JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4976-4983
https://publishoa.com
ISSN: 1309-3452

Wormhole Attack Detection in RPL- Protocol based on RSSI Value

[1]V. Mathavan, [2]S. Vanakovarayan, [3]K. Loganathan
[1] Associate Professor, Department of computer Science and Engineering,
Mailam Engineering College, Mailam
mathavancse@mailamengg.com
[2] Associate Professor, Department of computer Science and Engineering,
Mailam Engineering College, Mailam
vanakovarayancse@mailamengg.com
[3] Assistant Professor, Department of Information Technology
Mailam Engineering College, Mailam
klnathan83@gmail.com

Received: 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10

Abstract*:*
It is possible that the Internet of Things will revolutionize the world in the same way as the Internet did. This is possible to be much more so". The Internet of Things (IoT) does not fundamentally alter our lives or the computer sector, but it may be seen yet another step forward in the maturation of the Internet that we have already taken. This is accomplished via the development of a more advanced environment for humans, which will automatically recognise the needs of human beings and act in response to those needs. However, coordinating the communication of such many devices is a difficult issue for that. The Routing Protocol for Low-Power and Lossy Networks (RPL) is a unique routing protocol that has been standardised for use in limited situations such as 6LoWPAN wireless ad hoc networks. 6LoWPAN security is difficult to achieve because the devices are connected to the untrusted Internet and have limited resource availability, the communication links between the devices are lossy, and the devices use a variety of novel Internet of Things technologies such as RPL, 6LoWPAN, and CoAP/CoAPs. Throughout this article, we present a thorough examination of Internet of Things technologies, as well as their novel security capabilities that may be abused by attackers or intrusion detection systems. In this study, we provide the development and demonstration of well-known routing attacks against 6LoWPAN networks that use RPL as their routing protocol. This is a significant addition. We built the wormhole attack and its application on the Internet of Things with the aid of the contact operating system.

Keywords: Iot, Rpl- Protocol, Wormhole Attack

Introduction:

Modern computer and communication technologies are presently paving the way to realise the Internet of Things (IoT), a vision in which smart items, i.e. everyday objects that have been equipped with communication capabilities, may be effortlessly incorporated into information systems [1] [2]. The Internet of Things is predicted to bring about substantial changes in a variety of sectors of

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4976-4983
https://publishoa.com
ISSN: 1309-3452

our life, including health (e.g., remote patient monitoring), the home (e.g., smart lighting and heating),and the city (e.g., smart traffic and parking applications). When considered in this context, wireless sensor and actuator networks (WSANs) will be an important building block because they will allow for the rapid installation of smart objects over large areas while keeping deployment costs low. Wireless sensor and actuator networks (WSANs) are a type of network that uses radio waves to communicate with other devices.

Data distribution through wireless lines in a multi-hop method eliminates the requirement for sophisticated network infrastructure while still ensuring the flexibility necessary for extension and development of the network. The Internet Engineering Task Force (IETF) has standardised a set of protocols for IoT WSANs in order to make the integration of WSANs into existing information systems easier. The communication protocol stack is constructed on top of the IEEE 802.15.4 standard, which has been extensively used in WSAN installations [2], and uses IPv6 as the primary communication protocol. In order to achieve this, the group has defined 6LoWPAN [1, which is an adaptation layer that allows IPv6 packets to be transmitted on IEEE802.15.4 networks], as well as the IPv6 Routing Protocol for Low-Power and Lossy Networks, RPL [3, which is considered the standard routing solution for the Internet of Things [4]. The IEEE 802.15.4 and RPL specifications both contain a set of safeguards to protect communication security and network control operations from malicious activities [5], [6], the shared and open nature of the wireless medium renders WSANs inherently susceptible to a broad variety of security assaults [7].

The wormhole attack[8] is one of the most subtle of these attacks since it is both difficult to detect and difficult to resist. Wormhole attacks are conducted by hostile actors who build and control an out-of-band communication link between two remote nodes. Because of the ease with which this channel may be used, the routing provider is compelled to utilise it to forward the traffic. Therefore, the malicious actor has control over a potentially huge volume of communication, which he or she may eavesdrop on or delete entirely. When routing communications are encrypted and authenticated, it is also possible to launch a wormhole attack without having to acquire any cryptographic secrets from the nodes. Despite its significance, the wormhole assault has only been examined theoretically up to this point. Until date,no one has looked into the practical procedures that would be required to implement it on a WSAN. The following is the significance of this paper's contribution. •We provide an implementation of a wormhole that is capable of attacking an IEEE 802.15.4 WSAN, as well as a strategy for increasing the effect on the RPL routing protocol, in order to mitigate the risks (proxy acker technique). For proof of concept, we use our wormhole to attack a real WSAN and assess the effect of the assault on the network based on a variety of factors.

We discuss the numerous countermeasures that have been recommended in the literature, and we put one of them to the test using real-world data. We come to the conclusion that preventing or detecting a wormhole attack may be too costly for the average IoT WSAN, which is limited in resources. The

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4976-4983
https://publishoa.com
ISSN: 1309-3452

most convenient approach to prevent or detect further assaults, such as traffic eavesdropping and selective packet dropping, may be to use a centralised system. The remainder of the paper is arranged in the following manner. Similarly, in Section II, we discuss similar studies on RPL assaults and the effect evaluation of wormholes on the Internet. On the technical side, Section III discusses the IEEE 802.15.4 and RPL protocols and their implementation. Our wormhole implementation as well as the proxy acker approach are covered in full in Section IVof our paper. In Section V, we use our wormhole to attack a real WSAN, and we assess the effect of the assault based on a variety of criteria. Specifically, in Section VI, we explore the numerous countermeasures provided by the literature, test one of them with real-world tests, and conclude that the most simple strategy to combat a wormhole may be to prevent or detect future assaults. SectionVII is where we come to our findings.

Literature survey

Mamoona Humayun et al [1] proposed a ML based Hybrid RPL Protocol for Rank and Wormhole Attack Reduction. The goal of this research is to introduce RPL, its resilience to the two attacks, and the idea that ML techniques such as SVM can be used to develop a secure and improved version of RPL that can reduce both WSN-inherited and RPL-specific attacks in an RPL-based IoT network.

Charisma Samuel et al [2] considered Performance of a Wormhole Detection Method in RPL-Based 6LoWPAN Networks Using Round-Trip Times and Hop Counts. They developed and implemented a wormhole detection technique for 6LoWPAN using round-trip timings and hop counts in ContikiOS. This technique's efficiency has also been assessed in terms of power, CPU, memory, and communication overhead.

Fatima-tuz-Zahra et al [3] proposed a ML based Rank and Wormhole Attack Detection Framework. Using ML techniques, this study proposes a rank and wormhole attack detection system.

Minalini Goyal et al [4] recommended A Review of Wormhole Attack Intrusion Detection on the Internet of Things. The goal of this research is to investigate the present detection mechanism for detecting wormhole attacks in IoT-based networks. This document categorises and illustrates each process from a variety of perspectives.

Ruchi Mehta et al [5] suggested Securing the IoT Routing Protocol RPL against Wormhole and Grayhole Attacks using a trust-based mechanism. The suggested solution uses direct trust, which is computed based on node attributes, and indirect trust, which is computed based on nearby node opinions, to address Wormhole and Gray hole attacks in this study. The proposed technique is low-energy and does not incur significant network traffic overhead.

Proposed work:

Wormhole Attack is the attacker creates a place in the network to track the information from the network and get the confidential information from the users where a tunnel or wormhole link is created in between source and destination[14,15]. For these attacks a detection mechanism is represented so that during the occurrence of attack, it can detect the attack from avoiding the nodeto be in malicious state[16].

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4976-4983
https://publishoa.com
ISSN: 1309-3452

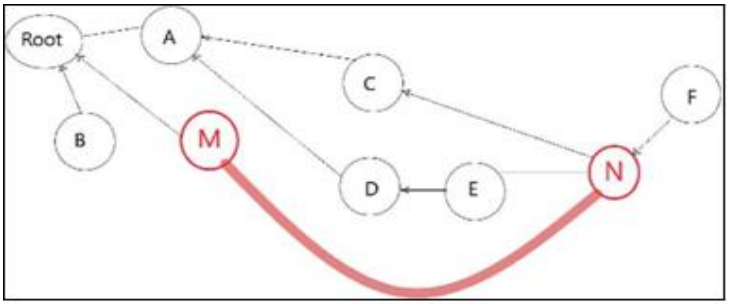

Fig-1: Wormhole attack in RP

Algorithm of the system:

1) Algorithm for wormhole attack detection on node side:

1) For each node N ,When it selects new parent send new parent info and RSSI value of packetreceived from parent to 6BR

2) If Ni receives the silent packet, then it will not forward any packet in threshold time ts, Ifismonitoring packet then It will start listening channel after ts and records RSSI value for that.

3) If Ni receives victim packet, then it will start sending fixed number of packets to another victimnode, If it is packet monitoring then Send RSSI value to 6BR and return to a normal state

4) If continuous packet loss found then broadcast the PathTrace packet, contains the list of nodes inthe path.

2) Algorithm for detection of the wormhole at the border router (6BR):

Let PL is list of nodes in path,
Let AL is list of nodes sent ACK on processing Path Trace packet Rmin and Rmax are the minimumand maximum range distance calculated from RSSI value

1) If Parent info received from node Ni then If actual distance between Ni and its parent is more thanthe range node Ni then

a)Calculate Rmin and Rmax form RSSI value

a) Find out suspect nodes in that range andneighbours of suspect nodes and expected RSSI value toreceive the packets.

b) Send silent packet to all nodesand monitoring packet to monitoring nodes Mi and victim packet to both parent and Node Ni

2) If receives the packet from monitoring node Mi then If only one packet is received then Suspect node is malicious node, generate alert. Else Choose the suspect node as malicious node whose monitoring node send the most approximate RSSI value.

Experimental results and discussion:

Used 4GB RAM and intel processor as hardware, Instant Contiki is a finished Contiki advancement condition running inside a Ubuntu Linux virtual machine (Ubuntu 14.04 LTS) that has every one of the compilers, improvement instruments and simulators expected to the examination.

Some of the metrics may be used as parameters to determine RPL's behaviour and performance. Energy consumption, Packet delivery rate, end-to-end latency, convergence time, and throughput are only a few examples of variables. Throughput, packet delivery ratio, and end-to-end latency were all considered in the research.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4976-4983
https://publishoa.com
ISSN: 1309-3452

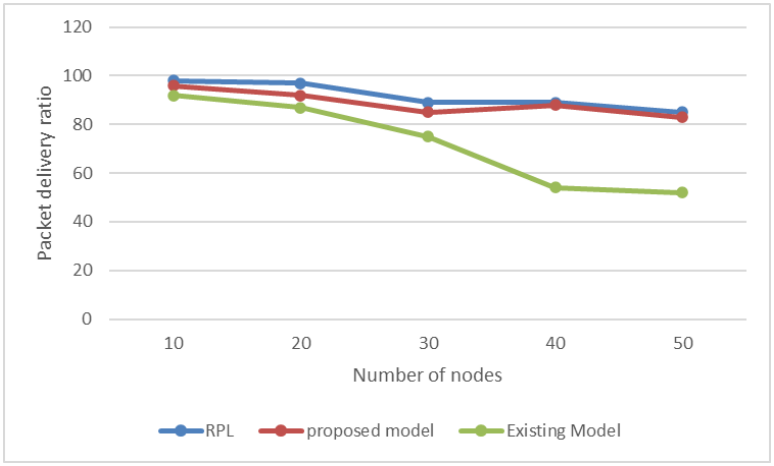

Fig-2: Packet Delivery Ratio

An illustration of a comparison between the proposed sinkhole attack detection model and existing approaches for detection of wormhole attacks in the RPL protocol may be seen on the right. It is a good indication of whether a routing protocol is in good working order or not to look at the packet delivery ratio. Having a high packet delivery ratio indicates that the routing system is performing at its best. Using the RPL protocol, we compared the impact of wormhole attacker nodes and detection techniques in this research. Conclusions According to the illustration, when compared to the present model, the recommended model outperforms it. But, in the previous model, the packet delivery ratio does not decrease dramatically as the number of nodes increases; however, when the number of sensor nodes increases, the packet delivery ratio decreases significantly as well.

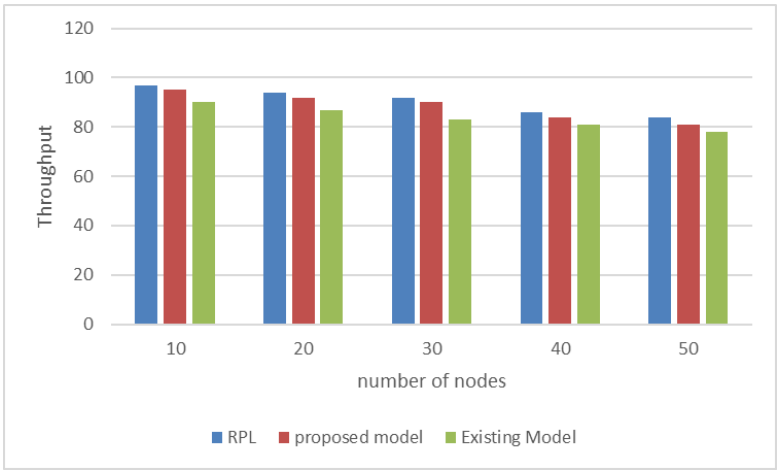

Fig-3: Throughput

Throughput is a useful measure of whether the routing protocol is in good working order for the time being. Being able to achieve a high throughput indicates that the routing system is in good working order. An illustration of the comparison between the proposed wormhole attack detection model and current methodologies for the detection of wormhole attacks in the RPL protocol, as well the proposed wormhole attack detection

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 4976-4983
https://publishoa.com
ISSN: 1309-3452

model, is shown in Figure 3. The influence of detecting measures in the RPL protocol was tested using data from wormhole attacker nodes, and the results were compared to the results of not having any detecting measures. According to the graphic, when the suggested model is compared to the current model, the recommended model outperforms the current model. As a result, while the throughput does not fall considerably as the number of nodes rises, the throughput of the present architecture does so much less so.

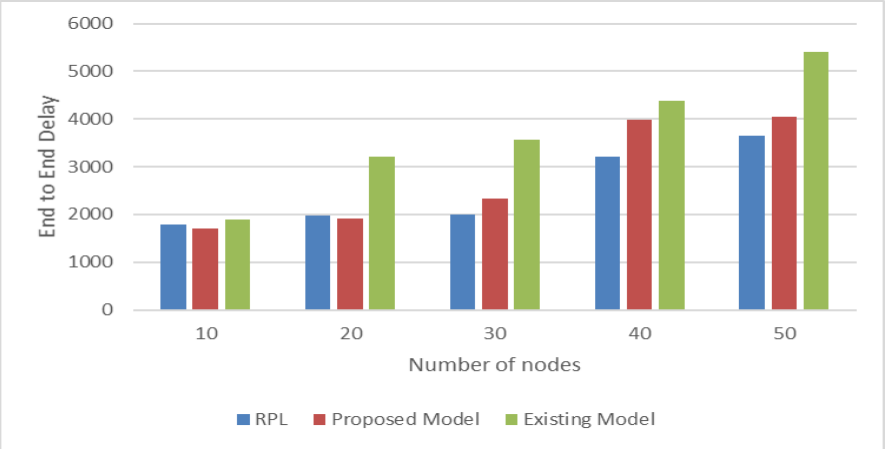

Fig-4: End to End Delay

Latency from source to destination is defined as the length of time it takes for a data packet to be delivered from one end of a network to the other and for the source to get an acknowledgement back from the other end. Figure 4 depicts a comparison of the end-to-end latency between the present and proposed methods of wormhole attack detection in the RPL protocol, as well as the results of the comparison. When comparing the current model to the recommended model, it is found that the existing model has a substantial amount of latency. Comparing the new technique to the current model, the new strategy results in a constant delay rather than an exponential growth in the amount of time taken.

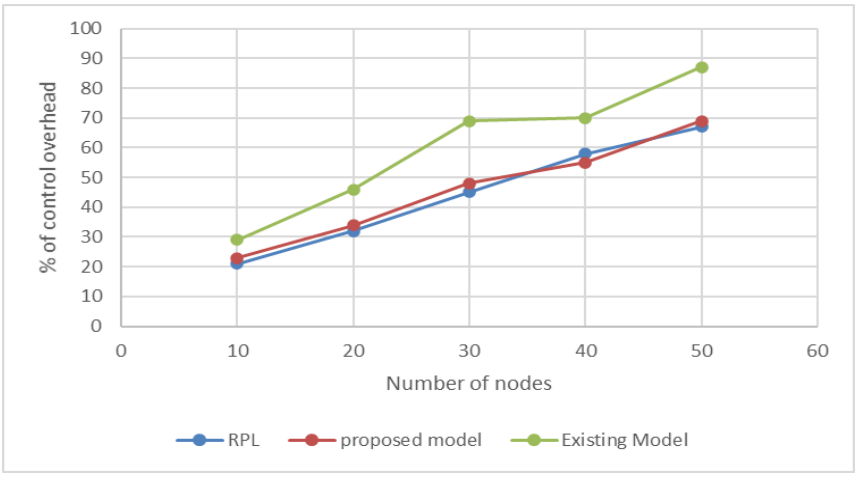

Fig-5: Percentage of control packet overhead

While generating the DODAG, the RPL incurs control overheads (DIO, DAO, and DIS), which are borne by the RPL. The nodes that use the trickle timer strategy interact with one another to ensure that the network continues to operate properly once it has been formed. These overheads have a negative impact on energy consumption, traffic congestion, and crashes, all of which are amplified. Figure 5 displays the control overhead of the present model, as well as the recommended wormhole attack detection models in the RPL protocol, in comparison to the previous model. Comparing the proposed technique to the current paradigm, the proposed approach has a lower control overhead.

Conclusion

Wormhole attack is one of the most serious assaults occurring at the 6LoWPAN layer of the RPL network of the Internet of Things. To yet, only a little amount of progress has been made in the detection of this assault. Using Contiki OS and the Cooja Simulator, we were able to build and construct an intrusion detection system that could identify wormhole attacks. Following the implementation of an IDS for the Wormhole Assault, it was discovered that the intended IDS had identified the attack with a success rate of around 90%. It is determined that the real positive detection rate for a small network size (N=8) is greater than the true positive detection rate for a larger network (N=16 or 24). The coefficient of correlation between the number of attacks carried out and the number of assaults identified is more than 90 percent for network sizes N=8 and 16. This figure is less than 90 percent for

N=24, and it has to be raised to meet the target. We are now working on increasing the rate ofpositive identification in networks with a larger number of nodes.

References

[1] Jhanjhi, N. Z., Brohi, S. N., Malik, N. A., & Humayun, M. (2020, October). Proposing a hybrid RPL protocol for rank and wormhole attack mitigation using machine learning. In 2020 2nd International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

[2] Samuel, C., Alvarez, B. M., Ribera, E. G., Ioulianou, P. P., &Vassilakis, V. G. (2020, July). Performance evaluation of a wormhole detection method using round-trip times and hop counts in RPL-based 6LoWPAN networks. In 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP) (pp. 1-6). IEEE.

[3] Jhanjhi, N. Z., Brohi, S. N., & Malik, N. A. (2019, December). Proposing a rank and wormhole attack detection framework using machine learning. In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) (pp. 1-9). IEEE.

[4] Goyal, M., & Dutta, M. (2018, December). Intrusion detection of wormhole attack in IoT: A review. In 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET) (pp. 1-5). IEEE.

[5] Mehta, R., & Parmar, M. M. (2018, April). Trust based mechanism for securing iot routing protocol rpl against wormhole &grayhole attacks. In 2018 3rd International Conference for Convergence in Technology (I2CT) (pp.

1-6). IEEE.

[6]Dr. T.PriyaRadhikaDevi "Android Application Forspontaneous Soilconstant Monitoring And Controlling Systemusing Raspberry Pi"Journal Of Critical Review Vol 7 Issue 16.

[7] Murali. D, Prasanna. S, Mathavan. V,Priyaradhikadevi. T" Linear Regression And Neural Networks Algorithm To Predicting The Real-Time Parameters Of Temperature And Humidity" Journal of Critical Review Vol 7 Issue 16