key. Any transmitted packet within the working network is attached with another message by the established process in a way that if the message is required to be accessed it a must-have required key and any sort of small tempering of the transmitted message can be easily recognized or detected [42]. These keys are also helpful to evaluate the nodes whether the message is coming from the base station of the network and also evaluates the message's authenticity [43].

F. Probabilistic approach

It is an adaptive sinkhole-aware algorithm to compute the probability of each node being affected or troubled by sinkhole attacks which are based on the subjective logic model and probabilistic extension model of timed automata. This method is being used effectively for the calculation and deciding on a reliable or trustworthy path. The subjective logic procedure was used efficiently as an adaptive engine, to expose the sinkhole attacks in the network. The probabilistic algorithm working has the feature to stay robust to baffled or confuse detection mechanisms [44].

G. Fuzzy Rule-based

This mechanism is used for detecting sinkhole attacks in the network by a mint route which is energy efficient. This procedure firstly selects the node which will be forwarded next to enable an efficient and right path establishment for the packet routing that will be based on a fuzzy logic model [46]. This mechanism is quite efficient to expose sinkhole attacks generally for mini-scale WSNs and can be also be configured using the scanner the detection competency of big-scale multi-hop WSN [47][48].

H. Agent-based

This procedure is used to put a stop to sinkhole attacks in a created wireless network of connected mobile nodes where validation of agent done on the valid node, on adversary node or fake agent done on the valid node, 3 steps intercession among neighbor nodes so they do not mind to the traffics generated by malicious or untrustworthy nodes. Work gets assessed and evaluated based on some crucial parameters such as the agent’s overhead, energy, throughput, and packet loss. In terms of some important factors like energy utilization, memory overhead, and cryptography, this mechanism is found very effective [49].

The summary of existing work on sinkhole detection using different approaches listed out in the below Table.

Table 1: Existing works on Sinkhole detection [32].

Year	Proposed Approach	Proposed by	Proposed solution	Results/Outcomes
2017	Probabilistic procedure	Jahandoust & Ghassemi [44]	For computing & decision of a safe and secure path suggested an adaptive sinkhole aware algorithm.	• Able to detect any sinkhole attack in the network, the subjective logic mechanism was applied effectively as an adaptive engine. • The suggested technique has the feature to stay strong to deception detection mechanisms.
2016	Statistical method	Gupta & H. Kaur et al. [45]	Given the use of advance & enhanced secure AODV routing protocol.	• Efficient in detecting malicious nodes. • Better throughput & packet delivery ratio.

2013	Agent-based procedure	S. Hamedheidari & R. Rafeh [49]	Suggested an approach can be used to prevent sinkhole attacks in particularly established mobile nodes networks.	• 3 steps intercession among neighbor nodes, verifying of agent on the valid node of the network, on the enemy node, & untrustworthy agent on the valid node of the network. • Work has been evaluated based on the cretin parameters such as energy, throughput, loss of packet, & agent's overhead of the network. • In terms of utilization of memory energy, overhead, & cryptography, this method is found very efficient.
2012	Fuzzy Rule-based method	Rassam & Rupinder Singh et al. [46][47]	The technique for exposing sinkhole attacks particularly in the mint route-oriented network.	• In the environment of TinyOS, a testbed was developed. • The suggested technique is quite efficient in detecting sinkhole attacks for limited-scale of WSNs • The technique can be also be configured using the scanner the detection competency of big-scale multi-hop WSN.
2011	Anomaly-based procedure	Sharmila & Umamaheswari [36][37]	The suggested algorithm of a transmitted message digests for detecting the sink node.	• Superb working is found when malicious nodes are fewer than 50%. • This algorithm is good in terms of data authenticity and integrity. • The normal & regular value of false -ve error was 10%.
2010	A non-cryptographic	D. Sheela & C. N. Kumar et al. [43]	Presented an effective technique for the protection against attacks using mobile agents.	• Probability of network's sinkhole & the number of network nodes having an inverse relationship. • This technique's issue is large network overheads.
	Hybrid	M. M. Ozcelik et al [40] & Coppolino et al. [41]	Intrusion detection mechanism capable of protecting crucial information from direct attacks in the WSN.	• The rate of detection found more than 94% when malicious nodes altered the sensor packet. • The rate of detection was around 94% & 3% +ve false rate if malicious node altered received and control packet.
2009	Key management method	A. Papadimitriou et al. [42][43]	Given the use of two RESIST protocols that are to be used efficiently to uplift resilience against sinkhole attacks in WSN.	• Resist-0 & RESIST-1 are two useful RESIST protocols. • Resist-0 is high resilience as compared to RESIST-1 in the situation of sinkhole attacks. • RESIST-0 will only be impacted from the collusion node.
2008	Rule-Based procedure	I. Krontiris et al. [17]	Rules for the indication by alarming if any attack to the network legitimate node is found.	• A LQI based Multi-hop vulnerability might be exploited by the network's sinkhole node. • Approached rules were not found very effective to avail any node ID of the sinkhole. • These effective rules are setting the protocol up more resilient.

VI. CONCLUSION AND FUTURE WORK

Based on existing and currently being used work this research has found that most researchers have been striving to look for ICT solutions for WSN related problems particularly identifying, detecting, and providing the resistance-oriented solution to sinkhole attacks in a working wireless network. Different researchers and analyzers had presented and shown several ways of intrusion detection proposals based on different methods with various versatile approaches to expose and identify the vicious sinkhole nodes. Most of the researches has also shown perplexity with security issues and few challenges in the network corresponding with the availability of resourceful devices and mobility and portability of wireless sensor nodes. Few experts have provided solutions only for static scenarios and few on the mobile network. To validating their security system, some of the researchers have tried and approached using real wireless sensor networks and they have found in results that high network overhead, low detection rate, and in some circumstances high communication cost. This study surveyed related work on exposing Sinkhole attacks of the network, different prevention procedures, and various techniques which are currently being used and also tried to highlight some of the open and unattended challenges in dealing with such attacks. This study has found that among discussed various techniques and mechanisms, fuzzy logic-based systems found effective so can be considered good in performance for intruder detection systems (IDS). The future work must focus on some other very important attributes like reducing high network overhead, rising the detection rate, and proposed the designed system must be validated in the real sensor network.

REFERENCES

1. M. C. Mancilla, E. L. Mellado, and Mario Siller, "*Wireless Sensor Networks Formation: Approaches and Techniques*", Journal of Sensors, vol. 2016. [CrossRef]
2. F. Hidoussi, H. Toral-Cruz, D. E. Boubiche, K. Lakhtaria, A. Mihovska, and M. Voznak, "*Centralized IDS based on misuse detection for cluster-based wireless sensors networks. Wireless Personal Communications*", 85(1), 207–224, 2015. [CrossRef]
3. B. Bhushan, & G. Sahoo, "*Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. Wireless Personal Communications*", 98(2), 2037–2077, 2018. [CrossRef]
4. Y. C. Hu, A. Perrig, and D. B. Johnson, "*Packet leashes: a defense against wormhole attacks in wireless networks*". In INFOCOM 2003, the twenty-second annual joint conference of the IEEE computer and communications, IEEE Societies (Vol. 3, pp. 1976–1986). IEEE, 2003.
5. S. Roy, S. Singh, S. Choudhury, and N. Debnath, "*Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management*", IEEE Symposium on Computers and Communications (ISCC), Marrakech Morocco, 2008 pp, 2013. [CrossRef]
6. I. Panagiotis, R. Grammatikis, G. Panagiotis, and D. Moscholios, "*Securing the Internet of Things: Challenges, threats and solutions*", Internet of Things, Volume 5, Pages 41-70, ISSN 2542-6605, 2019. [CrossRef]
7. M. Ndiaye, G. P. Hancke and A.M Abu-Mahfouz, "*Software Defined Networking for Improved Wireless Sensor Network Management: A Survey*", Sensors 2017, 17, 1031, 2017. [CrossRef]
8. J. Poza-Lujan, J. Posadas-Yagüe, J. Simó-Ten, and F. Blanes, "*Distributed Architecture to Integrate Sensor Information: Object Recognition for Smart Cities*", Sensors (Basel).;20(1):112, 2019. [CrossRef]
9. C.S. Reddy and N.P. Chandra Rao, "*An Empirical Study on Support Vector Machines for Intrusion Detection", International Journal of Emerging Trends in Engineering Research"*, Vol. 7, No. 10, pp. 383-387, October 2019. [CrossRef]
10. T. Nguyen, J. Pan, and T. Dao, "*An Improved Flower Pollination Algorithm for Optimizing Layouts of Nodes in Wireless Sensor Network*," in IEEE Access, vol. 7, pp. 75985-75998, 2019. [CrossRef]
11. J. Liu and J. Lampinen, "*A fuzzy adaptive differential evolution algorithm," IEEE Region 10 Conference on Computers, Communications"*, Control, and Power Engineering. TENCOM '02. Proceedings. Beijing, China, 2002, pp. 606-611 vol.1, 2002.
12. V. Tiwari, Dr. A. A. Waoo, "*Comprehensive Study on Metaheuristics FADE Based Artificial Bee Colony Optimization Algorithm to Improve Performance of Wireless Networks*", IJSRCSEIT, ISSN: 2456-3307, Volume 6 Issue 5, pp, 2020. [CrossRef]
13. G. Kalnoor, J. Agarkhed, and S.R. Patil, "*Agent-based QoS routing for intrusion detection of sinkhole attack in clustered wireless sensor networks"*. In Proceedings of the first international conference on computational intelligence and informatics (pp. 571–583). Springer, Singapore, 2017. [CrossRef]
14. E. Ngai, J. Liu, and M. Lyu, "*An efficient intruder detection algorithm against sinkhole attack in wireless sensor network".* Computer Communications, 30(11), 2353-2364, 2007. [CrossRef]
15. S.A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "*Detection of sinkhole attack in wireless sensor networks*", IEEE International Conference on Space Science And Communication (IconSpace), Melaka, pp. 361-365, DOI: 10.1109/IconSpace.2013.6599, 2013.
16. R. K. Sundararajan and U. Arumugam, "*Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks*", Journal of Sensors, vol. 2015, Article ID 203814, 12 pages, 2015. [CrossRef]
17. I. Krontiris, T. Giannetsos, and T. Dimitriou, "*Launch Sinkhole Attack in Wireless Sensor Network; the Intruder Side*", In Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, (pp.526-531). IEEE, 2008. [CrossRef]
18. K. Kim, and M. J. Baek MJ, "*Performance Evaluation of MINT Route Protocol at Different Scenarios"*. In Lee G., Howard D., Ślęzak D. (eds) Convergence and Hybrid Information Technology. ICHIT 2011. Lecture Notes in Computer Science, vol 6935, 2011.
19. M. Chaudhari, P. Koleva, V. Poulkov, et al, "*Performance Analysis of AODV with Sectoring in Resource Constrained Ad-Hoc Communication Network",* Wireless Pers Commun, 2019. [CrossRef]
20. L. Teng and Y. Zhang, "*Secure Routing Algorithm against Sinkhole attack for Mobile Wireless Sensor Network*", In Computer Modeling and Simulation, 2010. ICCMS'10. [CrossRef]
21. B. S. Kim, H. Park, K. H. Kim, D. Godfrey, K. Kim, "*A Survey on Real-Time Communications in Wireless Sensor Networks*", Wireless Communications and Mobile Computing, vol. 2017, Article ID 1864847, 14 pages, 2017. [CrossRef]
22. S. D. Roy, S. A. Singh, Subhrabrata Choudhury, and N. C. Debnath, "*Countering Sinkhole and Black hole Attacks on Sensor Networks using Dynamic Trust Management*", In computers and Communications, 2008. ISCC 2008. IEEE
23. H. Yadav, S. Tak, "*A Survey on Detection of Sinkhole Attack in Wireless Sensor Network"*, IJERT Volume 06, Issue 11, 2017.
24. Y. Lu, K. Lin, and K. Li, "*Trust Evaluation Model against Insider Attack in Wireless Sensor Networks*," 2012 Second International Conference on Cloud and Green Computing, Xiangtan, pp. 319-326, 2012.
25. K. Pathan, "*Security of Self Organizing Networks-MANET, WSN, VANET, WMN",* ISB N-13:978-1-4398-1920-3. Taylor and Francis Group, 2011.
26. D. C. Mehetre, S.E Roslin, and S. J. Wagh, "*Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust*". Cluster Comput 22, 1313–1328, 2019. [CrossRef]
27. W. Liang, "*Constrained resource optimization in wireless sensor networks with mobile sinks*," 2012 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, pp. 599-603, 2012. [CrossRef]

28. R. Priyadarshi, B. Gupta, and A. Anurag, "*Deployment techniques in wireless sensor networks: a survey"*, classification, challenges, and future research issues. J Supercomput 76, 7333–7373, 2020. [CrossRef]
29. J. Mao, X. Jiang, and X. Zhang, "*Analysis of node deployment in wireless sensor networks in warehouse environment monitoring systems"*. J Wireless Com Network 2019, 288, 2019. [CrossRef]
30. J. Sen, "*A Survey on Wireless Sensor Network Security"*, International Journal of Communication Networks & Information Security, 1(2), 2009.
31. A. Rehman, S.U. Rehman and H. Raheem, Sinkhole Attacks in Wireless Sensor Networks: A Survey. Wireless Pers Commun 106, 2291–2313 (2019). [CrossRef]
32. G. W. Kibirige and C. Sanga, "*A survey on detection of sinkhole attack in wireless sensor network"*. arXiv preprint arXiv:1505.01941, 2015.
33. A. D. Bello, and Dr. O. S. Lamba, "*How to Detect and Mitigate Sinkhole Attack in Wireless Sensor Network (WSN)*", International Journal of Engineering Research & Technology (IJERT) Volume 09, Issue 05, May 2020.
34. B. Zhanga, L. D. Zhaia, and X. Cuic, "*Sinkhole attack detection based on redundancy mechanism in wireless sensor networks*", Volume 31, Pages 711-720 Elsevier, 2014. [CrossRef]
35. I. Krontiris, T. Dimitriou, T. Giannetsos and M. Mpasoukos, "*Intrusion Detection Sinkhole Attacks in Wireless Sensor Network*". In Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE, 2008. [CrossRef]
36. S. Sharmila, and G. Umamaheswari, "*Detection of sinkhole attack in wireless sensor networks using message digest algorithms*". In 2011 international conference on process automation, control and computing (PACC) (pp. 1–6). IEEE, 2011. [CrossRef]
37. T. Wittaya and V. Siripunth, "*Detection of Sinkhole Attack in Wireless Sensor Networks"*, In ICCAS-SICE, 2009 (pp. 1966-1971). IEEE, 2009.
38. D. S. Roy, A. S. Singh, and S. Choudhury, "*Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management*". In Computers and Communications, 2008. ISCC 2008. IEEE Symposium on (pp. 537-542). IEEE, 2008.
39. 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) (pp. 711–716). IEEE, 2010.
40. M. M. Ozcelik, E. Irmak and S. Ozdemir, "*A hybrid trust based intrusion detection system for wireless sensor networks"*, 2017 International Symposium on Networks, Computers and Communications (ISNCC), Marrakech, pp. 1-6, DOI: 10.1109/ISNCC.2017.8071998, 2017. [CrossRef]
41. L. Coppolino, S. D'Antonio, and G. Spagnuolo, "*An intrusion detection system for critical information infrastructures using WSN technologies"*. In Critical Infrastructure (CRIS), 2010 5th International Conference on (pp. 1-8). IEEE, 2010. [CrossRef]
42. A. Papadimitriou, L. F. Fessant and C. Sengul, "*Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. In Secure Network Protocols*", 2009. NPSec 2009. 5th IEEE Workshop on (pp.43-48). IEEE, 2009. [CrossRef]
43. D. Sheela, C. N. Kumar, and G. Mahadevan "*A non-cryptographic method of sinkhole attack detection in wireless sensor networks"*. In international conference on recent trends in information technology (ICRTIT) (pp. 527–532). IEEE, 2011. [CrossRef]
44. G. Jahandoust, and F. Ghassemi, "*An adaptive sinkhole aware algorithm in wireless sensor networks".* Ad Hoc Networks, 59, 24–34, 2017. [CrossRef]
45. D. Gupta, H. Kaur, and R. Kumar, "*Detection of sink hole attack in wireless sensor network using advanced secure AODV routing protocol"*. International Journal of Computer Applications, 156(11), 1–5, 2016. [CrossRef]
46. S. M. Nam, T. H. Cho, "A fuzzy rule-based path configuration method for LEAP in sensor networks, Ad Hoc Networks, Volume 31, Pages 63-79, ISSN 1570-8705, 2015. [CrossRef]
47. M. A. Rassam, A. Zainal, M. A. Maarof, and M. Al-Shaboti, "*A sinkhole attack detection scheme in mint route wireless sensor networks*". International symposium on telecommunication technologies (ISTT) (pp. 71–75). IEEE, 2012. [CrossRef]
48. R. Singh and J. Singh, "*Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks*", Wireless Communications and Mobile Computing, vol. 2017, Article ID 3548607, 14 pages, 2017. [CrossRef]
49. S. Hamedheidari and R. Rafeh, "*A novel agent-based approach to detect sinkhole attacks in wireless sensor networks"*. Computers & Security, 37, 1–14, 2013. [CrossRef]

AUTHORS PROFILE

Dr. Akhilesh A. Waoo, Associate Professor and Head, Department of Computer Science & Engineering, AKS University, SATNA, M.P., India. Dr. Akhilesh A. Waoo is having 20+ years of academic and research experience. His qualification includes Doctorate from MANIT (Bhopal), UGC-NET, M. Tech. (CSE), RHCSA along with IIT-Bombay (RCC), Virtual Lab, and SWAYAM/MOOC coordinator. Academic Experience is flourished with the organization and coordination of national and international events/workshops/seminars. He had published around 80 research papers in international journals with Computer Networks, Network Security AI, IoT as a major areas of interest. He is awarded as Best Faculty. He had published a book on the C# along with chapters in various books. He is a member of Easy chair. He chairs international conferences and he is a member of the Program Committee of International Conference. His research contribution includes the supervision of a Ph.D. / M. Tech. students along with more than 100 dissertations at UG and PG level of students. Also, he is recognized as a reviewer in many international journals. He is a member of the Computer Society of India (CSI) and the International Association of Engineers (IAENG), Hong Kong.

Mr. Virendra Tiwari, Research Scholar, Department of Computer Science & Engineering, AKS University, SATNA, M.P., India. Current research focuses on scaling and extending the functionality of wireless sensor networks (WSN). Having 12+ years of academic and research experience. His qualification includes M.Phill(CSE) from Autonomous College Govt. Pt. Shambhunath (Shahdol) and MCA from SRIT College, Jabalpur (M.P.). Academic Experience is flourished with the organization and coordination of national and international events/workshops/seminars. He had published around 8 research papers in international journals with Computer Networks & Network Security as a major area of interest. He is a member of the International Institute of Organized Research, India. His research contribution got recognized as a Winner of the National Eminent Researcher Award 2020.