On the performance of 6LoWPAN using TSCH/Orchestra mode against a jamming attack

Conference Paper · September 2019

CITATIONS
0

READS
51

4 authors, including:

Cesar A. Azurdia-Meza
University of Chile
99 PUBLICATIONS **358** CITATIONS
SEE PROFILE

Claudio Valencia
University of Santiago, Chile
19 PUBLICATIONS **7** CITATIONS
SEE PROFILE

Samuel Montejo Sánchez
Universidad Tecnológica Metropolitana
54 PUBLICATIONS **147** CITATIONS
SEE PROFILE

On the performance of 6LoWPAN using TSCH/Orchestra mode against a jamming attack

Nicolas López, Cesar Azurdia-Meza, Claudio Valencia, Samuel Montejo-Sánchez.

***Abstract*— The active jamming for disrupting legitimate transmissions is currently one of the most used techniques by attackers. These attacks are difficult to detect and have been little addressed in low power and lossy networks (LLN), for instance there are few simulations of scenarios that consider the presence of an attacker in LLNs. In this work it is simulated the presence of an attacker in an LLN with IPv6 over the Time-slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e and over the most recent Orchestra mode. The results show remarkable variations, in terms of Packet Data Rate (PDR) and energy efficiency, on the simulated scenarios when a malicious node is present, despite the Medium Access Control (MAC) mode used. For instance, the PDR shows a variation of 20 % and the energy consumption 20 % in the jamming scenario. Based on our metrics, we suggest guidelines to generate countermeasures and detection of these types of attacks on indoor networks.**

***Index Terms*— Jamming, orchestra, TSCH, 6LoWPAN.**

I. Introduction

The massive deployment of low power and lossy networks (LLN) to acquire data from several environments has brought several challenges to the nodes that process and communicate these data. The principal challenges and limitations are in terms of energy, memory and processing costs. The RFC 7228 [1] defines a node with these limitations as a constrained node. To achieve the nodes communication, one of the used standards is the IEEE 802.15.4 [2] that allows different operation modes in the Medium Access Layer (MAC). The Time Slotted Channel Hopping (TSCH) is a mode in the MAC layer that allows the communication in a shared medium network using different channels and at different time slots as represented in Figure 1. The last improvement to the TSCH mode is called Orchestra mode [3] and combines the mechanisms of different channels and times with the addition of autonomous scheduling of communications as represented in Figure 2. This communication scheduling achieves better performance of the nodes in terms of Packet Data Rate (PDR) and energy efficiency

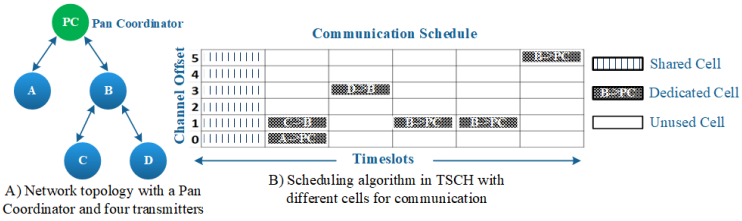

Fig. 1: TSCH algorithm

Some works have studied variables such as interference or an attacker in the communication to provide realistic data of the performance metrics [4] [5] .The TSCH mode has been tested both in ideal scenarios and scenarios with the presence of interference that could be malicious, such as in the event of an attacker, or not [4]. Moreover, in [5], the authors simulate and implement scenarios with TSCH, Efficient Multichannel-MAC [6], and Orchestra mode. The metrics PDR, latency, and energy consumption are used to evaluate the performance of the network in the scenarios. The retrieved data showed that TSCH and Orchestra mode has a better performance than the EM-MAC mode in the performance metrics. Although, the scenarios assume ideal conditions and do not analyze the presence of interference or an attacker.

However, to the best knowledge of the authors, the tested scenarios for Orchestra mode do not consider the presence of interference or an attacker in the communications. As a result, is not clear if Orchestra mode could perform better than TSCH mode in the simulated scenarios with the presence of an attacker.

The presence of attackers on the communications systems is a common issue that is considered in the deployment of a network. The attacks that are performed in the physical layer of the OSI model are eavesdropping and jamming attacks [7]. In particular, the jamming attacks, generate intentional interference for disrupting the data communications between legitimate nodes. The interference is generated by a jammer device that restricts the access of the authorized nodes to the resources of the network. In this work, we analyze the jammer device and the impact of the generated interference on the resources of the network through simulations.

Submmited 07/23/2019 “This work partially funded by Project FONDECYT 11160517 and FONDECYT Postdoctoral Grant n.3170021.”

Nicolas L. and Cesar A are with the Department of Electric Engineering, Universidad de Chile ,Tupper 2007, Santiago, Chile (e-mail : secdirdie@ing.uchile.cl).

Claudio V. is with the Department of Electric Engineering, Universidad de Santiago de Chile, Ecuador 3519 , Santiago, Chile (e-mail : claudio.valenciac@usach.cl).

S. Montejo-Sánchez is with the Programa Institucional de Fomento a la I+D+i, Universidad Tecnológica Metropolitana, Ignacio Valdivieso 2409, Santiago, Chile (e-mail: smontejo@utem.cl).

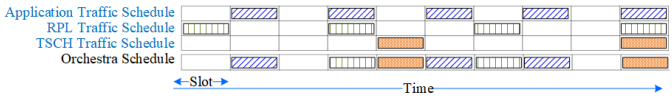

Fig. 2: Orchestra algorithm

II. Related Work

The LLNs are built by different constrained nodes that communicate through a wireless medium [8]. These networks can be used in diverse environments and applications to acquire data. Some of the typical uses are wireless sensor networks, vehicular networks, machine-to-machine (M2M) communication, unmanned aerial vehicle (UAV). The capability to acquire data in many of environments has brought the attention of the scientific and the industrial area [7]. One of the main topics of research from these areas is the security of these networks. Due to the broadcast nature of an LLN, they are exposed to different types of attacks. Eavesdropping, and Denial of Service (DoS) attacks are some of the attacks performed by the attackers [9]. The simplest attack performed on the physical layer that generates a DoS is known as constant jamming. Additionally, it is easy to implement and the circuitry it is inexpensive.

Recent works have evaluated and generated countermeasures against these types of attacks [10] [11] [12] [13] . In [13] authors used the TSCH mode with a random selection of the channels in the presence of a jamming attack. They assume that the attacker has information about the protocol of communications and that not all the channels can be affected at the same time. The proposed countermeasure algorithm presents notorious improvements in the PDR metric using TSCH mode. However, valuable performance metrics as energy consumption are not studied. Also, they do not establish a comparison between the TSCH and Orchestra mode with the algorithm.

In [12] they generate a model of jammer based in a gambling game for time-critical applications as a smart grid. They analyze the impact of a reactive jamming and non-reactive jamming in WiFi-based wireless. Based on the analysis, the authors design the JADE system to improve the efficiency of the network, and also to detect the attacker. However, the MAC modes TSCH/Orchestra and the energy consumption are not analyzed.

The focus on [10] is to generate a DoS attack to undermine the performance of the routing protocol (RPL). For that, they create an attack called “Hatchetman” that manipulates the head of the frames. As consecuence of this manipulation the receiver node discard the subsequent frames. Consequently, an excessive generation of error messages by the receiver node leads to an overflow of the communications. The results showed that the ”Hatchetman” attack decrease PDR and throughput and increase energy consumption and latency.

In [11], the authors perform an attack on the schedule algorithms in a network using TSCH and Orchestra. By observing the channel’s activities, they can reverse engineer the channel hopping sequences for both modes. The metrics analyzed consist in examine the performance of the cracking process to obtain the sequence as cracking time and accuracy. Also, they make suggestions to improve the robustness of the algorithms against this type of attack.

Studies that use the Orchestra mode against a DoS attack to analyze the impact on the algorithm and the metrics of the network are inexistent. Moreover, the different studies that consider the presence of an attacker on the networks do not assume the mobility of the nodes or the attacker. Also, they do not analyze the metrics of PDR, and energy consumption for each scenario.

The analysis of the Orchestra mode against a jamming attack is inexistent. For this reason, one of the main contributions of this work is the evaluation of the performance of the simulated network in the presence of a DoS attack. With this evaluation, in terms of the PDR and duty cycle, we could give insights about the impact of this type of attacks. Also, the experimental evaluation and generation of countermeasures are planned for future work.

III. Performance Metrics

We use the Packet Delivery Ratio (PDR) and duty cycle to analyze the behavior of the simulated network in various scenarios with an attacker. Further, the effects on the algorithms of the MAC modes will be linked through the metrics.

A. Packet Delivery Ratio

The PDR is the rate between the total successfully transmitted packets to the total sent packets by the transmitter. This metric is acquired in each receiver node through the calculation of the packets with a correct CRC field. Also, the PDR can be calculated in the sender node by the register of the ACK packets received by the destination node. The PDR is defined by:

$$PDR = \frac{\sum_{i=0}^{n} x_j}{\sum_{i=0}^{n} y_j}, \tag{1}$$

where x_j is the number of received packets from each sender node, and y_j is equal to the total number of the generated packets in each sender.

B. Energy Consumption

The nodes can work in different states as transmit, reception, and low power mode. These states have different values of current consumption that are calculated by the total time in the state, multiply by the current consumption in the specific state. The current used in each state is extracted from the datasheet of the emulated platform [14]. To obtain the total energy consumption E in miliJoules (mJ) for each node, we use the following equation [15]

$$E = \frac{(0.5\ t_{CPU} + 5e-4\ t_{LPM} + 17.4\ t_{Tx} + 18.8\ Rx)3}{32768} \tag{2}$$

where t_{CPU}, t_{LPM}, tTx, and t_{Rx} are the elapsed times in each state, and the denominator indicates the ticks per second for $Z1$.

IV. Methodology

We conducted extensive experiments using the Cooja simulator to evaluate the performance of the simulated network in the presence of a jamming node. We evaluated the TSCH and Orchestra algorithms on two simulated scenarios generated in the Cooja simulator. Once we have simulated the network, we test the network to verify a correct operation. Then, we acquire the performance metrics. Next, we add a jammer device into the network to generate the second scenario. Finally, we establish a comparison between the simulated scenarios.

Figure 3 shows the ideal scenario with five constrained nodes (1 root, 4 senders), transmitting packets related to the MAC and RPL non-storing mode. The nodes are uniformly distributed in a $10x10m^2$ square network area. The distance between each node is equal to $10m$ with a communication range of $50m$, without variations in the experiments. Also, the distribution order of the nodes in the deployment is the same, shown in the Figure 3. During the experiments, we do not consider mobility of the nodes. The radio model simulated is a Zolertia $Z1$ [14] with a data rate of $250kbps$ in the 2.4 GHz band.

In the experiments, the ideal scenario is used to establish a comparison. We employ this scenario to acquire performance metrics without an attacker. After that, the scheduling algorithms are implemented in the nodes to achieve Orchestra mode and later acquire the same performance metrics.

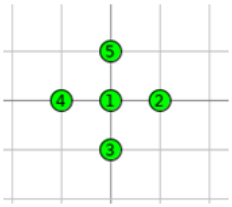

Fig. 3: Ideal Scenario

Subsequently we put a disrupt node in the simulated network, that will be the jammer device performing a DoS attack. The jammer generates a interference signal when a transmission of any legitime nodes is performed. We select two fixed places to put the jammer. These places allow the jammer to impact various nodes at the same time. The interference signal power and the transmission range is the same as the sender nodes. Also, we obtain the performance metrics for each node. Later, we compare and analyze the results obtained of the both scenarios.

V. Results

Using the defined metrics, we evaluated the performance of TSCH and Orchestra mode. In the scenario with the presence of an attacker, the disrupted node (jammer) is deployed in two different places as showed in figure 4 with the following considerations: interferes one transmitter node, interferes two transmitters and neighbors node, interferes two transmitters, neighbors and coordinator nodes. These variations are performed to analyze the behavior of the network and also, acquire the metrics of PDR and energy consumption. Also, we perform a third scenario where the jammer interrupts two transmitter nodes and the coordinator of the network. When the coordinator is affected, the scheduling algorithm is lost in the transmitter nodes but not in the coordinator. Consequently, the results of the PDR and duty cycle are not relevant as the other two scenarios. For this reason, the results obtained are not considered in the analysis.

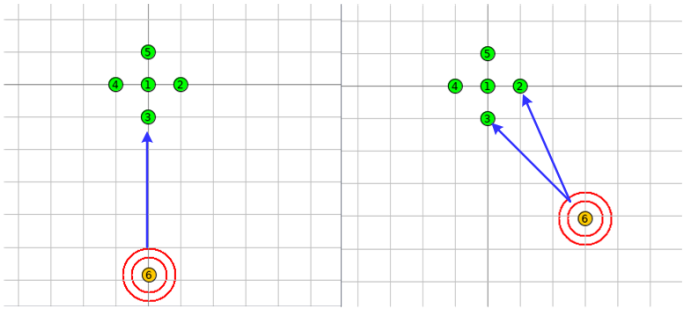

Fig. 4: Jammer fixed position through the simulations

We analyze the results in three parts. First, we simulate the network and we obtain the performance metrics of both TSCH and Orchestra mode in an ideal scenario. Then, we generate the second scenario. We perform the same steps as the first scenario with the presence of the jammer on the network. Finally, we compare the results of the performance metrics in both scenarios with TSCH and Orchestra mode. In the experiments the concurrent transmission of two or more packets always results in a collision and, hence, a transmission failure. Also, in the simulator, the radio medium is simulated and configured as Unit Disk Graph Medium (UDGM) in concordance with the related work. The other related parameters are configured with the default value described in the standard [16]. To obtain the PDR, we use radio message tool. This tool performs a log of the packets generated, transmitted or received for each node of the network with timestamps. Also, the tool incorporates a 6LoWPan analyzer with PCAP option to analyze the packets.

Modo	Ideal (%)	Jamming(A) (%)	Jamming (B) (%)
TSCH	99.3	81.04	62.78
Orchestra	99.9	80.82	63.14

TABLE I: PDR summary for the experiments. Both protocols are affected by the jammer device.

In the ideal scenario, TSCH and Orchestra mode have an optimal performance in terms of the evaluated metrics as presented in [3]. Under the jamming attack, the legitimate packets have more chances to collide with the jamming packets. Consequently as shown in table I and figure 5 the PDR decreases to 80.82% and 81.04% in the Orchestra and TSCH mode, respectively. Furthermore, as we expected when two transmitter nodes are affected the PDR decreases in 17% for both modes. As a consequence, the scheduling algorithm used in Orchestra mode cannot overperform the random allocation channel of TSCH mode. As a result, PDR are almost the same for both scenarios.

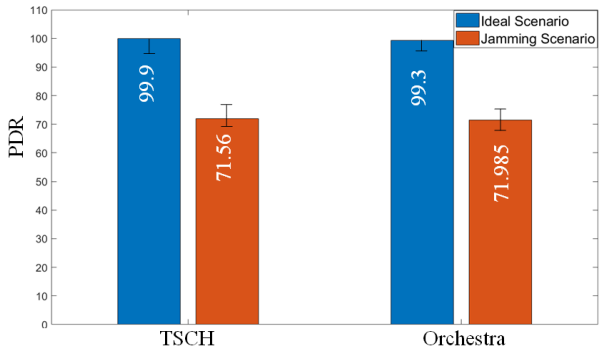

Fig. 5: Average PDR obtained from both tested scenarios

Finally, the energy consumption is analyzed. We acquired the results of the duty cycle and the energy consumption for each node and the network. In the ideal scenario, both modes achieves a low duty cycle and energy consumption. Most of the time, the nodes stay in an ”on” state when the network is formed as represented in Figure 6.

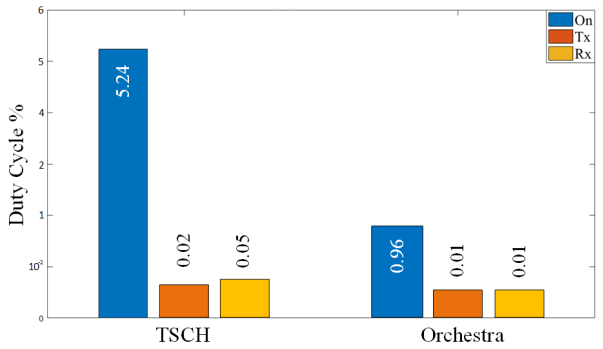

Fig. 6: Duty cycle of the transmitter node in the ideal scenario for both modes. The Tx and Rx states are negligible .

In the jamming scenario, and as expected, a higher energy consumption exists. A higher chance of collision of the packets triggers the retransmission and sense of the channel algorithms frequently. Consequently, the execution of the algorithms demands more energy to the nodes that increase the duty cycle to 96% on average, as shown in Figure 7.

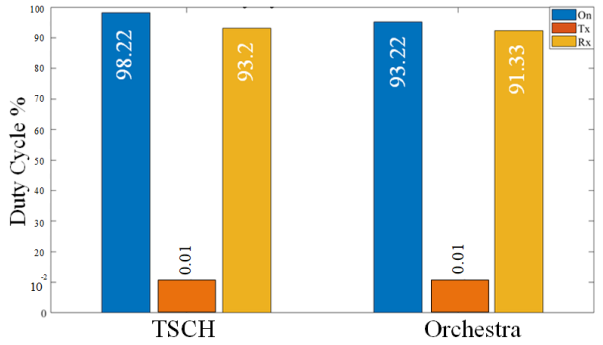

Fig. 7: The duty cycle of the transmitter node in the jamming scenario. The reception state leads to a considerable increase in energy consumption

Also, we can observe an unusual behavior of the nodes affected by the jamming attack. When a transmitter node is in the presence of the attacker, the synchronization and schedules are affected. As a consequence, the nodes decided to leave the network and enters a steady receiver state. In this state, the node performs a sense of the transmission channels perpetually. Therefore, the duty cycle of the node increases to almost 99% for both MAC modes as represented in Figure 8.

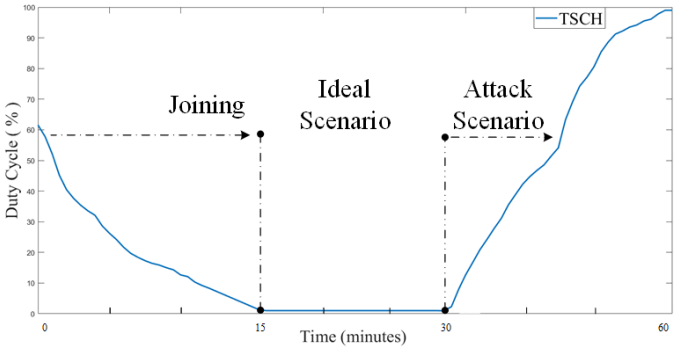

Fig. 8: Energy consumption as a timeline for TSCH mode in the different scenarios

Besides, we obtained a higher energy consumption in the joining process of the nodes for both MAC modes. Orchestra mode achieves a lower energy consumption than TSCH mode by 5% in the joining time process. The values of the duty cycle for the simulated scenarios are summarized in figure 8 as a timeline for the TSCH mode. Moreover, the timeline for Orchestra mode presents the same behavior to the obtained with TSCH.

As a result, the duty cycle is almost five times higher in the network with the presence of an attacker for TSCH mode and twenty times for Orchestra mode, as shown in Table I.

Modo	Ideal (%)	Jamming(A) (%)	Jamming (B) (%)
TSCH	5.24	24.08	42.792
Orchestra	0.96	20.768	40.176

TABLE II: Average Duty cycle summary for the network in the experiments. Both protocols are affected by the jammer device.

With the duty cycle obtained, we calculate energy consumption. For both modes in the jamming scenario, the consumption is considerably higher as represented in Table III. The node with orchestra mode is the most affected by the incidence of the jamming attack.

Modo	Ideal (mJ)	Jamming (mJ)
TSCH	$6.534e-4$	0.16491
Orchestra	$4.17619e-4$	0.161463

TABLE III: Average energy consumption summary for the node in the experiments.

To minimize energy consumption when an attack is present, the use of an algorithm that brokes the perpetual receiver state is recommended. Also, the record of the times that a

node resync with the coordinator could give insights about a jamming attack.

VI. Conclusion

In this paper, we presented the performance of TSCH and Orchestra mode in the presence of a constant jamming attack. Both modes are affected in terms of energy consumption and packet delivery ratio. Our results show that the energy consumption of the network increases almost four hundred times, with a steady receiver state of the nodes attacked. Moreover, the packet delivery ratio decreases by 30% due to the saturation of the channels used by the nodes.

VII. Acknowledgment

This work partially funded by Project FONDECYT 11160517 and FONDECYT Postdoctoral Grant 3170021.

References

[1] C. Bormann, M. Ersue, and A.Keranen, "Terminology for constrained-node networks rfc 7228," Internet Engineering Task Force (IETF), Tech. Rep., May 2014.

[2] I. Computer, Society, S. by the, L. Standards, and Committee, *IEEE Standard for Low-Rate Wireless Networks*, IEEE Computer Society Std., 2011.

[3] S. Duquennoy, B. A. Nahas, O. Landsiedel, and T. Watteyne, "Orchestra: Robust mesh networks through autonomously scheduled tsch," *SenSys15*, 2015.

[4] M. Mohamadi, B. Djamaa, M. Reda, Senouci, E. Militaire, P. Ecole, M. Polytechnique, E. Militaire, and Polytechnique, "Performance evaluation of tsch-minimal and orchestra scheduling in ieee 802.15.4e networks," in *The traffic patterns are also varied, and may comprise The Routing Protocol for LLNs is an oriented distance-*. IEEE, 2018.

[5] C. M. G. Algora, M. Bezunartea, and J. Tiberghien, "Performance comparison and of multichannel and mac protocols and for low-power and lossy," *Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2018.

[6] L. Tang, Y. Sun, O. Gurewitz, and D. B. Johnson, "Em-mac: A dynamic multichannel energy-efficient mac protocol for wireless sensor networks," *MobiHoc*, 2011.

[7] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," *IEEE CS*, 2008.

[8] E. X. Vilajosana, K. Pister, and T. Watteyne, "Minimal ipv6 over the tsch mode of ieee 802.15.4e (6tisch) configuration rfc 8180," Internet Engineering Task Force (IETF), Tech. Rep., May 2017.

[9] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, sep 2016.

[10] C. Pu and T. Song, "Hatchetman attack: A denial of service attack against routing in low power and lossy networks," in *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, jun 2018.

[11] X. Cheng, J. Shi, and M. Sha, "Cracking the channel hopping sequences in IEEE 802.15.4e-based industrial TSCH networks," in *Proceedings of the International Conference on Internet of Things Design and Implementation - IoTDI '19*. ACM Press, 2019.

[12] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1746–1759, aug 2014.

[13] D. Zorbas, P. Kotzanikolaou, and C. Douligeris, "R-tsch: Proactive and jamming attack and protection for and ieee 802.15.4-tsch networks," *IEEE Symposium on Computers and Communications (ISCC)*, 2018.

[14] Zolertia, "Z1 datasheet," 2010, z1 Datasheet.

[15] A. Bandekar, A. Kotian, and A. Y. Javaid, "Comparative analysis of simulation and real-world energy consumption for battery-life estimation of low-power IoT (internet of things) deployment in varying environmental conditions using zolertia z1 motes," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Springer International Publishing, 2017, pp. 137–148.

[16] I. Standard, for, Local, and metropolitan area networks, *Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*, IEEE Computer Society Std., 2019.