A Study on Sinkhole Attack Detection using Swarm Intelligence Techniques for Wireless Sensor Networks

G.Keerthana,
Research Scholar,
Department of Computer Science,
Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore, India
keerthana2492@gmail.com

Dr.G.Padmavathi,
Professor and Head,
Department of Computer Science,
Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore, India
ganapathi.padmavathi@gmail.com

Abstract *-- Wireless Sensor Network is one of the emerging fields in research area. It can be applied in several areas such as Area Monitoring, Health Care Monitoring, Environmental and Earth Sensing and Industrial Monitoring. WSNs are most vulnerable to various attacks like Denial of service attack, Wormhole attack, Sybil attack, Sinkhole attack, Select Forwarding attack, Blackhole attack, Malicious node and Hello flood attack. Among these attacks, sinkhole attacks are more vulnerable. This paper provides a survey of various techniques to detect sinkhole attack in WSN. The study also focuses on the application of swarm intelligence techniques for sinkhole attacks detection.*

Keywords - Intrusion Detection, Sinkhole Attack, Sinkhole Attack Detection, Wireless Sensor Network

1. INTRODUCTION

Wireless Sensor Network is a collection of tiny sensor nodes that are capable of sensing and processing the data. Sensor nodes are the basic units in a sensor network. WSN can be deployed in an unattended environment that is not physically protected. It is used to monitor the environment and send the collected data to the base station. The main components of WSN node are Controller, Communication device, Sensors, Memory and Power supply. It offers several advantages namely, Reliability, Scalability, Flexibility and Ease of Deployment [1]. A typical wireless sensor network scenario is shown in figure 1.

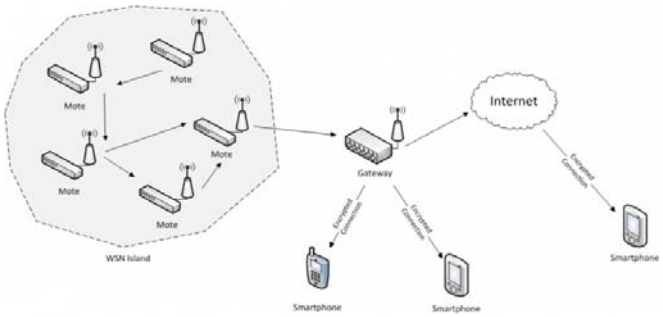

Fig.1 Example Wireless Sensor Network

Though WSNs are less protective, it is more vulnerable to various attacks. Attacks can be basically classified into two categories namely, Active attacks and Passive attacks.

A. Passive Attacks

The unauthorized attackers that monitor and listen the communication channel [2] are known as passive attacks. Classification of passive attacks is shown in figure 2.

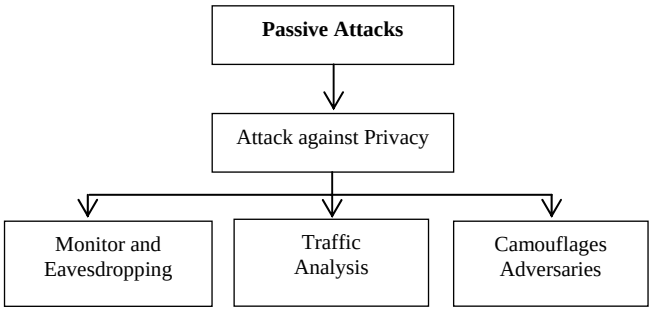

Fig.2 Passive Attacks

B. Active Attacks

The unauthorized attackers that monitor, listen and modify the data stream in the communication channel [2] are known as active attacks. Classification of active attacks is as follows.

i. Routing attacks
ii. Denial of Service
iii. Node Malfunction
iv. Node Outage
v. Physical attacks
vi. Message Corruption
vii. False Node
viii. Node Replication attack

Sinkhole attack is particular type of routing attack classified under active attack category.

C. Sinkhole Attack

In a sinkhole attack, the intruder's aim is to lure all the traffic from a particular area through a compromised node, to launch an attack. The compromised node tries to attract all the traffic from neighbor nodes based on the routing metrics used in the routing protocol [3]. Sinkhole attack is one among the routing attacks. Sinkhole attacks are difficult to counter because the routing information supplied by a node in a

wireless sensor network is difficult to verify. A network with a sinkhole attack is shown in figure 3.

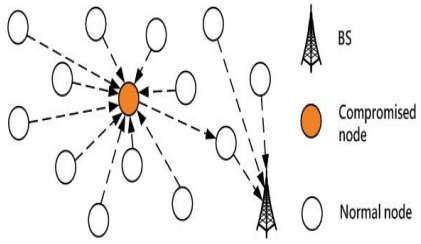

Fig.3 Sinkhole Attack

Sinkhole attack is a type of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself. Once Sinkhole attacks enter into a network, they are capable of performing series of attacks namely, Selective Forwarding attack, Wormhole attack, Flooding attack, Sybil attack and Black hole attack [4].

The objective of this paper is to discuss about sinkhole attack, its vulnerabilities, different sinkhole attack detection techniques and application of swarm intelligence techniques for sinkhole attack detection.

This section discussed about the wireless sensor networks, attacks in wireless sensor networks and in particular about sinkhole attack. Rest of the paper is organized as follows; Section 2 discusses the classification of intrusion detection system. Section 3 discusses about the different techniques in Detecting Sinkhole attacks. Section 4 discusses the experiments conducted and the results. Section 5 concludes the work.

2. Intrusion Detection Systems

Intrusion Detection System is a device which monitors the events taking place in a system. The goal of IDS is to accurately detect computer security incidents, and notify network administrators. Intrusion detection systems in wireless sensor networks are classified into three types on the basis of its detection technique [5]. They are Misuse detection Anomaly detection and Specification detection. Figure 4 shows the major Intrusion Detection Systems followed in most of the literature.

A. Misuse Detection

A signature is a pattern or string that corresponds to a particular activity or threat. Misuse Detection is the process to compare patterns against captured events for recognizing possible intrusions. Misuse Detection is also known as Knowledge-based Detection or Signature-based Detection [5].

B. Anomaly-based Detection

An anomaly is a deviation to a known behavior [5]. Generally, profiles represent the normal or expected behaviors derived from monitoring regular activities, network connections, hosts or users over a period of time. AD is also called as Behavior-based Detection. Some Anomaly Based Detection techniques are statistical model approach, Machine learning approach, Game theory approach and Swarm Intelligence.

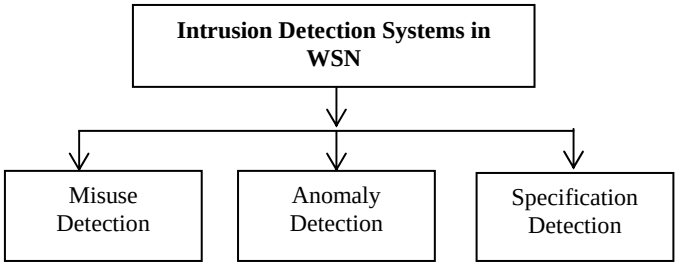

Fig.4 Intrusion Detection System in IDS

C. Specification-based Detection

Specification based techniques compare the behavior of objects with their associated security specifications that capture the correct behavior of the objects. This technique does not detect intrusions directly; it detects the effect of the intrusions as run-time violation of the specifications instead. This is also known as Stateful Protocol Analysis [5]. The next section explains the significant works on sinkhole attack detection.

3. Related Works for Sinkhole Attack Detection

Many researchers have proposed several techniques for detecting sinkhole attacks in wireless sensor networks [6-11]. It is observed that some recent works in sinkhole attack detection use techniques such as Swarm intelligence, Geostatistical model, Redundancy mechanism, using Request and reply of sequence numbers, analyzing the network information and using base station. They are presented below.

N.K. Sreelaja, G.A. Vijayalakshmi Pai [6] proposed a model to detect a sinkhole attack. This model identifies an intruder in a wireless sensor network using Ant Colony Optimization. The proposed ACO-AD algorithm for sinkhole attack detection is better when compared to the classical rule matching approaches. The ACO-AD algorithm does not generate false positives. Further, it overcomes the drawbacks of the neural network architecture and support vector machine architecture for rule matching. The number of searches using ACO-AD algorithm is less when compared to the traditional binary search and sequential search methods.

H.Shafiei, A.Khonsari, H.Derakhshi, P.Mousavi [7] proposed two techniques to detect and mitigate sinkhole attacks. It provides a centralized approach to detect suspicious regions in the network using geostatistical hazard model. This has been proposed to estimate the energy holes. A distributed monitoring approach has been proposed to detect malicious behaviors and to explore every neighborhood in the network to detect the energy holes. The authors proposed a lightweight mitigation method to eliminate sinkholes. The mitigation scheme prevents the traffic flow toward sinkholes and thus eliminates the threat of the sinkholes. Their approach successfully prevents traffic flow towards the regions reported

as suspicious, thus, the rate of packet delivery to those regions is reduced significantly.

Fang-Jiao Zhang, Li-Dong Zhai, Jin-Cu Yang, Xiang Cui [8] proposed a redundancy mechanism to detect the sinkhole attack in a network. In case, if there is any suspicious node in a network, messages are sent to them through multi-paths. The process of path establishment consists of three stages: Route request, Route reply and Route establishment. Trusted node forwards the routing request in any established paths. The reply messages sent by the suspicious nodes are used to confirm whether that suspicious node is malicious or not. The proposed detection algorithm is compared with classical detection algorithm and it is concluded that proposed algorithm has higher detection rate.

Tejindereep Singh and Harpreet Kaur Arora [9] proposed a novel algorithm for detecting sinkhole attack. They proposed a solution for sinkhole attack detection in three steps, i) the sender node first requests the sequence number with the rreq message, the node replies with its sequence number through rrepmessage, ii) transmitting node will match sequence number in its routing table. If it matches, then data will be shared; otherwise, it will assign the sequence number to the node, iii) If the node accepts the sequence number then the node will enter in the network; otherwise, it will be eradicated from the network. Two parameters, packet lost and packet received are considered for comparison.

Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi and Sanaz Sadegi [10] proposed a novel algorithm for detecting sinkhole attacks in WSN using base station. Base Station checks the data transmission path and keeps the existing nodes in its memory. Whenever it detects the existence of errors in a packet repeatedly, it checks the path and compares the nodes kept in memory with the new path. It keeps similar nodes in memory and deletes the remaining data. Hence base station detects the malicious node, notifying other nodes not to transmit data to malicious node anymore. The proposed algorithm decreases the packet loss and energy consumption.

Edith C.H.Ngai, Jiangchuan Liu, Michel R.Lyu [11] proposed an efficient algorithm to detect the sinkhole attack. The algorithm finds a list of suspected nodes through checking the data consistency. By analyzing the network flow information, algorithm identifies the intruder in the list. The algorithm is capable of dealing with multiple malicious nodes. The performance of the proposed algorithm is evaluated through numerical analysis and through simulations. Table 1 shows the comparison of sinkhole attack detection methods.

Table 1 Comparison of Sinkhole Attack Detection Techniques

Techniques and Authors	Method of Study	Metrics Considered for Evaluation	Tools used
ACO-AD algorithm N.K. Sreelajaa et al	Simulation	Detection rate, False alarm rate and Number of searches	--
Redundancy Mechanism H.Shhafiei et al	Simulation	Detection rate, Mistake rate, Miss rate	NS2
Geostatistical Hazard Model Fang-Jiao Zhang et al	Simulation	Threshold. Number of monitors and Number of hops	OMNET++
Method using Request (rreq) and Response (rrep) for sequence number Tejindereep Singh et al	Simulation	Packet lost and Packet Received	NS2
Method using Base Station Maliheh Bahekmat et al	Simulation	Packet lost, Accuracy and Energy consumption	MATLAB
Method by analyzing network information Edith C.H. Nagai et al	Real Deployment	Accuracy and Energy consumption	--

4. Observations and Discussions

Certain observations are made due to the study of literatures in sinkhole attack detection. It is observed that so far only one method is available in the literature using swarm intelligence techniques. Further not all swarm intelligence methods are explored for sinkhole detection. So an attempt is made to study the significance of the application of the particle swarm optimization to detect sinkhole attacks in wireless sensor networks. Apart from the detection rate and packet delivery ratio, message drop, average delay, false alarm rate, false positive rate, F-measure precision, ROC curves and area under ROC curves (AUC) are also important measures that can be applied evaluate the performance of sinkhole attack detection methods. As discussed above, the two swarm intelligence methods namely Ant colony Optimization and Particle swarm optimization are applied for sinkhole attack

detection. The next section discusses the experimental methodology and the results due to experimentation.

5. Experimental Results

Network Simulator 2 is used to create the experimental setup. It supports simulations of TCP and UDP, MAC layer protocols, various routing and multicast protocols in Wireless Sensor Networks. Ant colony optimization (ACO), Particle swarm optimization (PSO) algorithms are tested in the simulated environment. Flowchart of ACO is shown in figure 5 and flowchart of PSO is shown in figure 6.

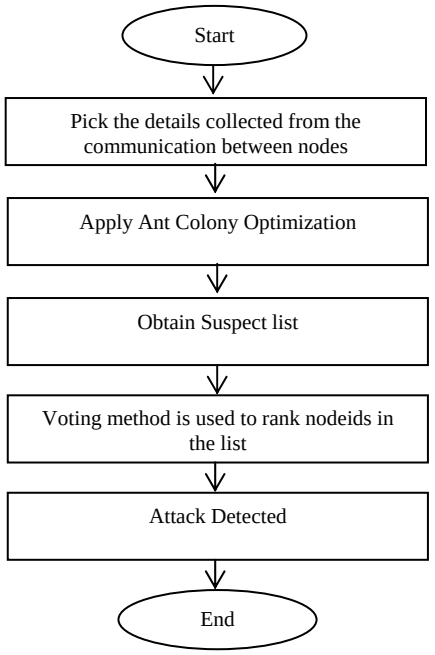

Fig.5 Flow chart of Ant Colony Optimization

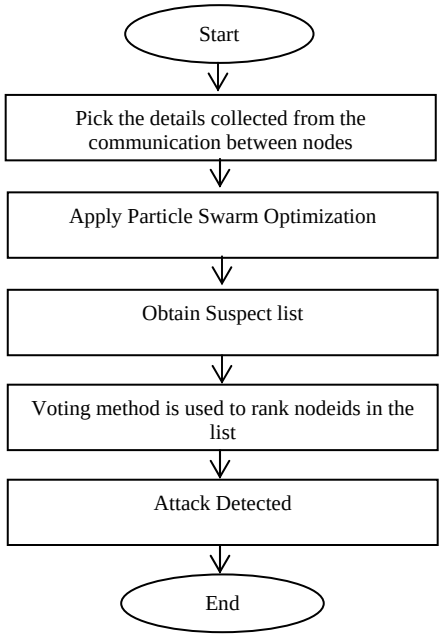

Fig.6 Flow Chart of Particle Swarm Optimization

Comparison of various performance metrics are given in the table 2. Performance metrics like detection rate, false alarm rate, packet delivery ratio, message drop and average delay are used for comparison. From the results it is concluded that particle swarm optimization performs better than ant colony optimization.

Table 2. Comparison of ACO and PSO

Metrics / Algorithms	**ACO**	***PSO***
Detection Rate (%)	87.062	***88.622***
False Alarm Rate (%)	10.648	***9.656***
Packet Delivery Ratio (%)	78.848	***81.178***
Message Drop (%)	7.616	***6.086***
Average Delay (sec)	11.918	***9.128***

5. Conclusion

This paper presented the different detection mechanisms of sinkhole attacks in the wireless sensor networks proposed by different researchers. Detecting sinkhole attack in wireless sensor network is a challenging task. Swarm Intelligence technique is one of the effective methods in detecting sinkhole attacks in wireless sensor network. It is concluded that swarm intelligence technique namely particle swarm optimization technique is more effective when compared to ant colony optimization in detecting sinkhole attacks.

REFERENCES

[1] Priyanka Rawat, Kamal Deep Singh, Hakima Chaouchi, Jean Marie Bonnin, "*Wireless sensor networks: a survey on recent developments and potential synergies*", Springer, Vol. 68, issue 1, pp. 1-48, April 2014.

[2] Dr. G. Padmavathi, D. Shanmugapriya, "*A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Network*", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[3] Vinay Soni , Pratik Modi , Vishvash Chaudhri, "*Detecting Sinkhole Attack in Wireless Sensor Network*", International Journal of Application or Innovation in Engineering & Management, Vol. 2, issue 2, pp.29-32, February 2013.

[4] Rajakumaran L, Thamarai Selvi R, "*Detection Techniques of Sinkhole Attack in WSNs: A Survey*", International Journal of Engineering Science Invention, Volume 3, Issue 6,PP.12-14, June 2014.

[5]Hung-Jen Liao, Chun-HungRichardLin, Ying-ChihLin, Kuang-YuanTung, "*Intrusion detection system: A comprehensive review*", Elsevier Journal of Network and Computer Applications, Vol. 36, pp. 16-24, 2013.

[6] N.K. Sreelajaa, G.A. Vijayalakshmi Pai, "*Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks*", Elsevier Applied Soft Computing, Vol.19, pp. 68-79, 2014.

[7] H.Shafiei, A.Khonsari, H.Derakhshi, P.Mousavi, "*Detection and mitigation of sinkhole attacks in wireless sensor networks*", Elsevier Journal of Computer and System Sciences, Vol.80, pp. 644-653, 2014.

[8] Fang-Jiao Zhang, Li-Dong Zhai, Jin-Cu Yang, Xiang Cui, "*Sinkhole attack detection based on redundancy mechanism in wireless sensor networks*", Elsevier Procedia Computer Science, Vol. 31, pp. 711 – 720,2014.

[9] Tejindereep Singh and Harpreet Kaur Arora, "*Detection and Correction of Sinkhole Attack with Novel Method in WSN using NS2 Tool*", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 2, 2013.

[10] Maliheh Bahekmat, Mohammad Hossein Yaghmaee, Ashraf Sadat Heydari Yazdi and Sanaz Sadegi, "*A Novel Algorithm for Detecting Sinkhole Attacks in WSNs*", International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012.

[11] Edith C.H.Ngai, Jiangchuan Liu, Michel R. Lyu, "*An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks*", Elsevier Computer Communications, Vol.30, pp. 2353–2364, 2007.

Author's Biography

G.Keerthana received her M.Sc Computer Science degree in 2014 from Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She is pursuing her M.Phil at Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. Her areas of interest are Network Security, Wireless Sensor Networks.

Dr.G.Padmavathi is the Professor and Head of computer science Department of Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. She has 27 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Wireless Communication, Network Security and Cryptography. She has significant number of publications in peer reviewed International and National Journals. Life member of CSI, ISTE, WSEAS, AACE and ACRS.