e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.327

Volume 8, Issue 2, February 2020

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Security Approach to Minimize Attacks in Low Power Networks

Anup W. Burange[1]
Department of Computer Science & Engineering
PRMIT&R, Badnera-444701
Maharashtra, India

Dr. V.M. Deshmukh[2]
Department of Computer Science & Engineering
PRMIT&R, Badnera-444701
Maharashtra, India

Abstract: The Internet of Things (IoT) is the network where physical devices, sensors, actuators and other different objects can communicate with each other without the need for human intervention. IoT consists of devices that have Low power and lossy networks (LLNs) which are featured by limited resources like memory, energy, processing power and bandwidth. These are connected with lossy links so they support low data rates. These features lead the system in unstable state. IETF designed new protocol for these devices called Routing protocol for low power and lossy networks (RPL). This protocol is also prone to number of attacks and does not support mobility of nodes. This paper deals with study of different types of attacks that are possible on RPL. The proposed method is an attack detection technique by using intrusion detection system that considers trust value of nodes.

Keywords: Trust, 6LBR.

I. Introduction

Internet of Things (IoT) is a fast-growing technology that has the capability to change the way human’s life at a great extent. It can be thought of as the revolution in Internet technology. The dynamic working environment related with the Internet of Things represents considerable impact to the attack surface and threat environment of the Internet and Internet-connected systems. IoT is diverse system consisting of various types of sensors nodes or devices with different kind of functionality at each layer. However, due to the limited address space of IPv4, objects in the IoT use IPv6 to accommodate space in Internet. Objects in the IoT can be devices with sensors, actuators, RFID’s etc [1]. IoT can be viewed as a mixture of heterogeneous networks that brings not only the same security challenges present in sensor networks, mobile telecommunications and the internet but also some peculiar and accentuated issues like, network privacy problems, authentication, access control and secure routing among these heterogeneous devices [2]. Routing and addressing are critical issues in IoT owing to the requirement of maintaining uniformity in the way packets are routed between source and destination between IoT devices traveling across varying network topologies. Making the process of routing secure enough in IoT is even more challenging [3]. Routing in IoT is more challenging because of constrained devices in network. IETF developed RPL for IoT routing RPL lets constrained devices, using a Low Power and Lossy Networks, to access the internet. Furthermore, the specification of designing RPL allows it to be very challenging and thus open to further improvement [4].

II. RPL Overview

Routing Protocol for Low Energy & Lossy Network (RPL) is a Distance Vector (DV) protocol developed by IETF. RPL constructs a Destination-Oriented Directed Acyclic Graph (DODAG) using one or many metrics. The DODAG structure is generated by considering the node attributes, link costs, and an objective function. Rank generation for every node on the DODAG is done by the objective function designed in RPL. RPL sorts the nodes as Destination-Oriented DAGs (DODAGs), the placement of sinks or the nodes which give a route to the Internet (i. e, gateways) behave as the DAGs root. A network might consist of one or more than one DODAG, that makes an RPL instance adapted by a unique ID, named RPL Instance ID. A network can control a group of RPL instances concurrently. These instances are naturally independent. A node is capable to connect to several RPL instances, but it should only relate to a single DODAG within every instance [5].

Hierarchical nature of RPL –based network topology makes self-organization of nodes based on the relationship of parent-to-child. Within a DODAG, RPL uses an Objective Function (OF) to select and optimize routes according to different metrics. Rank of node specifies the position of node with respect to sink node. RPL uses three types of control messages for establishing and maintaining the routing, which are DIO (DODAG Information Object) for setting and updating the topology; DAO (DODAG Destination Object) to propagate destination information upwards for route updating progress and DIS (DODAG Information Solicitation) for a new node to ask for topology information before joining the network. The DIO message includes all the routing information of a node such as Rank and Objective Function so that its neighbor can use to set up further route. On the other hand, the DAO and DIS messages are mainly used for the purpose of starting a topology set up or change process [6]. Route path selection is a key factor for RPL, RPL use the various routing metrics, route constraints and objective functions (OF) such as hop count, energy minimization and latency to compute the best route path. There are various attacks possible in RPL network which significantly impact the network resources and its performance

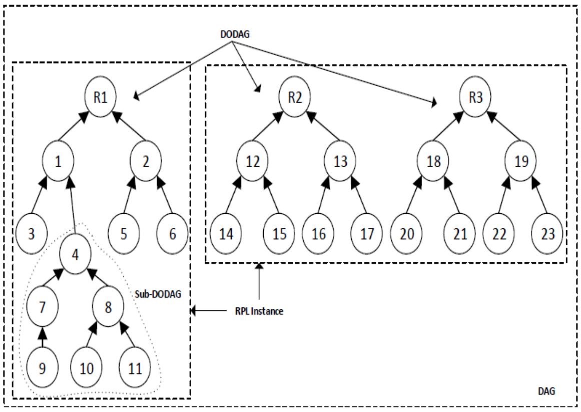

Fig 1 An example of a typical RPL-based IoT network [7].

A. Rpl Control Messages

There are 5 control messages, they form the spanning tree

- DODAG information object (DIO): This message is multicasted downwards. A node in a DODAG can multicast this message, which lets other nodes to recognize about it, things like whether the node is grounded or not, whether it storing or non-storing and it broadcasts other nodes “if they are interested to join” , please let me know.
- DODAG Information Solicitation (DIS): when no announcement is heard, and a node wants to join a DODAG it sends a control message, for that it wants to know if any DODAG exists. The message sends by it is like “Is there any DODAG?”
- DODAG Advertisement Object (DAO): It is a request send by a child to parent to root. This message allows the child to join to a DODAG.
- DAO-ACKNOWLEDGE: It is a response send by a root or parent to the child, this response can either be a “yes” or “no”.
- Consistency check: Deals with security and we need not to know much about it now.

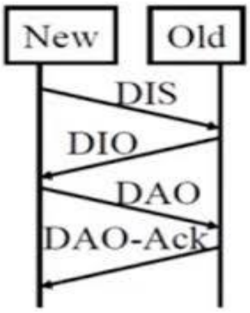

Fig. 2 RPL control messages [20].

B. RPL Attacks

There are various attacks possible in RPL network which significantly impact the network resources and its performance

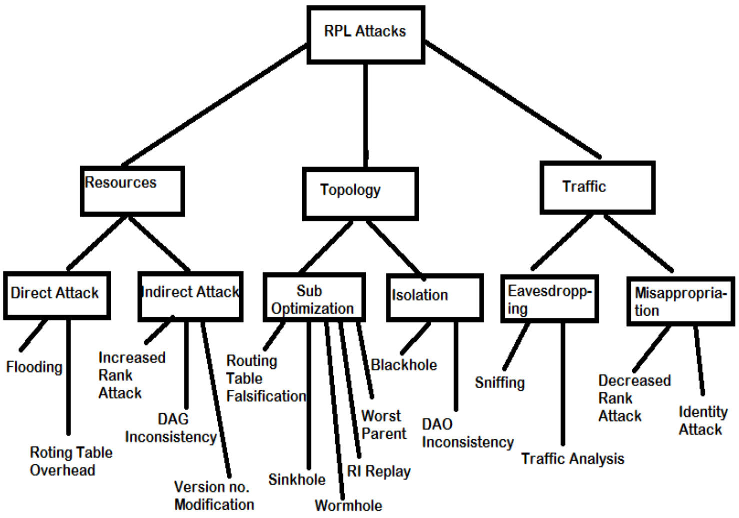

Fig. 3 Types of Attacks on RPL [11].

1. Sinkhole Attack: In this internal attack, attacker or compromised node advertises beneficial path to catch the attention of many close by nodes to route traffic through it. This attack disturbs the network topology and may become dangerous when combined with another attacks [7].

2. Version Number Modification Attack: This internal attack is caused due to changing version number (lower to higher) of a DODAG tree. When nodes obtain the new upper version number DIO message they initiate the creation of new DODAG tree. This results an un-optimized or discrepancy of network topology, increases control overhead and high packet loss [7].

3. Denial of Service Attack: Denial of service or Distributed denial of service attack is attempt to make resources unavailable to its legitimate user. In RPL this attack can be made by the IPv6 UDP packet flooding [7].

4. Wormhole Attack: In This attack, attacker node can create tunnel between the two attacker nodes and then by transmitting the selective traffic through it attempt to disturb the network topology and traffic flow [7].

TABLE 1. Attack Types

Attack	Effect on network/ topology	Techniques to counter	Remarks
Rank	Decrease packet delivery ratio, loop generations in network.	cryptographic techniques, Secure-RPL (SRPL) , RInA, VeRA, TRAIL , SVELTE	These techniques detect rank attack but energy usage is more. Detect for static network
Wormhole	Disrupt network topology & traffic flow	Location information & neighbor information, fuzzy logic approach, Hound Packet, merkle tree authentication, ML based	Uses minimum resources, high false positive rate & applicable for static network
Sinkhole	Malicious node falsely claims a lower rank in order to let its neighbors select this node as their parent.	IDS, Trust based, INTI- IDS	Trust based methods are used less resources. IDS have High false positive rate
Sybil	A malicious object may use different identities in the same network	K-mean clustering, location information,EAODV, ML based, Fine-grained physical channel information	To find broad range of Sybil attacks common strategy is needed.
Blackhole	A blackhole attack has been designed to drop silently all data packets that are meant to it by maliciously advertising itself as the shortest path to the destination it may lead to huge energy losses, congestion and network overhead issues	Hierarchical, trust based, multi hop, check agents and secure routing	Most of the techniques are designed for a specific purpose. Techniques should be develop considering the energy, processing and computation power of WSN nodes.
Selective forwarding	Forwarding selected packets by attacker to disturb routing paths is the primary goal of this attack.	Heartbeat protocol, End to end packet loss	Both techniques only detects the existence of attack
Version number	control overhead, delivery ratio, end to end delay	VeRA, IDS based on location information	Both techniques prevent the attack from occurring.

III. Intrusion Detection Systems

Intrusion detection system generates the alert when it detects any suspicious activity. There are mainly three types of IDS signature based, anomaly based and hybrid. Signature based IDS detects known attack types, anomaly based IDS are used to detect unknown attack pattern/ types. Hybrid IDS is combination of both signature and anomaly IDS. In anomaly based IDS different techniques like Fuzzy logic, Artificial neural network etc. can be used for detection or prediction of unknown patterns/ attacks. New IDS called trust based has been recently evolved which detect attacks on trust metric. Trust can be defined as relationship between the trustor and trustee. Trustworthiness of a node depends on node's behavior in network towards its neighbors. Trust value of a node is index that represents node's reputation. Trust evaluates the trustworthiness of a node and quality of services it provide to its neighbor. In addition reward and penalty can be applied to enforce trustworthy compliance of node [18]. Trust management does not include any complex cryptographic and hashing procedure so its suitable for resource constrained devices like in IoT. Trust management improves the traditional security systems by using trust system of evaluation to ensure the participation of trusted nodes [19].

TABLE 2. Different Intrusion Detection Systems

IDS	Detection	Architecture	Attack Types	Detection Performance
Khan et al. [8]	Anomaly based	Distributed	routing-specific attacks: sinkhole, selective forwarding and version number	Detection Rate= 50%
D. Summerville et al. [9]	Anomaly based	Distributed	Worm propagation, tunneling	Detection accuracy: 90%

Raza et Al [10]	Hybrid	Distributed	sinkhole and selective forwarding attacks	approx 80% for 30 nodes on avg.
A. Mayzaud, R. Badonnel, and I. Chrisment [11]	Specification based	Distributed	version number attacks	Detection accuracy: 81.97%
A.S. Chordia, S. Gupta [12]	Anomaly based	Centralised	DoS, Probe	Detection rate: 93.67%
Sedjelmaci et al. [13]	Hybrid	Distributed	DoS	Detection accuracy 92% for large number of nodes
V. Sivaraman, and R. Boreli [14]	Hybrid	Distributed	Masquareding	Accuracy: 94.25%,
Anhutan . Le, J. Loo, Y. Luo, and A. Lasebae [15]	Specification based	Hybrid	Rank, sinkhole and neighbour attacks	Detection accuracy: 80%
M. Surendar and A. Umamakeswari [16]	Specification based	Statistical probability	Sinkhole attacks	Improvement in QoS metrics over the existing INTI scheme.
N. Djedjig, D. Tandjaoui, and F. Medjek [17]	Trust Based	-	Internal and External RPL attacks	better performance in terms of detection accuracy, throughput, overhead and power consumption

Z. Khan and P. Herrmann designed trust management mechanism which collects the information about neighboring devices and their reputation. They proposed anomaly based intrusion detection is for detecting routing specific attack like sinkhole attack and version number attack.

D. Summerville, K. Zach, and Y. Chen presented a deep packet anomaly detection system involving feature selection conducted by pattern matching. It can be applied to either stateless or stateful configuration using sliding window operation which reduces the complexity.

S. Raza, Linus Wallgren , Thiemo Voigt presented SVELTE in contiki OS. SVELTE detects all malicious nodes that launch their implemented sinkhole and/or selective forwarding attacks. This IDS uses the feature of firewall. This technique has small overhead which is suitable for constrained devises which has limited capabilities.

A. Mayzaud, R. Badonnel, and I. Chrisment proposed a distributed system architecture for detecting the version number attacks in RPL-based networks and identifies malicious nodes.

Chordia and Gupta proposed an anomaly based IDS to reduce false alarm rates and increase the detection efficiency using data mining techniques. The proposed system monitor network traffic and uses techniques such as K-NN ,K-Means and Decision Table Majority Rule Based scheme.

H. Sedjelmaci, S. Senouci, and T. Taleb presented game theroretic technology to identify anomalies. They proposed lightweight anomaly based intrusion detection technique for IoT. It is combination of both signature based and anomaly based IDS but anomaly based detection activate only when unknown pattern appears.

V. Sivaraman, and R. Boreli propose a host based IDS using Software Defined Technology (SDN) for smart homes. The authors have defined three basic requirements for an efficient IDS for IoT i.e. unobtrusive approach, negligible overheads, and scalability. The detection can be performed using a choice of detection modules i.e. signature, anomaly or specification based techniques

A. Le, J. Loo, Y. Luo, and A. Lasebae proposed host based IDS using contiki os. IDS is able to perform detection based on information at node level and then transmit the data to some centralized system for further analysis. It performs the detection based on the information collected from individual nodes and does not consider the information from other nodes.

M. Surendar and A. Umamakeswari, they proposed probabilistic constraint based specification model to detect sinkhole attack in RPL network.

N. Djedjig, D. Tandjaoui, and F. Medjek proposed trust based intrusion detection system in which direct trust is calculated based on trustworthiness of direct neighbors and indirect trust is calculated based on the feedback received from neighbors. Average trust is calculated based on these two parameters to find parent node.

IV. Proposed Work

Security approach is proposed using trust management i.e trust based on traffic patterns, mobility and node's behavior as service provider to its neighboring nodes.

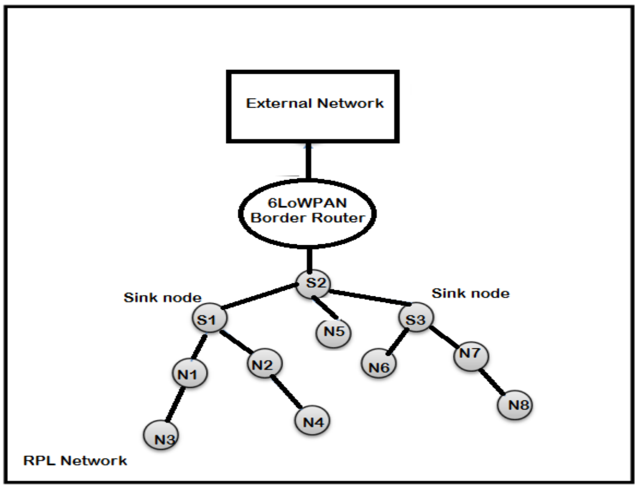

Fig 4. Proposed Framewaork

a) External attack: An approach for removing internal attacks and detection of malicious node based on analysis of behavior shown by the node can be used . We use network based intrusion detection system which will monitor all the traffic in the network and based on that it will create a trust model for the nodes. This module can be placed on sink nodes as well as on border router as most of the traffic passes through these nodes. Trust value generated by monitoring the traffic will be called as network trust.

b) Dynamic network: IoT devices can be either mobile or stationary which is attached to the local sink node. We consider the hybrid scenario in which one or more nodes can be static or dynamic (moving) so according to that parent selection objective function will be developed based on RSSI value. Previously some of has been done by different researchers but it consists of some pros and cons. We want to develop optimize objective function for parent selection considering frequent changes.

c) Internal attack: Trust based IDS is proposed which will consider the mobility also as trust parameter if any moving node send DIS message using new IPv6 address, node will verify RSSI value of other nodes etc. trustworthiness of mobile node will be analyzed. RPL does not have any technique to indentify the behavior of any node. Trust can be categorized as direct trust and indirect trust. Direct trust is of kind in which one has surety about genuineness of other whereas indirect trust refers to recommendations by other neighboring nodes. This module will be placed on all nodes to analyze the trust of neighboring nodes. Trust parameter and its location is used for selecting the best path towards sink node. Sink node maintains the history of all nodes & global sink node maintains the history of all sink nodes for countering attacks. This hybrid IDS is used to detect known attacks and this module can be placed on sink nodes.

V. Conclusion

6LoWPAN networks are vulnerable to different attacks due to its several limitations. In order to maintain security and normal operation of such network different attack detection and mitigation is important. Proposed light weight IDS system is build for resource constrained devices like in IoT. Mobility, Location information can make system more relevant for detection of wormhole and Sybil attacks. Traffic monitoring is used for detection of external attacks and malicious nodes. Trust based

IDS is used to counter internal attacks. Collectively we aimed to counter external and internal attacks using trust based distributed IDS considering mobility of nodes.

References

1. Pavan Pongle, Gurunath Chavan “Real Time Intrusion and Wormhole Attack Detection in Internet of Things” International Journal of Computer Applications (0975 - 8887) Volume 121 - No. 9, July 2015.
2. K Zhao, Lina Ge “.A survey on the internet of things security”.: Proceedings of the 9th International Conference on Computational Intelligence and Security (CIS). Pp 663–667.
3. Gubbi J, Buyya R, Marusic S, Palaniswami M. “Internet of Things (IoT): a vision, architectural elements ,and future directions.” Future Generation Computer System 2013;29:1645–60.
4. Winter, Lamaazi., “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks Low-Power.” RFC 6550, pp. 1–157
5. Ali Kadhum Idrees, Athraa J. H. Witwit “A comprehensive review for RPL Routing protocol in low power and lossy networks.”
6. Anhtuan Le, Jonathan Loo, Yuan Luo, Aboubaker Lasebae “The Impacts of Internal Threats towards Routing Protocol for Low power and lossy Network Performance” presented in IEEE conference
7. Ahmed Raoof, “Routing Attacks and Mitigation Methods for RPL-Based Internet of Things” published in IEEE Communications Surveys & Tutorials 2017.
8. Z. Khan and P. Herrmann, “Hive: Home automation system for intrusion detection,” in IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)., 2017.
9. D. Summerville, K. Zach, and Y. Chen, “Ultra-lightweight deep packet anomaly detection for internet of things devices,” in IEEE 34th International Performance Computing and Communications Conference (IPCCC), 2015.
10. S. Raza, L. Wallgren, and T. Voigt, “Svelte: Real-time intrusion detection in the internet of things,” AdHoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013.
11. A. Mayzaud, R. Badonnel, and I. Chrisment, “A distributed monitoring strategy for detecting version number attacks in rpl-based networks,” in IEEE Transactions on Network and Service Management, ser. 2, vol. 14, 2017, pp. 472–486.
12. A. S. Chordia and S. Gupta, “An effective model for anomaly ids to improve the efficiency,” in International Conference on Green Computing and Internet of Things (ICGCIoT), 2015.
13. Hichem. Sedjelmaci, S. Senouci, and T. Taleb, “An accurate security game for low- resource iot devices,” in IEEE Transactions on Vehicular Technology, 2017.
14. M. Nobakht, V. Sivaraman, and R. Boreli, “A host-based intrusion detection and mitigation framework for smart home iot using openflow,” in 11th International Conference on Availability, Reliability and Security (ARES), 2016.
15. Anhutan . Le, J. Loo, Y. Luo, and A. Lasebae, “Specification-based ids for securing rpl from topology attacks,” in IFIP Wireless Days (WD), 2011.
16. M. Surendar and A. Umamakeswari, "InDReS: An Intrusion Detection and response system for Internet of Things with 6LoWPAN," in 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp. 1903-1908.
17. N. Djedjig, D. Tandjaoui, and F. Medjek, "Trust-based RPL for the Internet of Things," in 2015 IEEE Symposium on Computers and Communication (ISCC), 2015, pp. 962-967.
18. F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," Transactions on Emerging Telecommunications Technologies, vol. 26, pp. 107-130, 2015.
19. David Airehrour, Jairo A. Gutierrez, Sayan Kumar Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things” published in future generation computer systems 2018.
20. Akif Mufti “What is RPL and how to simulate it in cooja?”,Published on website.