WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Impact of Selective Forwarding Attacks on the Performance of RPL Routing Protocol in the Internet of Things

Haitham Y. Adarbah[1] and Shakeel Ahmad[2]

[1]Gulf College, Oman, Haitham.Adarbah@gulfcollege.edu.om
[2]Solent University UK, Shakeel.Ahmad@solent.ac.uk

ABSTRACT.

The huge amount of data acquisition in the IoT (Internet of Things) systems makes data transportation and routing a massive challenge. One of the common routing protocols in IoT networks is RPL (Routing Protocol for Low-power and Lossy Networks), but it is prone to a number of attacks. This paper presents a thorough analysis of the effect of selective forwarding attacks on the performance of RPL routing protocol in the IoT. The main aim of this research is to measure and analyse the impact of selective forwarding attacks in IoT systems quantitatively and discuss the qualitative aspects of selective forwarding attacks that could provide stimulating grounds for future development to protect RPL from selective forwarding attacks. This work uses Cooja Simulator to implement the network scenario and simulate the selective forwarding attack for a varying number of network nodes and attacker nodes. The effects of selective forwarding have been measured on the system performance in terms of packet delivery ratio and end-to-end delay. The results show that having only 6% attacker nodes, the packet delivery ratio drops to 62% and end-to-end delay decreases by 19.04%.

Keywords: IoT, RPL, Selective Forwarding attack, RPL

1.Introduction

The Internet of Things (IoT) is made by integrating billions of things and smart objects. These IoT things are usually battery-powered nodes that are wirelessly connected and deployed in a mesh topology. As a result, these devices typically constrained with limited power, memory, and processing resources. The IoT network generally is optimized for energy-saving and operates under a variety of such working constraints.

The core of the IoT protocol stack used for communication between these low-power devices is Low-power Lossy Networks (LLNs). In most of the application scenarios, the nodes in LLNs operate independently and are unsupervised, causing a variety of attacks. To protect LLNs against these attacks, the ROLL working group at Internet Engineering Task Force (IEFT) has designed the Routing Protocol for Low-power Lossy Networks (LLNs) (RPL) [1].

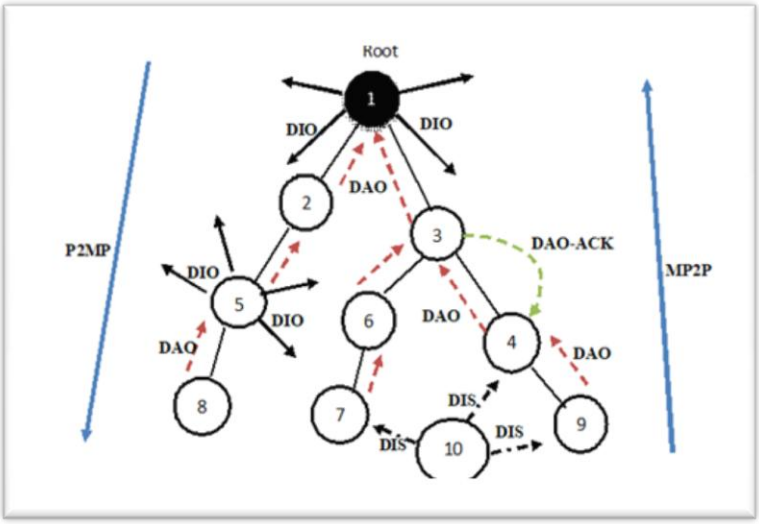


Fig.1. An example of a DODAG in RPL network

The RPL routing protocol is one of the popular IoT routing protocols that support IPv6 communication as specified in [1]. It is considered as a blend of

Distance Vector (DV) and source-routing (path addressing) protocol. It uses vectors (arrays) of distances to other nodes in the network and has a router to inform its neighbor of topology changes periodically. Each node in the RPL network maintains a vector (table) of the minimum distance of every node. The RPL routing protocol uses various route metrics in order to calculate the cost of reaching a destination. In the RPL network, a sender can partially or completely select the route the packet travel through the network. That is why it is a source routing protocol.

RPL builds a topology as a Directed Acyclic Graph (DAG) which divided into one or more Destination Oriented DAGs (DODAGs). Figure 1 shows an example of a DAG rooted at a single destination at a single DAG root (DODAG).RPLInstanceID is used to identify and maintain a topology RPL. An RPL Instance means a set of one or more DODAGs share a RPInstanceID. DODAGs having the same RPLInstanceID share the same Objective Function (OF) for computing the position of a node in the DODAG. Examples of OFinclude Objective Function Zero (OF0) andMinimum Rank with Hysteresis OF (MRHOF). DODAGID is a number version of a DODAG. It is a sequential counter incremented by the root to form a new version. The rank value of a node represents the node position in the DODAG with respect to the root. The rank values of child nodes must be greater than the value of their parents to maintain the acyclic nature of the graph. This value increases in the downward direction. There are two types of DODAG. A node in a grounded DODAG satisfies the application goal, but a node in floating DODAG is expected to satisfy the goal. A floating DODAG only offers routes within the DODAG. DODAG can offer two mode-of-operation: Storing and Non-storing. Nodes in a storing mode-of-operation maintain a downward routing table. Nodes with a lower rank like 1-3 nodes in figure 1 have bigger routing tables. The protocol wouldn't succeed in case any of these tables is full. On the other hand, in a non-storing mode-of-operation, root uses source routes to send packets to leaf nodes. This mode is more expensive compared with the storing mode-of-operation. RPL supports two traffic flows:Point-to-MultiPoint (P2MP) and MultiPoint-to-Point (MP2P) as shown in figure 1.

The RPL protocol uses four ICMPv6 control messages for sharing routing information and managing DODAGs: DIS (DODAG Information Solicitation), DIO (DODAG Information Object), DAO (Destination Advertisement Object) and DAO-ACK (Destination Advertisement Object Acknowledgement) messages. If a node wants to join the DODAG like node 10 in figure 1, the node uses the DIS messages in order to get routing-related information from the neighbor nodes which are 4, 9 and 7 in this example. These nodes reply by sending the DIO messages. The DIOmessageshave all the information required by RPL in order to join the DODAG.A DIO message consists of the following fields: the rank value, the mode-of-operation, the RPL instance ID, and the DODAG ID.

Table 1.RPL routing protocol attacks

Attack	Feature of the attach	Consequences on network's performance
spoofing/replaying information	Create non-existent information or partially modify data	Attracting/repelling network traffic, creating routing loops.
selective forwarding	Refusing to forward massages from selected nodes	Reducing traffic and increasing data loss
Blackhole	Failing to forward any data packets including its own	Reducing traffic and increasing data loss
sinkhole	Advertising false information to create a center of attraction for other nodes.	Compromise of transmission routes, reducing traffic and increase data loss.
node replication	Physical capturing of a node, its replication and deployment back into the network.	Compromise of transmission routes, eavesdropping on the falsely created links.
Wormhole	Create a low link tunnel between two malicious nodes in different parts of network	Sending data to the false distention, undermining cryptography protection.
hello flood	Broadcasting a hello packet to the whole network with great transmission power.	Increasing energy degradation and collisions, create false transmission routes.

The rank value of a node represents the node position in the DODAG with respect to the root. The rank values of child nodes must be greater than the

value of their parents to maintain the acyclic nature of the graph. This value increases in the downward direction. The nodes utilize the trickle algorithm [2] to set a timer for sending the DIO messages periodicallyin order to optimize the transmission frequency of control messages according to the network state. Nodes joining the DODAG use the DAO messages to build downward routes along the DODAG. If the DODAG root or DAO parent who receivers a DAO message wants to acknowledge this message, the receiver sends back to the sender in a unicast way a DAO-ACK.

Building a DODAG graph has several steps. First, as shown in figure 1, the root broadcasts a DIO message to its neighbors. Once a node receives a DIO message the node adds the sender of this message to its parents-lists, and calculates its rank value using the objective function mentioned in the DIO message. Then, the node broadcasts updated DIO messages. The node uses its parents-list to select a preferred parent (the default gateway). If the node wants to send data toward the DODAG root, it uses a preferred parent. All the nodes joining the DODAG graph have an upward default route toward the root. This route consists of all the preferred parents. After that, the nodes use the DAO messages to build the downward routes.

The DODAG root specifies the mode-of-operation by the DIO messages, and router nodes maintain routing tables. In the storing mode,the child node unicasts a DAO message to its selected parent. The routes received from other DAO messages are aggregated by the parent. The parent, then, sends the collected information to its parent recursively by a DAO message. On the other hand, in non-storing mode, the nodes unicast DAO messages to the DODAG root, and the parents do not store routing information. The nodes can acknowledge the receiving of DAO messages by DAO-ACK messages.

The RPL routing protocol has mechanisms to repair DODAGS, detect inconsistencies and avoid loops. DODAG loops occur if a node does not respect the rank value, and the DODAG graph is no longer acyclic. In order to avoid loops, if a node wants to leave the sub-DODAG, the node must advertise an infinite rank.The nodes may also use a detaching mechanism to leave the DODAG.This mechanism forms an intermediary floating DODAG which the nodescanrejoin the main DODAG later.The RPL routing protocol can use the data-path validation mechanismto detect inconsistencies [1]. After detecting the inconsistencies, the RPL nodes must trigger the repair mechanisms that the RPL rebuilds the network completely.

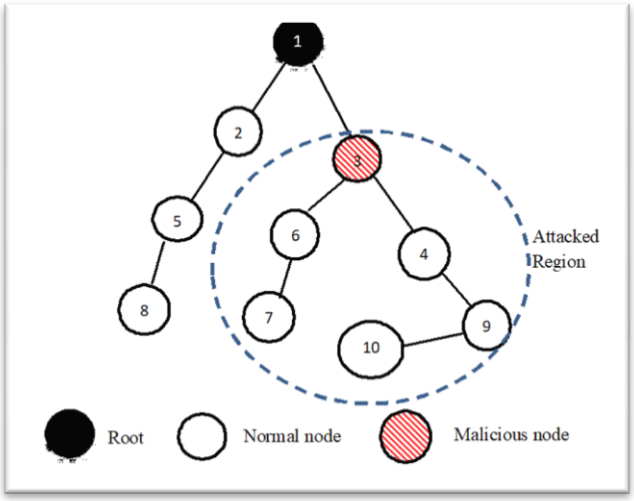


Fig. 2. An example of selective forwarding attacks in RPL network

However, while the IETF ROLL workgroup specified the security requirements of RPL, they did not specify security models for it. Basically, the standard RPL protocol utilizes key management in the application of sensor nodes which are already configured. The key management mechanism allows only the authenticated RPL nodes to join the network.The lack of specification that it does not define how RPL sensor nodes authenticate and securely connect among themselves is considered as a weakness in the security design of the IETF RPL standard. This makes the RPL protocol vulnerable to several routing attacks which are explained in Table 1 [3].

This research paper focuses on the impact of selective forwarding attacks on the performance of RPL-based IoTs. Figure 2 shows an example of selective forwarding attacks in RPL network.In this attack, malicious nodes can drop out a specific type of packets or drop packets from specific nodes in the network. In this researchwork,the authors have focused on dropping the data packets only not routing packets. In figure 2, node 3 will not forward the data packets received from its neighbor to the root while it will forward the routing packets. In this attack, if the malicious nodes drop all the packets (data packets and routing packets), this attack can be named as a black hole attack. However, because of such behavior, this attack is easy to detect compared with the selective forwarding attack.

The rest of the paper is organized as follows: Section II presents the related work; section III presents simulation results and analysis followed by conclusions in Section IV.

2.Related work

There are several research activities discussing the challenges of the RPL routing protocol in IoT regarding potential security threats and countermeasures. Tomić and McCann [4]surveyed the main security mechanisms and their effects on standards and the most popular protocols used in WSN deployments. In their work, they quantified the effect of attacks on the performance of the network using Cooja simulator. Similarly, Chris and Wagner [5] described attacks against sensor networks and suggested countermeasures and design considerations. In [6], the authors implemented and demon-

strated attacks against 6LoWPAN networks running IoT protocols, and they showed the impact of routing attacks against RPL and how some attacks can be avoided by RPL's self-healing mechanisms.

The research work in [7] and [8] discussed selective forwarding attacks and some of the mitigation schemes to defend this attack without any simulation experiments. Kaplantzis, et al. [9] proposed a centralized intrusion detection scheme that can detect selective forwarding attacks and black hole attack with less energy-consuming. The suggested scheme is based on sliding windows and Support Vector Machines (SVMs). Their simulation results showed that the suggested scheme can detect black hole attacks with 100% accuracy and selective forwarding attacks in which 80%.

To the best of the authors' knowledge, no previous work evaluated and highlighted the quantitative impact of selective forwarding attacks on the performance of RPL routing protocol in IoT. This work provides an insight to guide network protocol desingers protecting the RPL network from such attack.

3.Impact of Selective Forwarding Attack On RPL

This section presents the impact of the selective forwarding attack on the performance of RPL based networks. The performance has been measured in terms of two metrics namely packet delivery ratio and end-to-end delay for different node densities and varying number of attacker nodes.

3.1 Simulation Setup

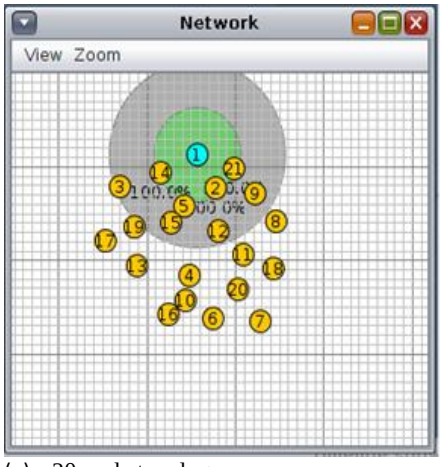
Cooja simulator (Contiki 2.7 [10]) has been used to implement RPL based IoT networks and evaluate the impact of selective forwarding attacks. The simulation used usedTmote sky [11] (alias sky mote) that is a mote platform for extremely low power, high data-rate sensor network applications. Sky motes have been used in three roles namely sink, sender and malicious. The sink mote operates as a destination point where sender nodes send their collected data. The sender mote operates as data collectors. The malicious mote drops the data packet received only by the neighbors (Selective Forwarding Attacks).

The IoT related simulation parameters generally follow [12][4][13]. The radio propagation is based on unit disk graph model. A source-to-root traffic is simulated where each sender node periodically sends data to the root node at a rate of one packet per 10 seconds, and the medium access control (MAC) protocol is simulated using the Contiki MAC, IPv6 [10]. Nodes are placed randomly in an area of 500 x 500 square meters where all nodes are reachable in a multi-hop manner. Transmission power and receive power threshold are set such that the effective transmission range is 50m, and no packet loss has been considered to better evaluate the impact of the selective forwarding attack. Nodes send data packets using UDP (User Datagram Protocol)protocol.

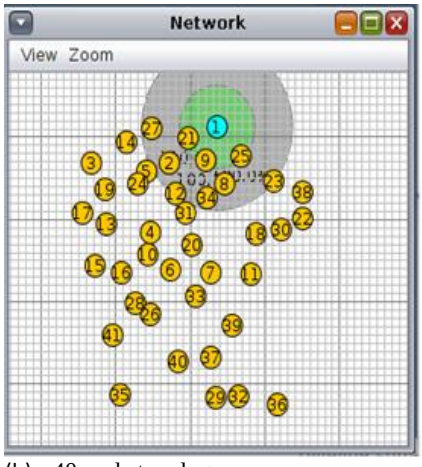
3.2 Simulation results and analysis

Two different simulation scenarios

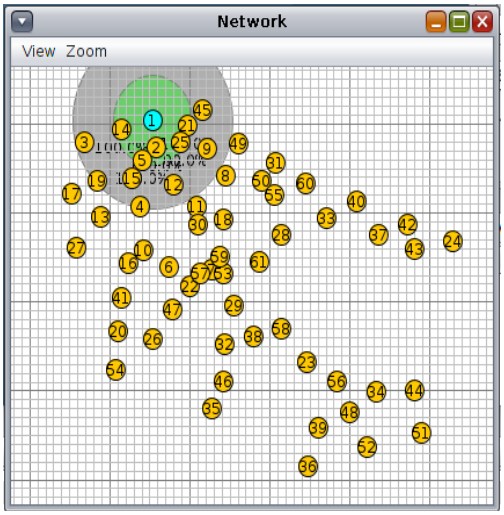
namely the density-scenario, and the attacker-scenariohave been used to see effects of varying node density, and varying number of selective forwarding attacker nodes respectively on the performance metrics namely packet delivery ratio and end-to-end delay. There are two variables namely the number of nodes (Sky mote, 20, 40, 60, 80, 100 senders, 1 root), and attackers (number of attackers: 2, 4, 6, 8, 10) involved in the two scenarios.



(a) 20-node topology

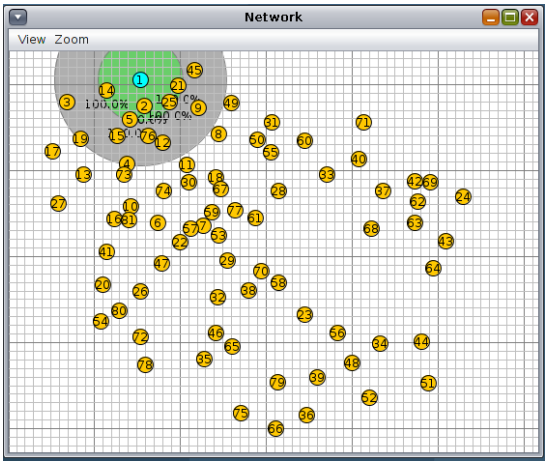


(b) 40-node topology

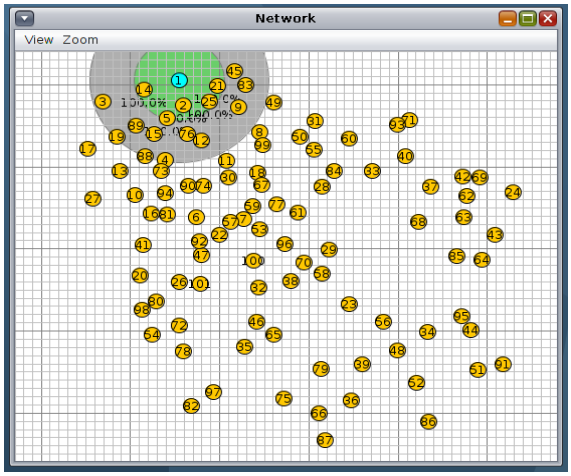


(c) 60-node topology

Fig.3. (A) the Network topologies of the simulation experiments



(a) 80-node topology

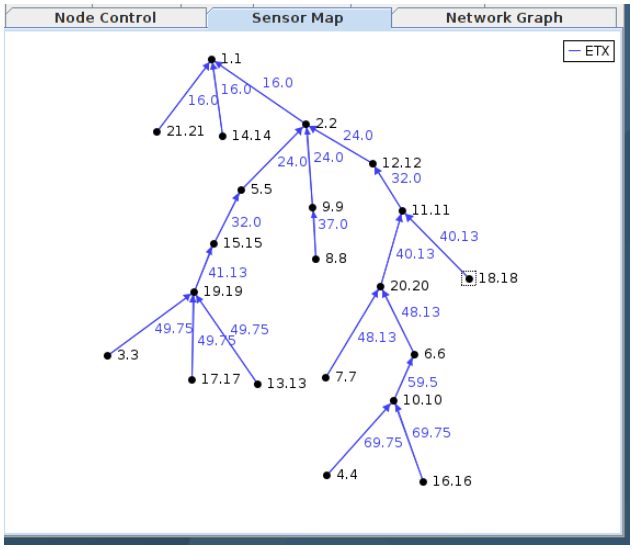


(b) 100-node topology

Fig. 3. (B) the Network topologies of the simulation experiments

The network topologies and a sample of sensor map are shown in figure 3. (A and B) and figure 4 respectively. In figure 3 (A and B), the root node is node number 1 with differentcolor from the reset of the nodes. The small green circle and the large grey one surrounding node 1 (root node) represent transmission range and interference range respectively. In figure 3 (A and B), 100% in the green circle means no packet loss to better evaluate the impact of the selective forwarding attack. In figure 4, the black numbers 1.1, 2.2, … 20.20 refer to node numbers while blue numbers 16.0, 24.0, …, 69.75 present the rank values that increase in the downward direction.

In each scenario, one variable is varied while the other variable is fixed. The density scenario has six attackers. The attacker-scenario uses a fixed



number of nodes which is set to 60. The position of malicious nodes was chosen tactfully to maximize their impact on the network e.g., an attacker node cannot be a leaf node because leaf nodes do not forward packets. The behavior of these malicious nodes is that they drop all data packets but they forward the routing packets. Results have been obtained via averaging values from two different runs with different seeds, and the duration of each one is three hours.

PDR (Packet Delivery Ratio)

The PDR represents the ratio of packets successfully delivered to the root. Figure 5 shows the PDR averaged for all nodes as a function of a number of nodes with six attackers. Figure 6 shows the average PDR as a function of a number of attackers when the number of nodes is 60.

If an attacker drops all messages completely, as in the black hole attack, it runs the risk that neighboring nodes can quickly conclude that an attack is underway and use other routes to avoid the attacker.It is more difficult to detect the attack if messages are selectively suppressed

As a general trend, the average PDR of nodes shrinks in both scenarios. This is because of that the malicious nodesdropdata packets leading to limit the achievable PDR.

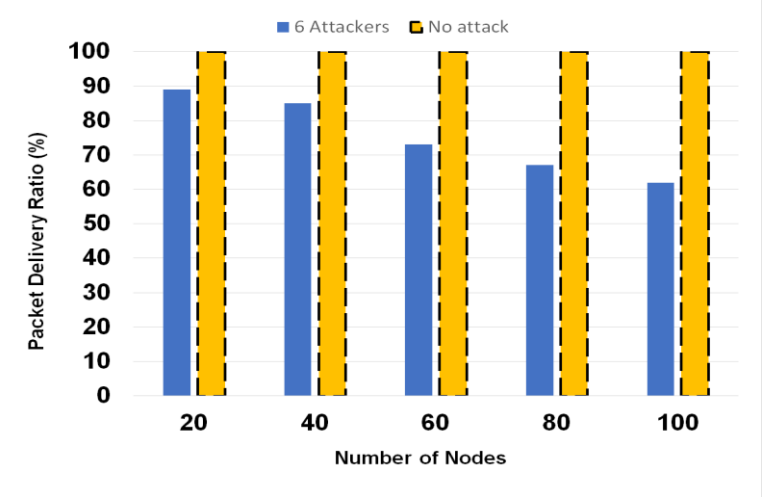


Fig. 4. Packet Delivery Ratio vs Number of Nodes (Density-scenario)

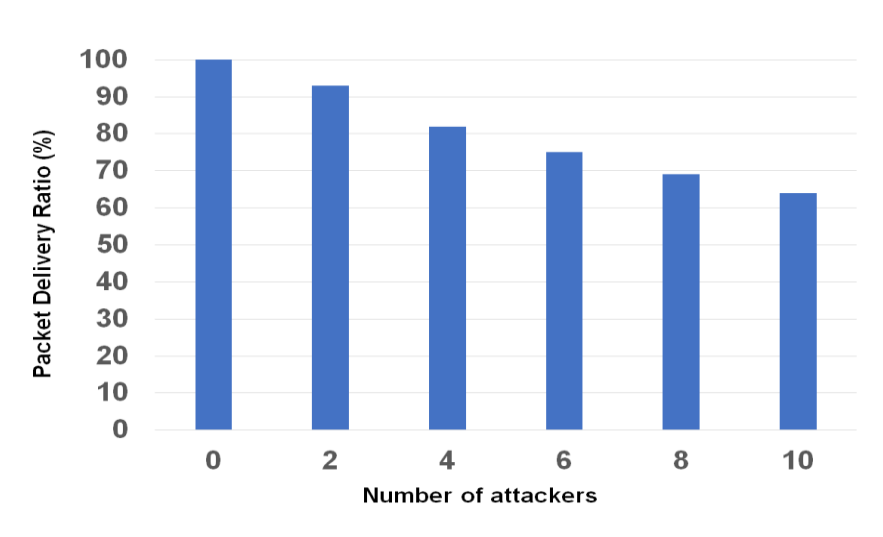


Fig 5. Packet Delivery Ratio vs Number of attackers (Attackers-scenario) When N=60

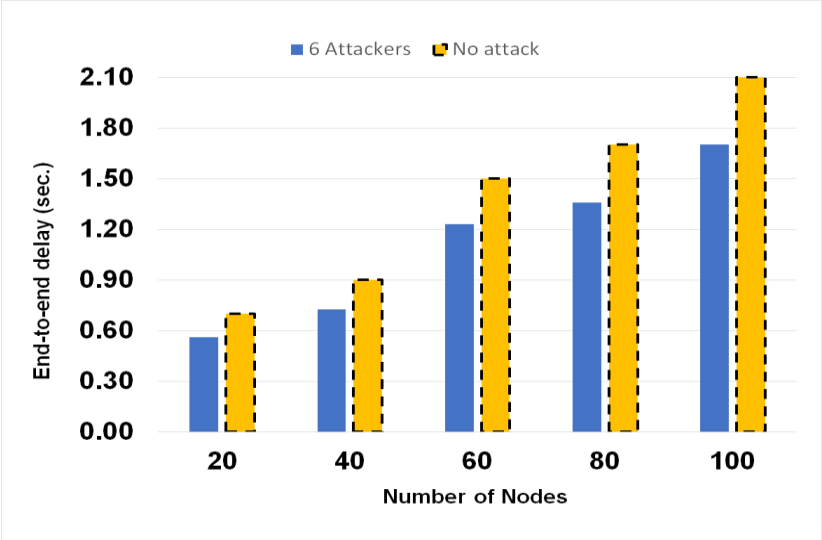
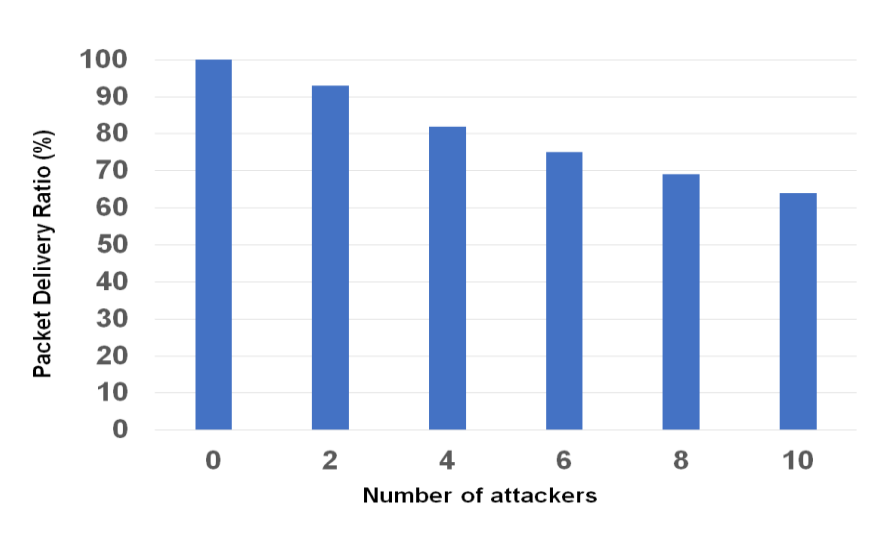


Fig. 6. End-to-end Delay vs Number of Nodes (Density-scenario)

End- to- end delay

End-to-end (E2E) delay is the average time a packet needs to travel between the sender node and the root node. Figure 7 shows the average end-to-end delay for data packets for all nodes as a function of varying number of nodes with six attackers. Figure 8 shows the average end-to-end delay for data packets for all nodes as a function of varying number of attackers when the number of nodes is 60.

Figure 7 shows that the average end-to-end delay increases with increasing number of nodes. By increasing the number of node contention increases leading to higher queuing delay at the transmitter's buffer and higher packet loss rate due to the malicious node attack. As a result of that, data packets



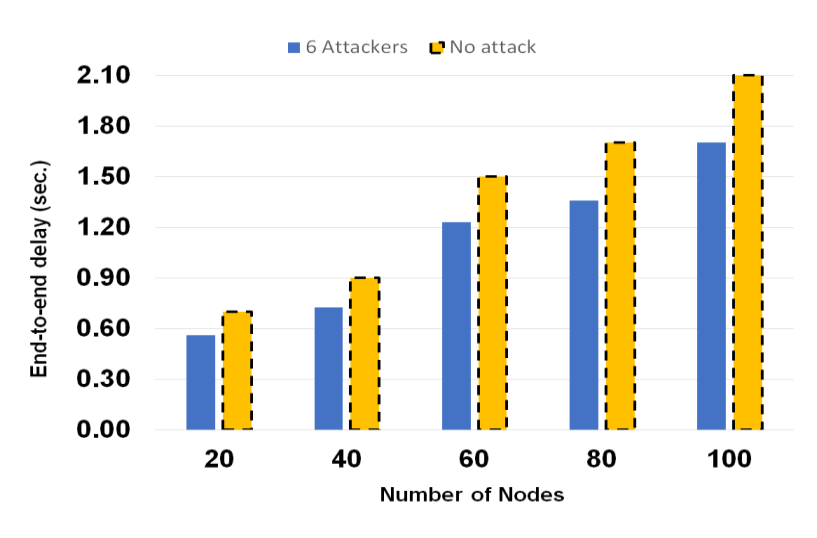


Fig. 7. End-to-end Delay vs Number of Nodes (Density-scenario)

End- to- end delay

End-to-end (E2E) delay is the average time a packet needs to travel between the sender node and the root node. Figure 7 shows the average end-to-end delay for data packets for all nodes as a function of varying number of nodes with six attackers. Figure 8 shows the average end-to-end delay for data packets for all nodes as a function of varying number of attackers when the number of nodes is 60.

Figure 7 shows that the average end-to-end delay increases with increasing number of nodes. By increasing the number of node contention increases leading to higher queuing delay at the transmitter's buffer and higher packet loss rate due to the malicious node attack. As a result of that, data packets need to be retransmitted. On the other hand, figure 8 shows how the malicious node attacks help the unaffected packets to go faster leading to a lower average delay.

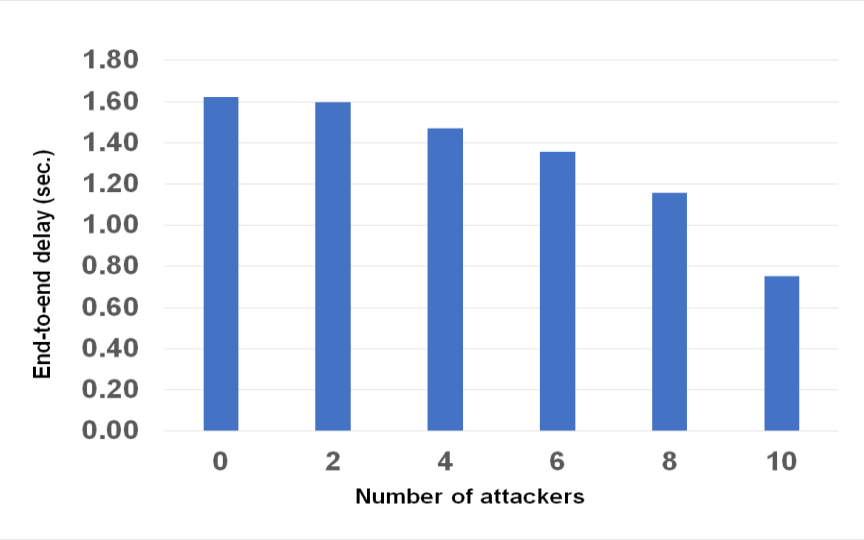


Fig. 8. End-to-end delay vs Number of attackers (Attackers-scenario) When N=60

4.Conclusion

Based on the simulation results and analysis, it can be concluded that in the selective forwarding attacks, the malicious nodes are active during the network lifetime because the malicious nodes drop data packets only, so the control packets are not affected. Consequently, the RPL will not run the self-healing mechanisms for rebuilding the topology in order to enhance the network performance. Therefore, the application layer factors need to be considered when the future solutions for this kind of attacks are suggested.

Obviously, in varying number of attackers' scenario, the malicious nodes have decreased the average of both packet delivery ratio and end-to-end delay. Some data packets are dropped by the malicious nodes, so the other data packets travel faster to the root. However, in the density scenario, the malicious nodes have more negative effects because it decreases the packet delivery ratio.

Reference

[1] T. Winter, P. Thubert, A. R. Corporation, and R. Kelsey, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *Internet Engineering Task Force (IETF)*. [Online]. Available: https://tools.ietf.org/html/rfc6550. [Accessed: 08-Apr-2018].

[2] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. KO, "The Trickle Algorithm," *RFC 6206, IETF*, 2011.

[3] R. Alexander and C. P. Systems, "A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL)," 2014. [Online]. Available: https://tools.ietf.org/pdf/draft-ietf-roll-security-threats-06. [Accessed: 10-Nov-2019].

[4] I. Tomić and J. A. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1910–1923, 2017.

[5] K. Chris and D. Wagner, "Secure Routing in Wireless Sensor Networks : Attacks and Countermeasures," in *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, 2005, pp. 113–127.

[6] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," *Int. J. Distrib. Sens. Networks*, vol. 2013, pp. 1–11, 2013.

[7] L. K. Bysani and A. K. Turuk, "A survey on selective forwarding attack in wireless sensor networks," *2011 Int. Conf. Devices Commun. ICDeCom 2011 - Proc.*, pp. 1–5, 2011.

[8] H. M. Sun, C. M. Chen, and Y. C. Hsiao, "An efficient countermeasure to the selective forwarding attack in wireless sensor networks," in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 2007, pp. 4–7.

[9] S. Kaplantzis, A. Shilton, and N. Mani, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines," in *2007 3rd International Conference on Intelligent Sensors Sensor Networks and Information*, 2007, pp. 335–340.

[10] "Cooja Simulator." [Online]. Available: https://github.com/contiki-os/contiki/wiki/An-Introduction-to-Cooja. [Accessed: 20-Oct-2019].

[11] J. Polastre, R. Szewczyk, and D. Culler, "Telos: Enabling ultra-low power wireless research," in *2005 4th International Symposium on Information Processing in Sensor Networks, IPSN 2005*, 2005, vol. 2005, pp. 364–369.

[12] L. Lassouaoui, S. Rovedakis, F. Sailhan, and A. Wei, "Evaluation of energy aware routing metrics for RPL," in *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2016, pp. 1–8.

[13] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sens. J.*, vol. 13, no. 10, pp. 3685–3692, 2013.