Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 511-515
Received 15 April 2021; Accepted 05 May 2021.

A Survey on Sinkhole Attack in RPL

T.Parkavi*[1],Dr.L.Arockiam[2]

*[1]Department of Computer Science, St. Joseph's College(autonomous), (Affiliated to Bharathidasan university)Tiruchirappalli, Tamil Nadu, India.
[2]Department of Computer Science, St. Joseph's College (autonomous), (Affiliated to Bharathidasan university), Tiruchirappalli, Tamil Nadu, India.

ABSTRACT

Internet of Things (IoT) is an innovative idea intended to perform a complex task. In IoT, the devices are connected to the physical world to collect data. The works performed by the IoT devices are sensing, routing and storing. There are certain drawbacks in the IoT environment and most of the issues are occurring in the routing process. The routing process is performed by the routing protocol. In the process of routing, the attacker node creates some issues in the normal packet transmission process. This paper focuses on the Routing Protocol for Low- Power and Lossy Network (RPL) and some security issues occurring in the routing protocol. A brief discussion on the sinkhole attack in RPL and the issues related to this attack in IoT environment is also given. The sinkhole attack creates network traffic, drops the information and gives fake information. Finally an analytical survey on sinkhole attack is also given in this paper.

KEYWORDS: Internet of Things (IoT), Network, RPL, Sinkhole attack.

INTRODUCTION

Internet of things (IoT) is one of the fascinating advancements in the technological world. IoT concept helps us to perform complex tasks. Many IoT devices are designed and launched. There is no standard architecture for IoT. Depending on the application of the architecture, the IoT functionality varies. There are three-layer, four-layer, five-layer and seven-layer architectures. Each layer has an individual role in performing the task. The three-layer architecture consists of an application layer, network layer and sensing layer. The sensing layer collects the information using the sensors. The sensor is connected to the physical environment. The information from the sensor is collected, and it is transferred by the network layer. Routing the information is the main task of the network layer that is done using the wired or wireless medium. The application layer collects information from the network layer. The collected information is stored and displayed to the user.

In this paper, the issues occurs in the routing process are discussed. The RPL is the routing protocol specially designed for Internet of Things. In RPL, the routing process will begin after constructing the DODAG. DODAG stands for Destination Oriented Directed Acyclic Graph. The DODAG is constructed by using the control messages. The control messages used in RPL are DODAG Information Object (DIO), Destination Advertisement Object (DAO), DAO Acknowledgement (DAO-ACK) and DODAG Information Solicitation (DIS). The Rank values are calculated based on the Objective Function (OF). The OF is used to construct the path based on the scenario in the network. There are three types of Objective Functions used in the RPL. They are Hop, Energy and Expected Transmission Count (ETX). Each Objective Function uses a different method to calculate the rank value. Routing attacks occur during the routing process, because of the security problems that emerge during the construction of routing path on the network.

In this paper, a brief discussion is done on the security issues in RPL and sinkhole attack. This paper is organized as follows: Section 1 provides a brief introduction to IoT and RPL. Section 2 presents the state of the art of existing works, Section 3 elaborates the issues and challenges of RPL and sinkhole attack, Section 4 presents the existing works on sinkhole attack in RPL and Section 5 presents the conclusion.

RELATED WORK

The Routing Protocol for Low-Power Lossy Network (RPL) is a routing protocol for the resource constrained environments. In routing, attacker forwards all fake messages to legitimate nodes. These attacks create a dynamic path between parent and children. There are different types of attacks against on RPL

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 511-515
Received 15 April 2021; Accepted 05 May 2021.

topology such as Sybil, Selective-Forwarding, Black hole, Wormhole, Sinkhole, Hello Flood, Rank attack etc. This section discusses the related works on sinkhole attack in the RPL network.

Mahmood et al [1] proposed a lightweight technique named as Neighbor-Passive Monitoring Technique (NPMT), and also explained the need to protect the RPL network against internal attacks. This technique was evaluated by the Cooja simulator. The Performance considers the routing metrics namely power consumption and detection accuracy. The sinkhole attack detection can be enhanced by focusing on the re-ranking method.

Stephan et al [2] proposed an Alternative Parent (AP) information method to identify the sinkhole attack. This method provides security to the IoT nodes against the unwanted traffic created by the attacker node. The simulation resulted in the lowest false positive and false negative.

Byung et al [3] proposed a technique with two phases. The two phases are network initialization phase and attack detection phase to identify the sinkhole attack in Link Quality Indicator. Network initialization phase collects the normal information in the network to detect the attack. Attack detection phase uses two methods to identify the attacker node in the network based on link quality and the change in smallest value. Finally the indicator node detects the falsification path cost in routing request message.

Kannan et al [4] proposed a Flow Based mitigation model to detect and mitigate Sinkhole attacks with the support of time variant snapshots (FBSD). This method is to maintain the traffic flow and features to make logs into the dataset. It helps to reduce the network's over-head caused by flooding control messages and improves its efficiency.

Mahmood et al [5] proposed a hybrid monitoring technique for detecting abnormal behavior in RPL -based network. The performance of this method was evaluated by using Cooja simulator. In this method, passive nodes are introduced. It can control data processing and analysis without affecting network constrained nodes. The power consumption in each node is decreased to 55%.

Jin Qi et al [6] proposed the multi hop link quality mechanism to detect sinkhole attack in wireless sensor network. The mechanism verified the link quality by using the sender's log files to identify the malicious node. Link quality was computed based on hop. The mechanism achieved better result to detect the sinkhole attack and increased Packet delivery ratio of the nodes in the network.

Khurram et al [7] proposed a novel method for ad hoc networks. It can modify Ad Hoc On-Demand Routing Protocol for Sinkhole Detection and Removal (AODV-SDR). In this method, only destination node is authorized to reply the route request. The simulation result for this environment identified the attacker node with high accuracy and low latency.

Yuxin et al [8] proposed a Probe Route based Defense Sinkhole Attack (PRDSA) to detect the sinkhole attack. The main contribution of this scheme is to provide an effective means to bypass the sinkhole attack and also to find the safe path. This method very effectively detected and located the sinkhole attack. The performance of this environment can be designed to achieve better network security and lifetime.

From this review, the security issues in sinkhole attack related to RPL are understood. In the following section, the issues and challenges in RPL network are presented.

ISSUES AND CHALLENGES IN RPL NETWORK

The concept of the Internet of Things has the capability of performing challenging and complex tasks. Due to the lack of some security aspects, there are many challenges in IoT. Data Confidentiality, Data Integrity, Data Authentication, Data Freshness, Availability, Self -Organization, Time Synchronization, Secure Localization, Flexibility, Robustness, and Survivability are some of the security issues [11] .

Some other issues that affect the performance of the IoT are Devices heterogeneity, Scalability, Ubiquitous data exchange through wireless technologies, Energy-optimized solutions, Localization and tracking capabilities, Self-organization capabilities, Semantic interoperability and data management, Embedded Security and privacy-preserving mechanisms [12]. The RPL network is specially designed for IoT. There are lots of security issues occurring in the routing process.

In the routing process, one of the main issues is the entry of a malicious node into the network. A malicious node enters into the network as a neighbor and drops the information. There are different types of attacks in the RPL network layer, such as Sybil, Selective-Forwarding, Black hole, Wormhole, Sinkhole, Hello Flood, Rank attack etc. During routing, the attacker node causes some interruption in the normal packet transmission process of the RPL network. This paper focuses on the sinkhole attack; these attacks drop the message and give fake information to the network.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 511-515
Received 15 April 2021; Accepted 05 May 2021.

SINKHOLE ATTACK

The sinkhole attack is a kind of routing attack that affects normal routing process in the network. The attack is like a sink, acts as a source node and gets all the information and drops it. The attacker node creates network traffic and gives false information. It utilizes the threats and Vulnerabilities in the RPL network to attract huge traffic by advertising fake information data that can be modified in it.

When comparing all routing attacks the sinkhole attack is the most destructive attack in the network. This attack creates more damage in the routing path of the network. It increases the network traffic and collapses the network communication and also generates fake information and sends the route request to neighbor nodes. This attack is performed to compromise the neighbor nodes.

The compromised nodes try to attract all network traffic from other nodes. Sinkhole attack introduces fake routing information to attract network traffic. The compromised node can achieve it and also launch this attack. Fig 3.1 explains the sinkhole attack in the RPL.

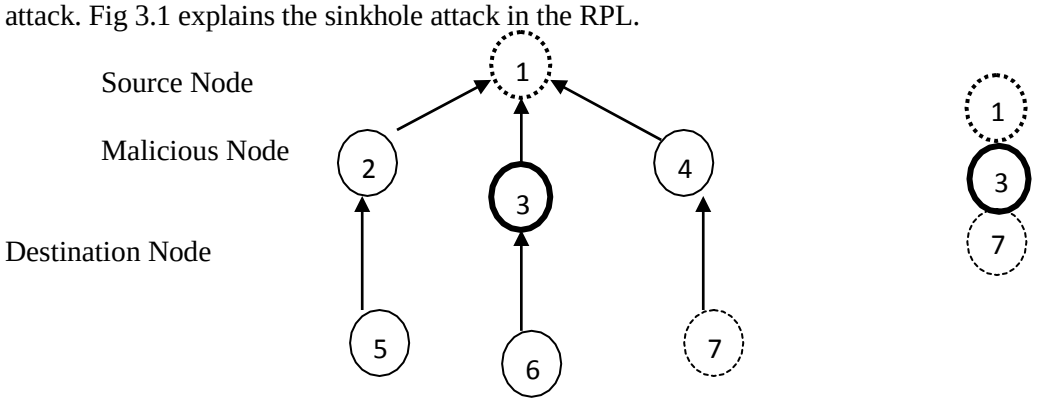

Figure3.1- Sinkhole Attack

This figure 3.1 explains the sinkhole attack in the routing network. Node 1 is a source node, 7 is the destination node and 3 is the malicious node. The attacker node 3 acts as source node 1 and gets all the information and drops the messages. Finally, the attacker node creates network traffic and gives fake information to the network.

EXISTING SYSTEM

In routing, the attacker node has some interruption in the normal packet transmission process. The existing methods to detect the sinkhole attack are given in table 4.1. There are more drawbacks and issues on existing works for detecting the sinkhole attack.

Table4.1: Overview of existing system used to detect Sinkhole Attack on RPL.

Author Name	Proposed technique	Parameters Considered for Evaluation	Drawback
Mahmood et al.,[1]	Neighbor Passive Monitoring Technique (NPMT)	Energy, Accuracy	It concentrated on two passive nodes only.
Byung et al.,[3]	Network Initialization and attack detect phase	Cost	Sometimes, there is no detector node in neighborhood of source node.
Wei yang et al.,[10]	Finite State Machine(FSM)	Time	It focused on only one parameter.
Jin Qi et al.,[6]	Robust sensing mechanism	Cost	It does not allow parent changing process.
Mahmood et al.,[5]	Hybrid Monitoring Technique	Energy, Accuracy	High resource consumption due to the agent overhead processing, which is

			placed in each node.
Yuxio Liu et al.,[8]	Probing Route Defense Sinkhole Attack(PRDSA)	Energy, Lifetime, Packet Loss Rate	The network Life time is too short.
Kannan et al.,[4]	FBSD Method	Packet delivery ratio, Energy, Lifetime	Only a few numbers of traffic pattern will be maintained.
Khurram et al.,[7]	AODV-SDA	Energy, Time, Accuracy	The detection system has only proper Limited validation period.
Kevin et al.,[9]	Parent fail-over and Rank authentication technique	Energy, Accuracy	Need to combine two techniques to detect the attack.

This article cites the various techniques, methods, mechanisms to detect the sinkhole attack. Many researchers proposed techniques to detect the sinkhole attacks and gave solution for this attack. Routing parameters are used to increase the performance of the method in the RPL network. In the existing methods, some drawbacks have been found and are given in table 4.1.

CONCLUSION

The Internet of Things (IoT) can perform sensing, routing and storing in the network. Here the work is focused on the routing side. The routing protocol is used to share the information between the nodes in the network. In routing, there are a lot of issues and challenges in RPL network. The survey is based on the routing attacks in RPL network. The existing methods are analyzed to find out the drawbacks in sinkhole attack detection. The sinkhole attack drops the message and sends fake information to the source node and cause the environment to collapse. This work is to focus and carryout the sinkhole attack to analyze and identify the attacker node.

REFERENCES

[1] Alzubaidi, Mahmood, Mohammed Anbar, and Sabri M. Hanshi. "Neighbor-passive monitoring technique for detecting sinkhole attacks in RPL networks." In Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence, pp. 173-182. 2017.

[2] Stephen, Raju, A. Dalvin Vinoth Kumar, and L. Arockiam. "Deist: dynamic detection of Sinkhole attack for Internet of Things." International Journal of Engineering And Computer Science 5, no. 12 (2016): 19358-19362.

[3] Choi, Byung Goo, Eung Jun Cho, Jin Ho Kim, Choong Seon Hong, and JinHyoung Kim. "A sinkhole attack detection mechanism for LQI based mesh routing in WSN." In 2009 International Conference on Information Networking, pp. 1-5. IEEE, 2009.

[4] Devibala, Kannan, SaminathanBalamurali, AyyanarAyyasamy, and Maruthavanan Archana. "Flow based mitigation model for sinkhole attack in wireless sensor networks using time-variant snapshot." International Journal of Advances in Computer and Electronics Engineering 2, no. 05 (2017): 14-21.

[5] Alzubaidi, Mahmood, Mohammed Anbar, Yung-Wey Chong, and Shadi Al-Sarawi. "Hybrid Monitoring Technique for Detecting Abnormal Behaviour in RPL-Based Network." Journal of Communications 13, no. 5 (2018).

[6] Qi, Jin, Tang Hong, KuangXiaohui, and Liu Qiang. "Detection and defence of Sinkhole attack in Wireless Sensor Network." In 2012 IEEE 14th International Conference on Communication Technology, pp. 809-813. IEEE, 2012.

[7] Rana, Khurram Gulzar, Cai Yongquan, Allah Ditta, Muhammad Azeem, and Muhammad Qasim. "Circumventing sinkhole attack in ad hoc networks." International Journal of Wireless and Mobile Computing 9, no. 4 (2015): 363-369.

[8] Liu, Yuxin, Ming Ma, Xiao Liu, NaixueXiong, Anfeng Liu, and Ying Zhu. "Design and analysis of probing route to defense sink-hole attacks for Internet of Things security." IEEE Transactions on Network Science and Engineering (2018).

[9] Weekly, Kevin, and Kristofer Pister. "Evaluating sinkhole defense techniques in RPL networks." In 2012 20th IEEE International Conference on Network Protocols (ICNP), pp. 1-6. IEEE, 2012.

[10] Yang, Wei, Yuan Wang, Zhixiang Lai, Yadong Wan, and Zhuo Cheng. "Security Vulnerabilities and Countermeasures in the RPL-based Internet of Things." In 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 49-495. IEEE, 2018.

[11] Balte, Ashvini, AsmitaKashid, and Balaji Patil. "Security issues in Internet of things (IoT): A survey." International Journal of Advanced Research in Computer Science and Software Engineering 5, no. 4 (2015).

[12] Rondon, Luis Puche, Leonardo Babun, Ahmet Aris, Kemal Akkaya, and A. SelcukUluagac. "Survey on Enterprise Internet-of-Things Systems (E-IoT): A Security Perspective." arXiv preprint arXiv:2102.10695 (2021).