Addressing Sinkhole Attacks In Wireless Sensor Networks - A Review

Mubashir Ali, Muhammad Nadeem, Ayesha Siddique, Shahbaz Ahmad, Amir Ijaz

Abstract: Wireless Sensor Networks is a cooperative network of number of sensor devices that communicate in a short range to share the sensed information. The sensor networks have got a great attention due to low cost and ad-hoc deployment structure. Thus, wireless sensor networks have become an important interest of research and many researchers have been working on different aspects of wireless sensor networks i.e. routing mechanism, energy efficiency and security etc. Wireless sensor networks are characterized with low resources i.e. low processing power, low communication resources, low memory and are powered by a battery. To utilize these scarce resources well different trade-offs are their when designing the protocols for wireless sensor networks. Security is most crucial issue in wireless sensor networks due to their nature. The low processing and low memory constraints prohibit the deployment of a protocol with security mechanisms in it. Wireless Sensor networks are deployed in vulnerable environment and are open to sinkhole attacks, wormhole attacks, Greyhole attacks etc. Sinkhole attacks are one of the most dangerous attacks where some fake node advertises fake routing update i.e. shortest path to sink node to malfunction network traffic. In this paper, a systematic literature review is conducted to highlight up to date sinkhole attacks along with their prevention techniques in wireless networks. The analysis is based on various parameters of proposed solutions. The paper also discusses the challenges in detecting the sinkhole attacks.

Index Terms: Wireless Sensor networks, Sinkhole attacks, Wormhole attacks, Blackhole attacks, Sybil attacks, Mitigation Techniques

1. INTRODUCTION

Wireless sensor network (WSN) is a network of tiny radio devices which are sensitive to environment and intelligently collect data from the environment [1]. These collected information is then sent to the sink node that acts as a base station [2]. A basic model of wireless sensor network is shown in figure 1. Communication in sensor nodes is multihop basis and each sensor has limited resources like memory, energy, data rate, communication range and computation power [1], [2].

- *Mubashir Ali is currently associated as a Lecturer with Department of Software Engineering, Lahore Garrison University, Pakistan. His work has appeared in many leading journals and international conferences. His research interests include Internet of Things, Wireless Sensor Networks, Cloud Computing, Data Analytics and Machine Learning.*
  E-mail: dr.mubashirali1@gmail.com, mubashirali@lgu.edu.pk
- *Muhammad Nadeem pursuing his MSCS from Virtual University, Pakistan. Currently, he is affiliated with Punjab School Education Department (PSED). His research interest includes Networks, Information Security and Internet of Things.*
  E-mail: ms170400678@vu.edu.pk
- *Ayesha Saddique received her MS Computer Science degree from University of Agriculture, Faisalabad, Pakistan. She is currently working as a lecturer with Department of Computer Science, United School and Colleges Faisalabad. Her research interest in Networks, Cloud Computing, Big Data and Artificial intelligence.*
  E-mail: ashiayesha1287@gmail.com
- *Shahbaz Ahmad completed his MCS from Islamia University Bahawalpur in 2013 and MSCS from National College of Business Administration & Economics, Sub Campus Bahawalpur in 2018. Currently, he is working as a researcher. His research interest includes Information Security, Network Security, Internet of things and Wireless Sensor Networks.*
  E-mail: shahbaz4426@gmail.com
- *Amir Ijaz received his BEng (Hons) Electronic Engineering degree from Manchester, United Kingdom and his MS Electrical Engineering degree from Islamabad, Pakistan. He is currently based in the department of Computer Engineering at the HITEC University, Taxila, Pakistan. He has published in leading international journals and national venues. His research interests include but are not limited to Communication Engineering, Electronic Systems, Next Generation Networks, Wireless Sensors and the Internet of Everything/Things (IoE/T).*
  E-mail: amirijaz@live.com

These constraints make network very malicious to network attacks and also makes it challenging to deploy any security detection or prevention mechanism due to constrains [3]. Another problem with wireless sensor network cannot use direct routing mechanism. They also cannot use security protocols in their routing mechanisms. Wireless sensor nodes use shortest path routing of nodes deployed in malicious environment [4]. A selfish node take advantage of this malicious environment to advertise fake information through the e network of short range communicating nodes with limited resources [4]. There are various types of attacks in wireless sensor networks like blackhole attack, Greyhole attack, Sybil attack, wormhole attack, sinkhole attack etc [3]. In this paper we focus on sinkhole attacks.

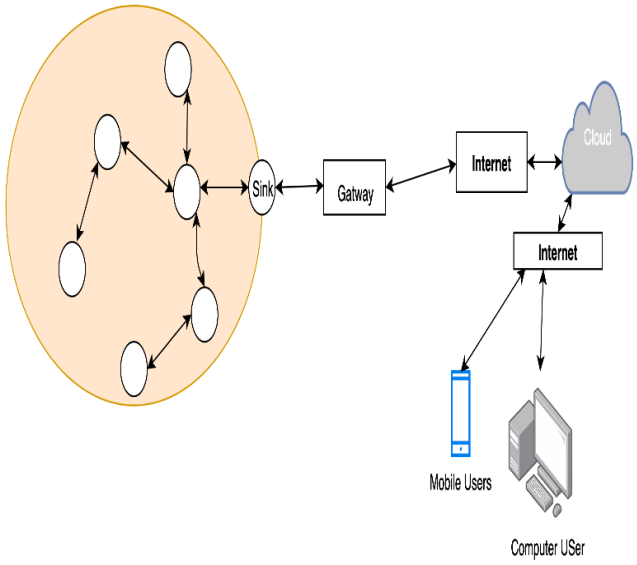

Figure 1. *Wireless Sensor Networks*

Sinkhole attacks take advantage of weak routing mechanism in wireless sensor networks [4]. In Sinkhole attack a fake node intrudes into the network and forms peer with real nodes. It then advertises fake information to change the nodes default forwarding mechanism and prevent the real nodes to send the sensed information to sink node [5]. The malicious node sends

its routing information to decide it the selfish node as the best path to sink node based on routing matrices. The real node then sends its data to that selfish node which can either discard packets or may selectively send packets to sink node [4], [5].

2 LITERATURE REVIEW

Technology has made our environment smart and computing devices very small. This development moved us to sensor networks that is network of cooperative sensor node connected for purpose spaced in a small geographic area. These type of network becoming part of our environment rapidly growing exponentially [2]. The interest in wireless sensor networks actually originated from battlefield and then the commercial user found it very useful for their business premises [1], [2]. Wireless sensor networks are constrained with low power low memory, low storage, low processing speed, short-range communication and are adaptive to form network [1]. Sensor's information is used to make decisions or to take the advantages, thus the information should be original and is not altered in way. Wireless nodes are thus exposed to vulnerability attacks easily [3], [4], [6]. Several issues in wireless sensor network security are managing the keys, authenticating the users, authorizing the nodes, integrity of the messages. These security issues need to be mitigated by using some sophisticated security mechanism which needs more computational power and energy. Moreover, the security issues need an update to the existing network routing mechanisms [6]–[9]. The routing protocols in wireless sensor network do not used direct routing through hops like in wired network, rather they use different routing techniques like flat routing, tree based routing, hierarchical routing and other cognitive approaches based on swarm intelligence and machine learning [4], [10]. One of the most discussed part of wireless sensor networks is their routing mechanism. As wireless nodes have low physical and low network resources, all of their proposed routing protocols take care of these constraints. These requirements trade-off between protocol design and security needs [4], [11], [12]. It is complex task to mitigate the security issues due to constraints on WSN and thus attackers take advantage of these weakness and exploit WSN with different types of attacks. The following are some famous attacks mechanisms deployed in wireless sensor networks.

A. Selective Forwarding: In selective forwarding attacks, some malicious node lies to be real node and selectively drops the packet that are destined to base station. The packets are randomly dropped and thus it is nearly impossible to detect these type of attacks [8]. The selective forwarding creates confusion in packets received in the base station. The dropped packets are requested again and thus reduces the network performance in wireless sensor networks [3], [7], [8].

B. Jamming attacks: In jamming attacks the short-range radio signals of wireless sensor networks are interfered and hence hindrance in reception and transmission of packets. In these types of attacks mostly the resources are overutilized like memory and battery resources [8]. Due to this overutilization the nodes become unavailable to the network most of the time and hence availability constraints [3], [6], [8].

C. Wormhole attacks: In wormhole attacks one or more fake nodes advertise fake short route between two nodes to disrupt the communication between these two nodes [8]. The fake nodes then can drop or selectively forward the data to the base station in wireless sensor network [3], [6], [8].

D. Sybil attacks: In Sybil attacks geographic protocols are infected by adversary which lies to be present at different location in the network and creates multiple identities in the network [8].

E. Sinkhole attacks: In sinkhole attacks a false node sits between base station and neighboring nodes to confuse the communication between them by advertising a false routing information in order to attract the network traffic [8]. The false node can then selectively forward or drop the packet in order to malice the network function [3], [6], [8].

F. Hello Flood attacks: In routing protocols every node need to broadcast hello message to introduce themselves into the network. In hello flood attack a powerful malicious node convinces every node to add it to the network by flooding hello messages [8].

3 SINKHOLE ATTACKS

Sinkhole attack is popular network layer attack in which a false node sits inside the network of real nodes and informs the neighbor nodes a bogus shortest path to base node in order to trap them if it were a best path to send the information to the base node to attract the network traffic. This false node thus disharmonises the network traffic, disrupts network latency and creates indigestion in other network factors to make network as ill as possible [5], [13] as shown in figure 2.

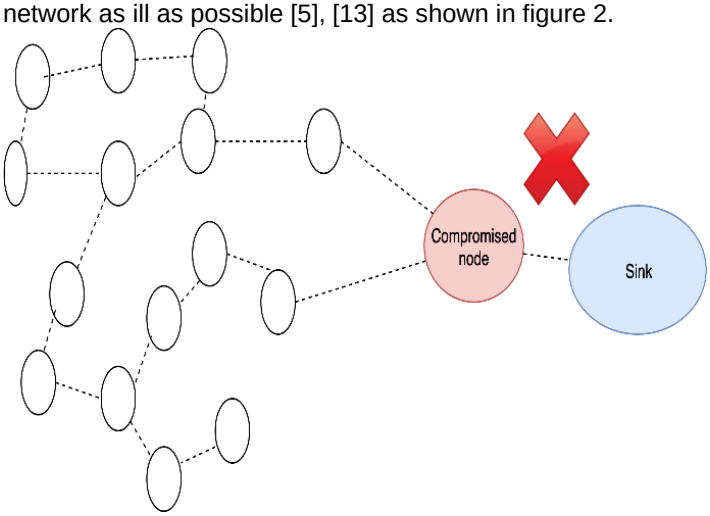

***Figure 2**. Sinkhole Attack*

A sinkhole attack is a serious threat to WSN and most of WSN routing protocols are not good enough to detect this attack [10]. Direct diffusion is a data-centric routing mechanism for forwarding messages through wireless sensor networks [14]. Sink node sends query and waits for node's response. A capable node then sends reply to query of sink node. If multiple queries are sent from multiple nodes for same query, then fake node can take advantage of it and may spoof the broadcast message [5]. In tree-based routing protocols, a minimum spanning tree is constructed to advertise the shortest path to the sink. A false node then can sit between the real node and sink and advertise itself as shortest path to the sink node. All neighbors are then informed about that path and network traffic is trapped to that node to send data to sink. False node then can drop the packet or may selectively forward the messages [5]. TinyOS uses breadth first spanning

tree with sin node. Sink node broadcasts the routing information on regular basis. When updates are available base node acts as parent node and broadcasts the new information to all nodes. A powerful false may sit between the base station and target node and update the routing information. The two nodes then use this information and false node becomes successful to grab the network traffic [5]. A minimum cost forwarding is a mechanism where a cost based shortest path is constructed. A false node advertises minimum cost and traps the node to form shortest path with false node with minimum cost [5].

4 SECURITY GOALS IN WIRELESS SENSOR NETWORKS

In wireless sensor networks, the main focus is on the following security matrices to securely provide the data to sink.

A. Confidentiality: confidentiality means when the data is flying through the sensor nodes to base station, it is kept secret from the middleman or some selfish node who tries to alter or drop the packet. Signature based methods are used to ensure the confidentiality in WSN [3]–[5].

B. Integrity: when data is being transmitted over the network, there may be some false node who react as real node and receives the data. The false node then can alter the message before sending it to the base station. Integrity mechanisms ensure that the data has not been altered during its forwarding by some false node or may detect any change in order to request packet replay [3]–[5].

C. Authentication: In WSN, selfish nodes can add themselves to breach the security. The authentication ensures the identity of the real nodes so that any selfish node may not for peer with the real node [3]–[5], [15].

D. Availability: In WSN, nodes have low energy, low computational resources and low network resources [1], [2]. But still nodes must be available to receive the request all the time. The nodes should be available to sense the environment and collect information to their base station. A selfish node may start a DOS attack to make them unavailable or may start flooding the nodes to consume their energy and computational resources. Availability constraint ensures that nodes are always available for services during network lifetime [3]–[5].

E. Non-repudiation: In sensor network, base node may detect any modification to message for integrity purpose and if modification is detected, base node may ask message replay. The non-repudiation constraint ensures that no node deny replaying the message [3]–[5].

F. Data freshness: one of the security goals in sensor network is to avoid redundancy that is the message received at base station is fresh and no old message is replayed unless requested by the base station [2]–[5].

G. Authorization: In WSN, selfish nodes are harmful. Authorization ensure that only authorized nodes are allowed to send data and are allowed to form peer with other real nodes. Cryptographic methods like hashing and encryption is used to achieve authorization [3]–[5], [16], [17].

5 CHALLENGES IN DETECTION OF SINKHOLE ATTACKS IN WIRELESS SENSOR NETWORKS

Researches have pointed out following challenges in detecting sinkhole attacks.

A. Communication style: In wireless sensor network all the messages are forwarded toward the base station leaving it open to the sinkhole attacks. A sinkhole attacks starts when a false node advertises false routing information in order to attract the network traffic [18]. Based on the communication style the false node only traps the nodes closer to the base station rather than all nodes which make attackers task easy and hence a challenge in detecting the sinkhole attack [5], [13], [17], [18].

B. Unpredictable nature of sinkhole attacks: In WSN, for routing different routing matrices are used for packet forwarding. A false node lies to real nodes about those matrices to be ideal for routing. Thus, real nodes mistakenly use false node. Because of different nature of routing protocols, the nature of sinkhole attack is impulsive [5], [15], [18].

C. Insider node attack: In insider node the false node first becomes part of network by tempering some node or taking advantage of weak system thus acquiring all network privileges and all necessary information of the network. As the false node becomes the part of WSN it becomes challenging for detection system to observe the sinkhole attack in order to prevent or detect it [5], [13], [17]–[19].

D. Limited resources: WSN have limited resources i.e. low energy, low communication range, low memory and storage, less processing power. Therefore, for any protocol design, these constraints should be taken into account. These constraints thus hinder implementing security mechanism in routing protocols [2], [5], [6], [16], [18].

E. Physical attacks: In WSN, nodes are deployed in an unfriendly environment and left unattended most of the time. This makes easy for an intruded to attack a node physically and access to all information [5], [13], [17], [18].

6 ADDRESSING SINKHOLE ATTACKS

To detect attacks on WSN, one needs to regularly check the network behavior. Many researchers classified the detection approaches into the following categories.

A. Rule Based Approach: Sinkhole attacks behavior are impulsive but researcher have tried to investigate specific common attack patterns of sinkhole attacks. These behaviors are then embedded into the detection system. The nodes are checked against these rules in order to detect the false node [3], [5], [13], [18].

B. Anomaly Based Approach: In anomaly-based detection system the detection system searches for anomalies in the sensor network. An anomaly is deviation from what is called normal behavior of sensor nodes [5], [13], [18], [20].

C. Statistical Approach: In statistical approaches nodes physical and network resources are studied to measure the threshold values. Sensor nodes are checked by the detection system against these threshold values to detect the false node [5], [13], [17], [20].

D. Prevention Based Approach: In prevention based approaches, the system is secured through using some cryptographic techniques for preventing the false node to become part of the network [3]–[5], [13], [17], [18].

E. Hybrid Approach: In hybrid approaches both anomaly and cryptographic techniques are used. This ensures the authenticity of the messages and also detects the false nodes [4], [5], [13], [17], [18].

The following table shows various algorithms on these different techniques.

***Table. 1**. Existing Approaches to Address Sinkhole Attacks*

Year	Author	Algorithm	Approach	Outcomes
2017	G. Jahandoust et al. [21]	An adaptive sinkhole aware algorithm	Probabilistic	A probabilistic model is designed to approximate the threshold values from history to and subjective logic model to detect the sinkhole [21].
2017	Z. Zhang et al. [22]	RMHSD algorithm	Rule Based	The approach uses optimal data transmission scheme and uncertainty of the node to detect the sinkhole attack [22].
2018	N. Nithiyanandam et al. [23]	Enhanced particle swarm optimization	Cognitive approach	Ant colony optimization and particle swarm intelligence are used to detect the sinkhole attacks [23].
2019	S. Kori et al. [24]	Wormhole node mitigation algorithm	Fuzzy rule Based approach	Fuzzy inference technique is used to detect the wormhole attack [24].
2018	B. Subba et al. [25]	Game theory Based	Agent Based	The algorithm uses IDs agents at three different level (sensor level, cluster head level and base station level) to guard against malicious nodes [25].
2018	L. Sejaphala et al. [26]	Hop count-based algorithm	Statistical approach	The algorithm uses hop count based threshold values to detect the sinkhole attack [26].
2019	M. Jamshidi et al [27]	Agent Based	Cognitive approach	Intelligent learning agents are used to monitor the network traffic and nodes position in order to detect the false node [27].
2018	K. G. Rana et al [28]	Next neighbour authentication	Signature Based	Every intermediate node that claims fresh route is authenticated against next hop and previous hop to detect the false node [28].
2018	R. R. Malladi et al. [9]	Kalman Filter	Signature Based	A Kalman filter based trust prediction of given node is done to detect false node [9].
2019	V. Gayathri et al. [29]	Randomized algorithm	Signature Based	The algorithm uses randomized algorithm and encryption to achieve security goals [29].
2018	I. J. Jebadurai et al. [30]	Collusion based sinkhole detection	Rule Based	A collusion based algorithm in DSR protocol is used to detect and isolate the sinkhole node [30].
2018	T. T. Vo et al. [31]	MLAMAN	Signature Based	MLAMAN uses multi-level hop-by-hop authentication and neighbourhood relation analysis to prevent wormhole attacks [31].

2018	F. Shang et al. [32]	Cumulative summation algorithm	Anomaly Based	The algorithm uses link quality and majority rule to detect the sinkhole attacks in wireless sensor networks [32].
2019	N. T. Luong et al. [33]	Machine learning algorithm	Cognitive Approach	The approach uses K-Nearest neighbour data mining algorithm to detect and isolate the malicious node for flooding attacks [33].
2015	R. K. Sundararajan et al. [34]	IDs agent algorithm	Statistical approach	The algorithm uses detection metrices such as packets drop rate and network latency to detect the sinkhole through Intrusion detection agents in the network [34].
2015	M. Guerroumi et al. [35]	Hierarchical topology-based scheme	Signature Based	The algorithm divides the network into cells and creates cell leaders to activate their intrusion detection system that uses signature mechanism to detect the false node in the network [35].
2015	O. Naderi et al. [36]	Trust based model	Rule based approach	The authors presented trust model for packets to be delivered and use energy model to detect the sinkhole attack [36].

5 CONCLUSION

Wireless sensor networking is fast growing networks in our daily life. We are having sensor devices all around us. The networking protocols in Wireless sensor networking come with inherent limitations due to the constraints embedded in Wireless devices. These limitations restrict the protocols to mitigate with the challenges that are present in Wireless networks. The most challenging problem in Wireless sensor networks is to propose and energy efficient protocols with security mechanisms due low resources. One of the security challenges in Wireless sensor networks is sinkhole attack which prevent the sensor nodes in dense networks to communicate with sink node. In this paper we have studied sinkhole attacks and provided a review of recent development for detecting the sinkhole attacks. Sinkhole attacks are challenging to design routing protocols and different techniques are proposed to mitigate the sinkhole attacks in wireless sensor network. The paper can be used to study recent advancement and collaborate the new idea in field of sensor networks security.

ACKNOWLEDGMENT

We would like to thank journal editor, area editor and anonymous reviewers for their valuable comments and suggestions to help and improve our research paper.

CONFLICT OF INTEREST

On behalf of all authors, the corresponding author states that there is no conflict of interest.

REFERENCES

[1] J. Zheng and A. Jamalipour, “Introduction to Wireless Sensor Networks,” in Wireless Sensor Networks, J. Zheng and A. Jamalipour, Eds. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2009, pp. 1–18.

[2] S. M. A. Oteafy and H. S. Hassanein, “Evolution of Wireless Sensor Networks,” in Dynamic Wireless Sensor Networks, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2014, pp. 1–8.

[3] C. Li, “Security of Wireless Sensor Networks: Current Status and Key Issues,” in Smart Wireless Sensor Networks, Y. K. Tan, Ed. InTech, 2010.

[4] J. Sen, “Routing Security Issues in Wireless Sensor Networks: Attacks and Defenses,” in Sustainable Wireless Sensor Networks, Y. K. Tan, Ed. InTech, 2010.

[5] A. Rehman, S. U. Rehman, and H. Raheem, “Sinkhole Attacks in Wireless Sensor Networks: A Survey,” Wireless Personal Communications, vol. 106, no. 4, pp. 2291–2313, Jun. 2019.

[6] S. Gothane, Dr. M. V. Sarode, and Dr. K. S. Raju, “Study of Wireless Sensor Networks its Security Issue, Challenges and Security Management,” in NCCSIGMA-16, 2016, pp. 101–104.

[7] I. Tomic and J. A. McCann, “A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1910–1923, Dec. 2017.

[8] “Security Attacks in Ad Hoc, Sensor and Mesh Networks,” in Security in Wireless Ad Hoc and Sensor Networks, Chichester, UK: John Wiley & Sons, Ltd, 2009, pp. 105–120.

[9] R. R. Malladi and D. A. Govardhan, “Securing Wireless Networks Using Trust Based Adaptive Acknowledgement,” vol. 13, no. 13, p. 6, 2018.

[10] V. K. Singh, “Routing in Wireless Sensor Networks,” in Energy-Efficient Wireless Sensor Networks, 1st ed., V. Sharma and A. Pughat, Eds. CRC Press, 2017, pp. 43–68.

[11] M. E. M. Campista and M. G. Rubinstein, “Sensor Routing,” in Advanced Routing Protocols for Wireless Networks, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2014, pp. 71–92.

[12] “Routing,” in Security in Wireless Ad Hoc and Sensor Networks, Chichester, UK: John Wiley & Sons, Ltd, 2009, pp. 65–79.

[13] J. Chaudhry, U. Tariq, M. Amin, and R. Rittenhouse, "Dealing with Sinkhole Attacks in Wireless Sensor Networks," (:unav), Nov. 2013.
[14] N. S. Samaras and F. S. Triantari, "On Direct Diffusion Routing for Wireless Sensor Networks," in 2016 Advances in Wireless and Optical Communications (RTUWO), Riga, Latvia, 2016, pp. 89–94.
[15] ChonBuk National University et al., "Dealing with Sinkhole Attacks in Wireless Sensor Networks," in Interdisciplinary Research Theory and Technology, 2013, pp. 7–12.
[16] N. J. Patel, "Detection & Prevention Techniques of Sinkhole Attack in Mobile Adhoc Network: A Survey," p. 5.
[17] 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 2008 IEEE Symposium on Computers and Communications, Marrakech, 2008, pp. 537–542.
[18] A. Mathew and J. S. Terence, "A survey on various detection techniques of sinkhole attacks in WSN," in 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2017, pp. 1115–1119.
[19] 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, vol. 80, no. 3, pp. 644–653, May 2014.
[20] E. C. H. Ngai, J. Liu, and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," Computer Communications, vol. 30, no. 11–12, pp. 2353–2364, Sep. 2007.
[21] G. Jahandoust and F. Ghassemi, "An adaptive sinkhole aware algorithm in wireless sensor networks," Ad Hoc Networks, vol. 59, pp. 24–34, May 2017.
[22] Z. Zhang, S. Liu, Y. Bai, and Y. Zheng, "M optimal routes hops strategy: detecting sinkhole attacks in wireless sensor networks," Cluster Computing, Mar. 2018.
[23] N. Nithiyanandam, D. P. L. Parthiban, and B. Rajalingam, "Effectively Suppress the Attack of Sinkhole in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique," p. 18.
[24] KLS Gogte Institute of Technology, Department of CSE, Belagavi, Karnataka, India, S. Kori, K. G N, and N. Sidnal, "Distributed Wormhole Attack Mitigation Technique in WSNs," International Journal of Computer Network and Information Security, vol. 11, no. 5, pp. 20–27, May 2019.
[25] B. Subba, S. Biswas, and S. Karmakar, "A Game Theory Based Multi Layered Intrusion Detection Framework for Wireless Sensor Networks," International Journal of Wireless Information Networks, vol. 25, no. 4, pp. 399–421, Dec. 2018.
[26] L. Sejaphala, M. Velempini, and S. V. Dlamini, "HCOBASAA: Countermeasure Against Sinkhole Attacks in Software-Defined Wireless Sensor Cognitive Radio Networks," in 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), Durban, 2018, pp. 1–5.
[27] M. Jamshidi, S. Sheikh Abooli Poor, N. Nasih Qader, M. Esnaashari, and R. M. Mohammad, "A Lightweight Algorithm against Replica Node Attack in Mobile Wireless Sensor Networks using Learning Agents," IEIE Transactions on Smart Processing & Computing, vol. 8, no. 1, pp. 58–70, Feb. 2019.
[28] K. G. Rana, C. Yongquan, and M. Azeem, "Wireless ad hoc network: detection of malicious node by using neighbour-based authentication approach," p. 9.
[29] V. Gayathri and Y. S. Kumarswamy, "Routing and Neighbor Node Cooperation Scheme to Achieve Energy Efficient Encryption for Integrating Wireless Sensor Networks with Internet," vol. 14, no. 11, p. 14, 2019.
[30] I. J. Jebadurai, E. B. Rajsingh, and G. J. L. Paulraj, "A Novel Node Collusion Method for Isolating Sinkhole Nodes in Mobile Ad Hoc Cloud," in Advances in Big Data and Cloud Computing, vol. 645, E. B. Rajsingh, J. Veerasamy, A. H. Alavi, and J. D. Peter, Eds. Singapore: Springer Singapore, 2018, pp. 319–329.
[31] T. T. Vo, N. T. Luong, and D. Hoang, "MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network," Wireless Networks, May 2018.
[32] F. Shang, D. Zhou, C. Li, H. Ye, and Y. Zhao, "Research on the intrusion detection model based on improved cumulative summation and evidence theory for wireless sensor network," Photonic Network Communications, vol. 37, no. 2, pp. 212–223, Apr. 2019.
[33] N. T. Luong, T. T. Vo, and D. Hoang, "FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks," Wireless Communications and Mobile Computing, vol. 2019, pp. 1–17, Jan. 2019.
[34] 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, pp. 1–12, 2015.
[35] M. Guerroumi, A. Derhab, and K. Saleem, "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink," in 2015 12th International Conference on Information Technology - New Generations, Las Vegas, NV, USA, 2015, pp. 307–313.
[36] O. Naderi, M. Shahedi, and S. M. Mazinani, "A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks," International Journal of Information and Education Technology, vol. 5, no. 7, pp. 520–526, 2015.