TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 4, August 2020, pp. 1849~1856
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i4.15768

RPL routing protocol performance under sinkhole and selective forwarding attack: experimental and simulated evaluation

Bimal H. Patel, Parth Shah
Department of Information Technology, CSPIT, Charotar University of Science and Technology, India

Article Info

Article history:

Received Feb 10, 2020
Revised Mar 21, 2020
Accepted Apr 10, 2020

Keywords:

6LoWPAN
Contiki
Cooja
Internet of things (IoT)
RPL
Selective forwarding attack
Sinkhole attack

ABSTRACT

To make possible dream of connecting 30 billion smart devices assessable from anywhere, anytime and to fuel the engine growth of internet of things (IoT) both in terms of physical and virtual things, internet engineering task force (IETF) came up with a concept of 6LoWPAN possessing characteristics like low power, bandwidth and cost. To bridge the routing gap and to collaborate between low power private area network and the outside world, IETF ROLL group proposed IPv6 based lightweight standard RPL (routing protocol for low power and lossy networks). Due to large chunks of random data generated on daily basis security either externally or internally always remain bigger threat which may lead to devastation and eventually degrades the quality of service parameters affecting network resources. This paper evaluates and compare the effect of internal attacks like sinkhole and selective forwarding attacks on routing protocol for low power and lossy network topology. Widely known IoT operating system Contiki and Cooja as the simulator are used to analyse different consequences on low power and lossy network.

Corresponding Author:

Bimal H. Patel,
Department of Information Technology, CSPIT,
Charotar University of Science and Technology,
Changa 388421, India.
Email: bimalpatel.it@charusat.ac.in

1. INTRODUCTION

Ever since the emergence of the term Internet of things (IoT) proposed by Kevin Aston in the late 1990's, it has completely change era from analog to digitized world [1]. When IPv6 was introduced in 2011 momentum gained in terms of smartness connecting physical and virtual thing with the help of embedded and sensor network technology. Smartness and intelligence are now widespread in the industry by way of Industrial IoT, agriculture, smart home, healthcare, logistics etc. making life smoother and easier to live and enjoy with fullest [2]. To make possible dream of 30 billion smart devices connected as predicted by Gartner report [3], IETF (Internet Engineering Task Force) came with the concept of 6LoWPAN (IPv6 over low power wireless private area network) [4].Since standard routing protocol like AODV, DSR and OLSR for wireless networks are not fitted for LLN due to its higher energy usage, repair in case of network failure and lack of consideration of node/link properties for establishment of routes, IETF ROLL working group comes up with RFC 6550 proposed standard RPL [5] which is IPv6 based lightweight, distance vector, loop-free, proactive source routing protocol applied for highly adaptive and dynamically changing network conditions with low power and lossy constraints personal area network. It fills the routing gap between LoWPAN and on other side IP world. As more and more devices are connected, larger chunks of data will be

generated on network leading to security concerns and greater possibility of network attacks externally as well as internally. The aim of this paper is to evaluate performance of RPL protocol considering power consumption as quality of service parameter under sinkhole and selective forwarding networking attacks.

In section 2 state of art related to RPL is mentioned which section 3 discuss two network attacks and its implementation flow scenario in contiki operating system and Cooja as simulator support. Section 4 will give idea about simulation configuration parameters and various scenario details. Section 5 discusses result analysis in terms of power consumption for all three scenarios. Section 6 provides conclusion and throw some light on future directions.

2. RPL (ROUTING PROTOCOL FOR LOW POWER AND LOSSY NETWORKS) IN LITERATURE

RPL support mesh and hierarchical topology by considering routing through backup siblings/parent when needed based on concept of "DODAG (Destination oriented directed acyclic graph)".Acyclic property helps to achieve loop free networks in graph.RPL supports all three traffic types i.e. P2MP (point to multipoint) in terms of downward routes, MP2P (multipoint to point) using upward routes towards LBR and P2P (point to point) for both transmission type like unicast and multicast.

RPL categorized nodes in three ways. 1) LBR (Low power and lossy border router) also called DODAG root or sink node as shown in Figure 1 which acts as gateway between internet and LLN networks. It has a property to generate new DODAG or its different versions. 2) Routers which is used for forwarding and generating traffic. 3) Host also called leaf node or end device (indicated by 3 and 4 in DODAG1 and 3 in DODAG2) which is capable of only generating traffic. As shown in Figure 1 there are two DODAG (DODAG1, DODAG2) which combines as one RPL instance uniquely identified by RPLInstanceID. Nodes may belong to multiple instances but should remain in one DODAG at a time within individual instance [6]. Each node in DODAG is differentiated with rank which defines nodes individual position and path to its LBR. Rank values increases when you move in downward direction form sink node. Rank is computed based on objective function (OF (0) and MRHOF) [7-9].

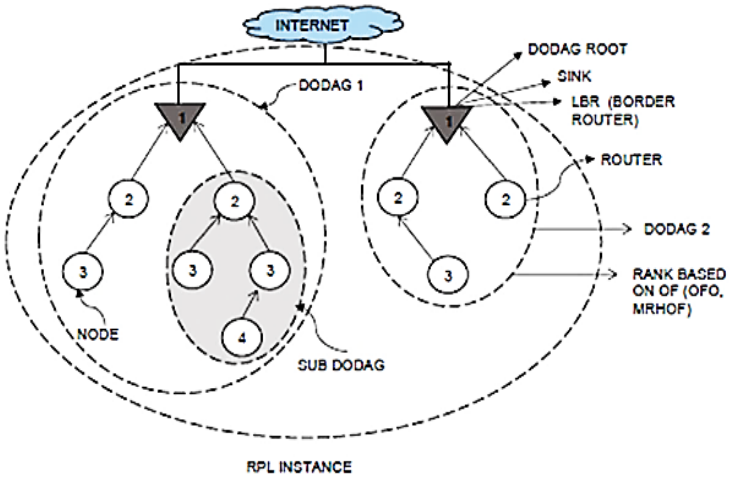


Figure 1. RPL concepts/terminology

2.1. RPL DODAG construction

It supports two route formation.MP2P traffic is supported using upward routes with the help of DIO and DIS messages [10] for both grounded and floating node. P2MP and P2P traffic is supported using downward routes with the help of DAO message. It carries out both route formation with the help of neighbor discovery protocol which helps in local repair internally [11].

2.1.1. Upward route

Grounded node acting as LBR or sink node broadcast DIO which contains necessary information like RPLInstanceID, objective function (OF (0) or MRHOF), version, trickle timer [12] information and other parameters required for calculating rank to its neighbours. If the node willing to join DODAG receive DIO message for first time it adds its address to parent list and compute rank as per prescribed objective

function and then multicast updated DIO message to others. If a node which is already part of DODAG receives DIO it discards or process it by analysing mentioned criteria. Based on criteria if node's new rank is less than old rank it changes it rank and updates its information to avoid loops else maintain its current position in DODAG [13, 14]. If floating node wants to join DODAG it multicast DIS message to nearer nodes. After receiving DIS message one of the grounded nodes send unicast DIO message back to floating node which select appropriate neighbor or preferred parent to join DODAG [15].

2.1.2. Downward route

P2MP and P2P traffic is supported by downward route with the help of DAO control message. RPL uses two modes of operation for maintaining downward routes; (a) Storing mode in which every router node maintains routing information; (b) Non-storing mode in which only sink node will have routing information and acts as source node to send traffic information to other nodes [16]. RPL provides both local and global recovery schemes. If there is any link failure between two nodes or loop is generated it performs local repair with the help of back up parent, rank and neighbor discovery protocol. Since by rule every child will have higher rank compare to its parent it will never form loop and count to infinity problem will not occur. Though local repair will not lead to optimal path and results in terms of quality of parameters global repair is required by incrementing DODAG version number and whole DODAG is constructed with no concern to previous version and new version will have optimal path for reaching sink node with the help of rank as parameter by considering various objective functions.

3. ROUTING ATTACKS AGAINST RPL NETWORKS

RPL routing protocol for 6LoWPAN due to its properties like limited processing power, changing network topology in terms of DODAG, link failures and mobility are prone to various network attacks. Broadly attacks can be classified as external attack effected by internet (example brute force attack and malware attack) and internal attacks due to wireless sensor networks [17, 18]. Again, internal attacks on overall network can be categorized as attacks targeting exhaustion of networks, attacks targeting RPL network topology and attacks against network traffic. In this paper, we will focus on the two routing attacks sinkhole attack and selective forwarding attack and in further section we will evaluate it effect on power consumption by comparing it with normal scenario.

3.1. Sinkhole attack

In sinkhole attack malicious node by artificially changing rank somewhat higher than border router deceives legitimate nodes to get attacked towards itself claiming better path and link availability [18]. As shown in below Figure 2 left hand side shows normal scenario where node 2 and 3 can be reached directly to sink node/border router but when node 6 advertise its rank lower artificially than nodes which are in vicinity will get attracted towards it.All nodes 2, 3,5,7,9 and 10 will get attracted towards malicious node 6 which is shown in right hand side of Figure 2. This attack is more devastating and cause larger network problems when it is combined with other attacks [19].

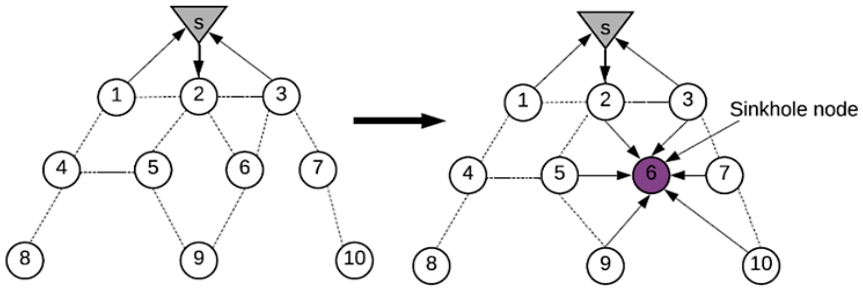


Figure 2. Normal to Sinkhole attack scenario

3.2. Selective forwarding attack

As name suggest this attack will forward control packets of RPL and drop data packets. Selective forward attack will work in tandem with sinkhole attack and cause severe consequences to network by attracting nodes and disrupting routing routes [18]. As shown in Figure 2 node 6 after attracting nearby nodes either drops control packets or data packets and will not forward to legitimate node or to border router [19]. Overall flowchart describing implementation scenario is shown in below Figure 3. Here we are going to

compare normal case and by button click event malicious behavior is activated and finally in terms power consumption both scenarios is compared [20].

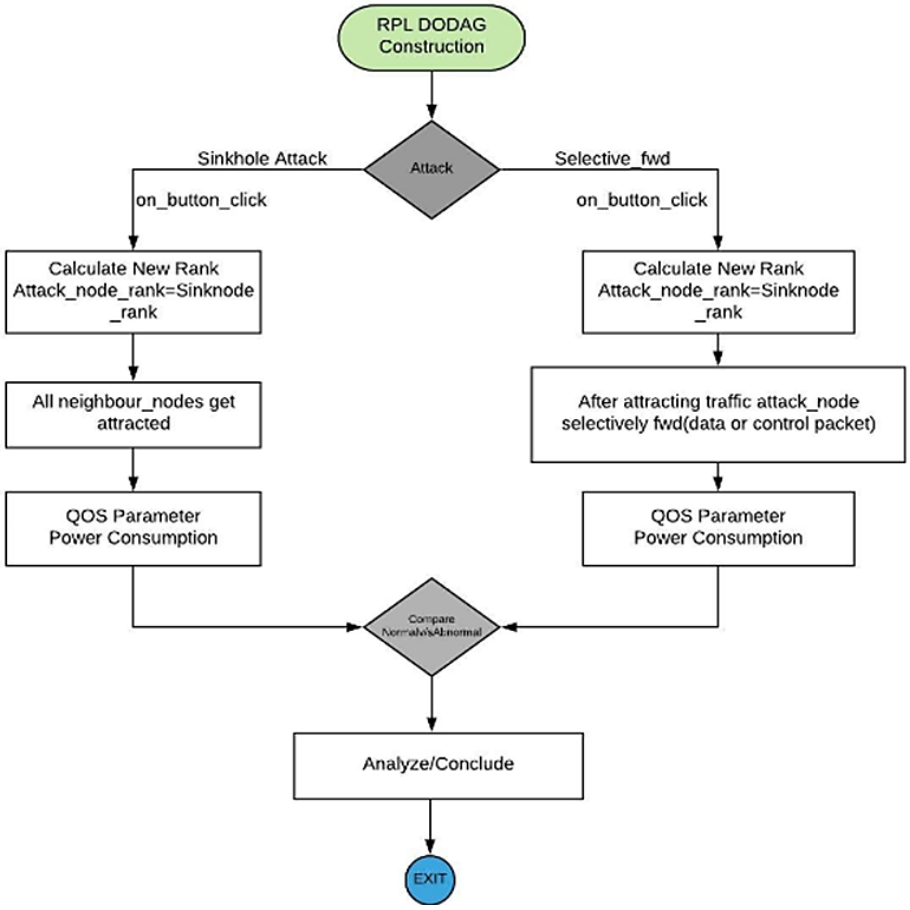


Figure 3. Implementation scenario of RPL attacks

4. SIMULATION ENVIRONMENT

The performance of RPL protocol has been evaluated and analyzed under normal [21-23] and attack scenario (Sinkhole and Selective forwarding attacks) with the help of widely used IoT operating system Contiki [24] while simulation support is provided by Cooja [25]. Various configuration parameters considered to carry out simulation is shown in Table 1.

Table 1. Configuration parameters

Parameters	Values
OS	Contiki OS3.0
Mote Type	Z1 mote
Number of Nodes (attack Nodes)	5nodes(1attack),10nodes(2attack),20nodes(3attack)
Radio Medium Model	Unit Disk Graph Medium (UDGM): Distance Loss
Nodes Transmisson Range	30-50m
Nodes Interference Range	70-100m
Tx/Rx Ratio	100/50
DIO Min	12
DIO Doublings	8
RDC Chanel Check Rate	16
MAC Layer	IEEE 802.15.4
Duty Cycle	nullRDC
Network protocol	ContikiRPL
Objective Function	MRHOF
Simulation Time	Scenario1:45 min, Scenario 2:30 min, Scenario 3:20 min

To get meaningful results three different scenarios is considered, such as;

a. Scenario 1

As shown in Figure 4 5 Z1 motes are considered out of which 1 mote will act as sink/border mote, 1 mote will act as attacking mote and rest 3 will behave normally.

b. Scenario 2

Here we have considered 10 motes out of which 2 motes are behaving abnormally. Figure 5 (a) and Figure 5 (b) gives us idea about what are the other motes in range of these attacking motes 9 and 10 which are getting affected.

c. Scenario 3

To get accurate effect of power consumption on various motes due to attack scenario 20 motes are considered out of which 3 are misbehaving. Figures 6 (a), (b) and (c) gives information about motes which are getting affected in terms of power due to attacking motes 18,19 and 20.

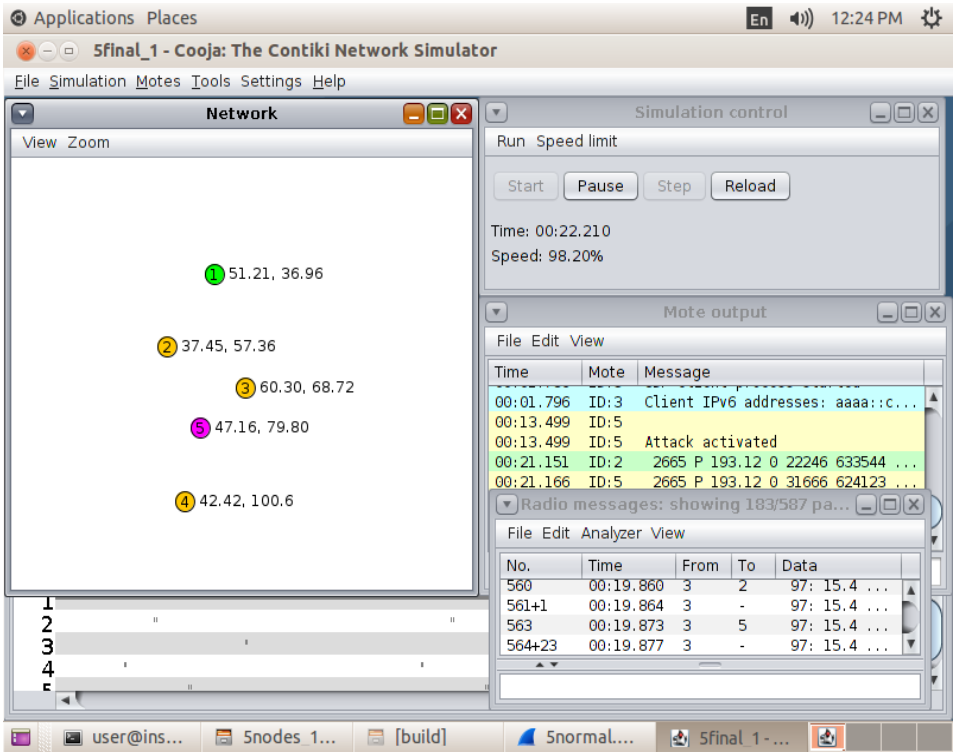
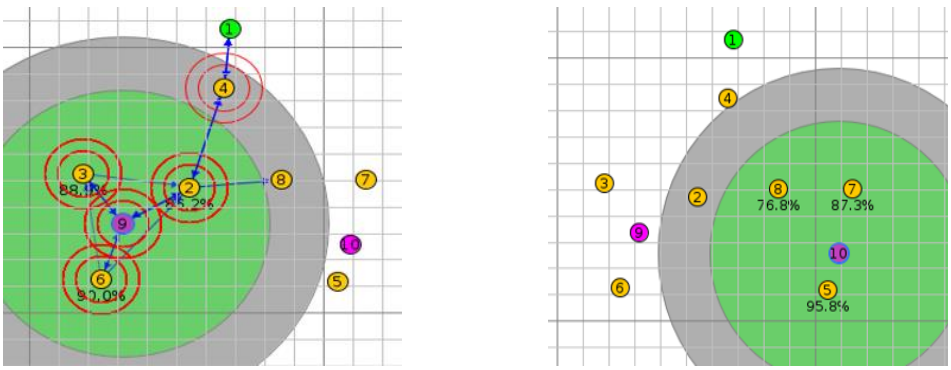
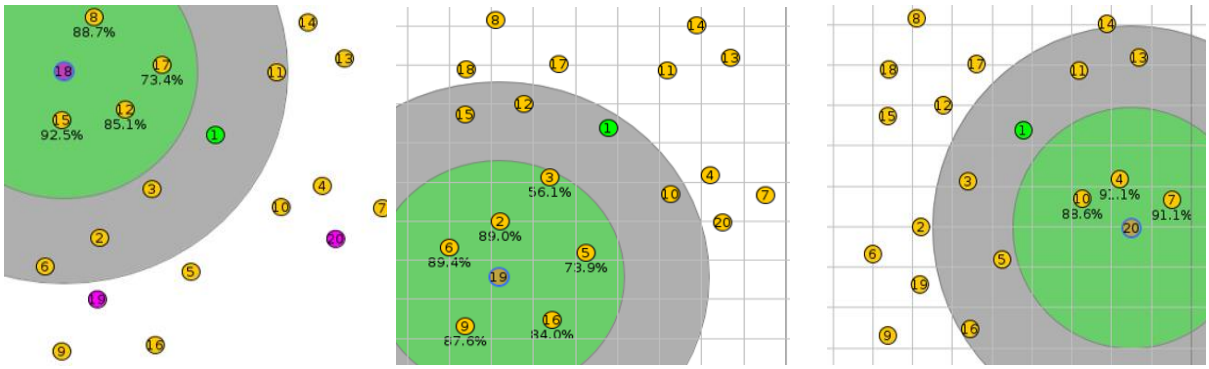


Figure 4. Scenario 1 (5motes with 1 mote as malicious)



(a) (b)

Figure 5. Scenario 2 (10 motes with 2 malicious behavior); (a) mote 9 range and (b) mote 10 range



(a) (b) (c)

Figure 6. Scenario 3 (20motes with 3 malicious behaviour);
(a) mote 18 range, (b) mote 19 range and (c) mote 20 range

5. RESULT AND DISCUSSION

In this section we investigate and compare normal and malicious behavior of all three scenarios taking into account power consumption of motes as quality of service parameter. The formula for calculating power and energy is described in (1) which takes into consideration approximate current consumption of Z1 motes circuits [26].

$$\text{Energy Usage (mJ)(Z1 mote)} = \frac{((17.4\ \text{mA} * \text{transmit} + 18.8\ \text{mA} * \text{listen} + 0.426\ \text{mA} * \text{CPU} + 0.02 * \text{LPM}) * 3\text{V})}{4096 * 8}$$

$$\text{Power Consumption (mW)} = \frac{\text{Energy Usage (mJ)}}{\text{Time(s)}} \quad (1)$$

For scenario 1 as you can see from Figure 4 that 2 and 3 are neighboring nodes which get affected due to mote 5 acting as attack node (sinkhole and selective forwarding). Power consumption of node 2 and 3 is increased compared to normal scenario is shown in Figure 7. In terms of percentage node 5 power consumption is drained more compare to normal case since all traffic gets attracted.

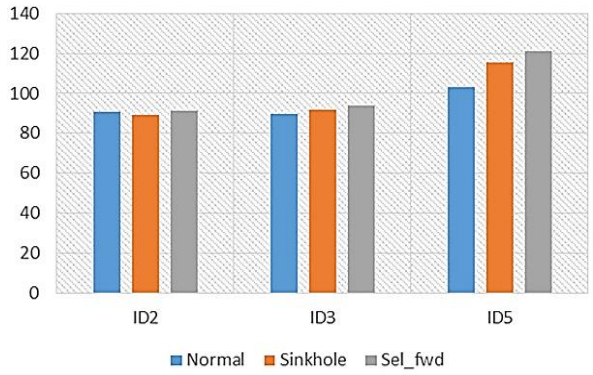


Figure 7. Node 5 attack scenario

For scenario 2 as you can see from Figure 5 (a) that 2 and 3 are neighboring nodes which get affected due to mote 9 acting as attack node (sinkhole and selective forwarding). Power consumption of node 2 and 3 is increased compared to normal scenario is shown in Figure 8 (a). Node 2 power is consumed more since it is nearer to sink node also. From Figure 8 (b) it shows that power consumption of node 8 and 7 is increased compared to normal scenario due to effect of attack on mote 10. In terms of percentage mode 9 and 10 power consumption is more compare to normal case since all traffic gets attracted.

For scenario 3 we have tried to cover bigger picture by considering 20 motes as you can see from Figure 6 (a) that 8,12,15 and17 are neighboring nodes which get affected due to mote 18 acting as attack

node (sinkhole and selective forwarding). Power consumption of node 8, 12, 15 and 17 is increased compared to normal scenario is shown in Figure 9 (b). Similarly, power consumption effect of neighboring nodes due to attack of mote 19 and 20 is shown in Figures 9 (a) and (c). It can be noted that effect of power on attack motes due to sinkhole attack and select forwarding which is far from sink node is almost same (18 and 19 mote). The motes which are located below attack node shows varying result since they are not affected much. As we can see from Figure 9 (c) mote 16 which is in vicinity still is not affected much due to attack effect on mote 19.

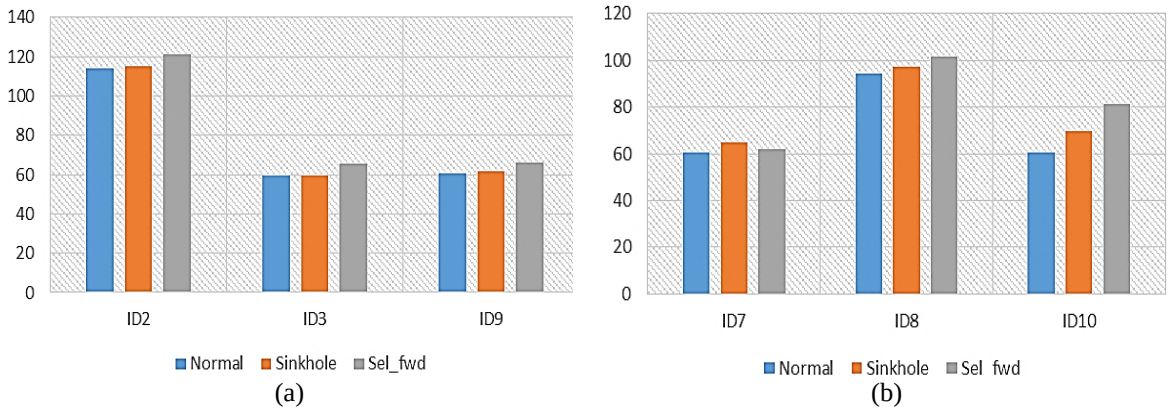


Figure 8. Effect of Power consumption on other motes due to attack motes;
(a) mote 9 attack scenario and (b) mote 10 attack scenario

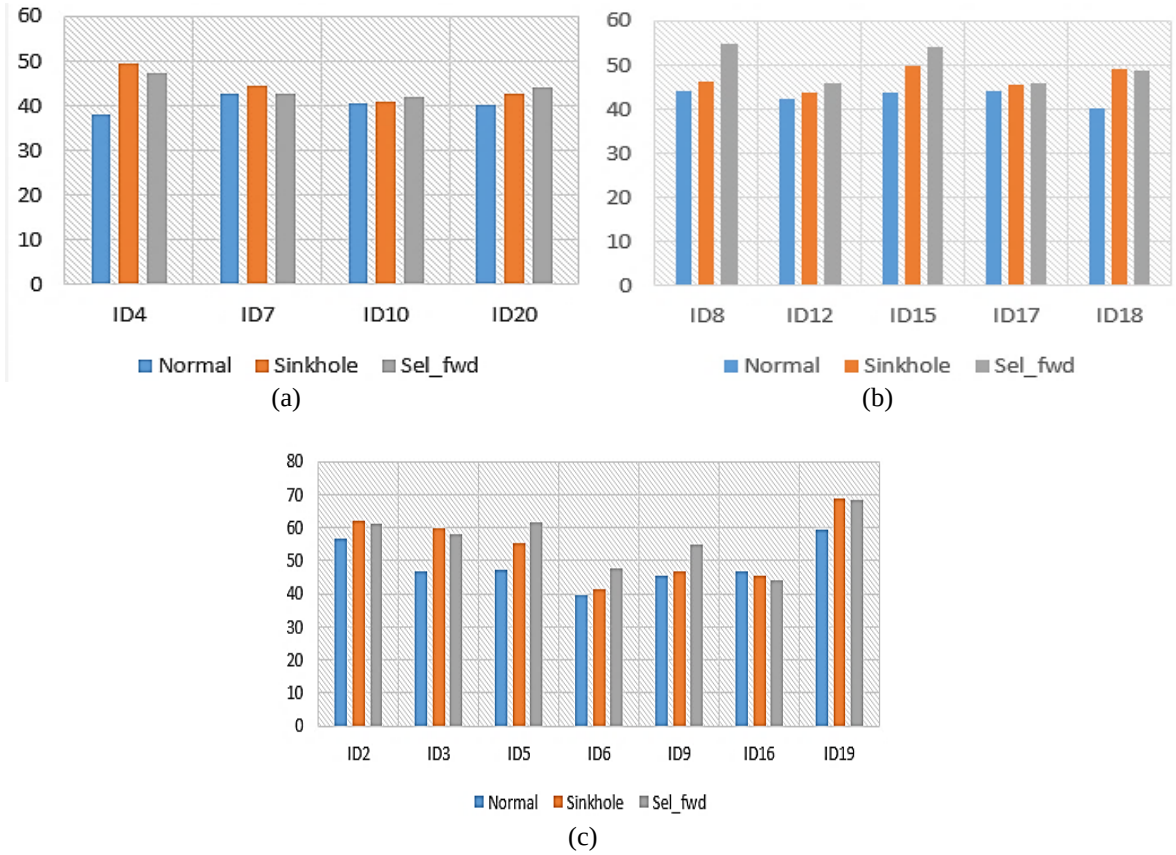


Figure 9. Effect of power consumption on vicinity motes due to attack motes; (a) Mote 20 attack scenario, (b) Mote 18 attack scenario and (c) Mote 19 attack scenario

6. CONCLUSION AND FUTURE WORK

This paper compares normal and attack scenario using three different experiments. As we can see from scenario 1, 2 and 3 that motes which are in vicinity and higher rank than attacking motes get affected most in terms of power consumption while motes which are having already lower rank and choosing attacking motes as parent are not affected much in both normal as well as abnormal scenario. We can also conclude that power consumption of attacking motes is much more than motes when behaved normally. In future same attacks can be compared with other quality of service parameters like PRR (Packet Reception Ratio) and throughput along with packet delivery fraction. Sinkhole and Selective forwarding attacks can be combined with wormhole attack which may show devastating effect on network resources.

REFERENCES

[1] Atzori L., Iera A., Morabito G., "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp 2787-805, 2010.
[2] Gubbi J., Buyya R., Marusic S.., Palaniswami M., "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645-1660, 2013.
[3] Gartner, "Newsroom". [Online]. Available: https://www.gartner.com/newsroom/id/2636073.
[4] Kushalnagar N., Montenegro G., Schumacher C., "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals," 2007. [Online]. Available: https://tools.ietf.org/html/rfc4919
[5] Winter T., Thubert P., Brandt A., Hui J. W., Kelsey R., "RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," 2012. [Online]. Available: https://tools. ietf. org/html/rfc6550.
[6] Gaddour O., Koubâa A., "RPL in a nutshell: A survey," *Computer Networks*, vol. 56, no. 14, pp. 3163-3178, 2012.
[7] Thubert P., "Objective function zero for the routing protocol for low-power and lossy networks (RPL)," 2012. [Online]. Available: https://tools.ietf.org/html/rfc6552.
[8] Gnawali O., Levis P., "RFC 6719: The Minimum Rank with Hysteresis Objective Function," *Internet Engineering Task Force (IETF)*, 2012.
[9] Vasseur J., P., Kim M., Pister K., Dejean N., Barthel D., "RFC 6551: Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks," *Internet Engineering Task Force (IETF)*, 2012.
[10] Tsvetkov T., Klein A., "RPL: IPv6 routing protocol for low power and lossy networks," *Network*, 2011.
[11] Iova O., Picco P., Istomin T., Kiraly C., "RPL: The Routing Standard for the Internet of Things... Or Is It?," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 16-22, 2016.
[12] Levis P., Clausen T., Hui J., Gnawali O. J. Ko, "The Trickle Algorithm. RFC 6206," 2011. [Online]. Available: https://datatracker.ietf.org/doc/rfc6206/
[13] Lamaazi H., Benamar N., Jara A. J., "Study of the Impact of Designed Objective Function on the RPL-Based Routing Protocol," *Advances in Ubiquitous Networking*, pp. 67-80, 2017.
[14] Tripathi J., De Oliveira J. C., Vasseur J. P., "Proactive versus reactive routing in low power and lossy networks: Performance analysis and scalability improvements," *Ad Hoc Networks*, vol. 23, pp. 121-44, 2014.
[15] Tang W., Ma X., Huang J., Wei J., "Toward improved RPL: A congestion avoidance multipath routing protocol with time factor for wireless sensor networks," *Journal of Sensors*, vol. 2016, pp. 11, 2016.
[16] Ishaq I., Carels D., Teklemariam G. K., Hoebeke J.., Abeele F. V., Poorter E. D., Moerman I., Demeester P., "IETF standardization in the field of the internet of things (IoT): a survey," *Journal of Sensor and Actuator Networks*, vol. 2, no. 2, pp. 235-87, 2013.
[17] Mayzaud A., Badonnel R., Chrisment I., "A Taxonomy of Attacks in RPL-based Internet of Things," *International Journal of Network Security*, vol. 8, no. 3, pp. 459-73, 2016.
[18] Le A., Loo J., Lasebae A., Aiash M., Luo Y., "6lowpan: a study on qos security threats and countermeasures using intrusion detection system approach," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1189-212, 2012.
[19] Wallgren L., Raza S., Voigt T., "Routing Attacks and Countermeasures in the RPL-based Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, pp. 1-11, 2013.
[20] Verma A., Ranga V., "Analysis of Routing Attacks on RPL based 6LoWPAN Networks," *International Journal of Grid and Distributed Computing*, vol. 11, no. 8, pp. 43-56, 2018.
[21] Zikria Y. B., Afzal M. K., Ishmanov F., Kim S. W., Yu H., "A survey on routing protocols supported by the Contiki Internet of things operating system," *Future Generation Computer Systems*, vol. 82, pp. 200-19, 2018.
[22] Mohamed B., Mohamed F., "QoS routing RPL for low power and lossy networks," *International Journal of Distributed Sensor Networks*, vol. 2015, no. 2, pp. 1-10, 2015.
[23] Nygaard F., "Intrusion Detection System in IoT," Master's Thesis, NTNU.
[24] Dunkels A., Gronvall B., Voigt T., "Contiki-a lightweight and flexible operating system for tiny networked sensors," *29th annual IEEE international conference on local computer networks*, 2004.
[25] Osterlind F., Dunkels A., Eriksson J., Finne N., Voigt T., "Cross-level sensor network simulation with cooja," *Proceedings 2006 31st IEEE Conference on Local Computer Networks*, 2006.
[26] Zolertia, "Z1 Datasheet," 2010. [Online]. Available: http://zolertia.sourceforge.net/wiki/images/e/e8/Z1_RevC_Datasheet.pdf