International Journal of Network and Communication Research, Vol.10, No.1, pp.1-9, 2026
ISSN: ISSN 2058-7155(Print),
ISSN: ISSN 2058-7163(Online)
Website: https://www.eajournals.org/
Published of the European Centre for Research Training and Development UK

Secure Wake-up Radio against Denial-of-Sleep Attacks for Wireless Multi-Hop IoT Networks

Taiki Kirigami[1], Noriko Matsumoto[2], Norihiko Yoshida[3]
[1]NRI Secure Technologies, Ltd., Tokyo, Japan
[2]Kyushu Sangyo University, Fukuoka, Japan
[3]Rissho University, Saitama, Japan

doi: https://doi.org/10.37745/ijncr.16/vol1019 Published August 17, 2025

Citation: Kirigami T., Matsumoto N., Yoshida. (2026) Secure Wake-up Radio against Denial-of-Sleep Attacks for Wireless Multi-Hop IoT Networks, *International Journal of Network and Communication Research*, Vol.10, No.1, pp.1-9

Abstract: *Minimization of energy consumption is critical for wireless IoT networks, in which sensor device nodes are resource-constrained and battery-powered, and communicate over unstable and unreliable radio links. A denial-of-sleep attack is a kind of denial-of-service attacks particular to wireless networks. It forces each node to keep their radio on, exhausts battery-powered devices, and consequently impairs availability of the network. The "Wake-up Token" (WuT) method is the most lightweight countermeasure against the denial-of-sleep attack. Its most promising improvement, SWARD (Secure WAke-up RaDio), was proposed; however, discussed only on a single-hop network. We applied it to multi-hop networks, GPSR and AODV, and examined the feasibility and performance of SWARD.*

Keywords: denial-of-sleep attack, wake-up call, wake-up token, GPSR, AODV

INTRODUCTION

An IoT system includes a network of sensor device nodes as its crucial part to collect data. The network is often wireless, where each device communicates over unstable and unreliable links. The devices are resource-constrained and battery-powered, possibly left unmanaged, while expected to be operational for a long time. A device dies, i.e., cannot function any longer, when its battery is exhausted. Therefore, minimization of energy consumption is critical. Each device turns off its radio interface as soon as network traffic stops sending or relaying.

There are two schemes regarding when and how to turn on and off radio interfaces: scheduled and on-demand. The former assigns time slots to each device node in the net-work for communication, and each node activates its interface during the assigned time slots [1]. This also includes cluster-based synchronization [2]. The latter uses "wake-up radio" (WuR) [3-4]. An ultra-low-power sender/receiver with a low data rate is added alongside the main transceiver in each node and continuously monitors for a "wake-up call" (WuC) delivered from other nodes [5-6]. The former is less efficient than the latter because unnecessary activation with no communication, or idle listening, wastes energy.

There are various types of attacks on wireless IoT networks [7]. An energy-drainage attack is a type of denial-of-service attacks that drains and wastes energy to exhaust battery-powered devices and

consequently impairs the availability of the network [8-9]. The characteristics of wireless IoT networks summarized above incur a new type of energy-drainage attack, i.e., a denial-of-sleep (DoSL) attack [10-11]. It consists in exhausting devices by forcing them to keep their radios on. The scheduled scheme is prone to jamming attacks [12], while the on-demand scheme is vulnerable to forged wake-up radio attacks.

Although defending against the DoSL attacks is an old topic, it is still being vigorously studied, and many methods have been proposed. Some remarkable techniques underlying them are:
(1) authentication and cryptography,
(2) MAC layer protocol modification [13-14],
(3) fuzzy logic [15],
(4) genetic algorithms [16],
(5) trust-based routing [17], and
(6) machine learning [18-19].
The method (2) is difficult to deploy in practice, and (3)-(6) are computationally intensive. The method (1) is further subcategorized into:
(1.1) wake-up tokens [20],
(1.2) one-time passwords [21-22],
(1.3) RSA cryptography [23], and
(1.4) physical unclonable functions [24-25].
The method (1.1) is the most lightweight of software implementations. (1.4) is an interesting hardware solution; however, not common in practice yet.

In consequence, this short paper focuses on the "wake-up token" (WuT) method and its improvements. Among them, SWARD (Secure WAke-up RaDio) [26] in particular is regarded as one of the most promising [27]. The original proposal of SWARD discussed its design only on a single-hop star-shaped network. Therefore, we aimed at applying it to various types of multi-hop IoT networks. This short paper examines the performance of SWARD on some routing protocols used in practice: GPSR (Greedy Perimeter Stateless Routing, position-based) [28] and AODV (Ad hoc On-demand Distance Vector, topology-based) [29]-[30].

The rest of the paper is organized as follows. Section 2 summarizes some background and necessary knowledge, and Section 3 introduces the purpose of this study to apply SWARD to GPSR and AODV. Section 4 presents some simulation-based experiments and examines their results. Section 5 contains concluding remarks and future work.

LITERATURE REVIEW

Wake-up Radio and Wake-up Tokens

As mentioned above, the WuR scheme sends and receives "wake-up call" (WuC) signals or packets via an ultra-low-power transceiver; therefore, the WuC packets must be as small as possible. It may be only a trigger signal without any header or payload; however, an attacker can also send a wake-up signal. The header may be added, which contains the sender address and the destination address; however, the legitimacy of the addresses can only be verified by the main transceiver communication.

Falk et al. proposed a method of "wake-up token" (WuT) to ensure that only legitimate packets can wake up sleeping nodes [20]. A sender transmits a secret WuT to the wake-up radio device of the intended receiver. The receiver's device stores a list of WuT reference values (WuTRVs) that are used to authenticate a received WuT. The device node is activated and uses the main radio for communication only if the WuT matches one in the WuTRVs. An attacker cannot know a WuT in advance; therefore, it cannot activate nodes at will, making DoSL attacks difficult.

A WuT and items in a WuTRV list may be assigned in advance, for example, by applying a hash function to sender and receiver MAC addresses, a wake-up counter, and some secret key as:

$$e = trunc\big(hash(MAC_{send}, MAC_{rcv}, cnt, key)\big)$$

Otherwise, they may be assigned using a hash chain as:

$$e_{n+1} = trunc\big(hash(e_n)\big)$$

where the truncate function is to reduce the WuT size, as well as to hide the entire hash output.

It remains unaddressed how to share the common key in the former and the common initial e_0 in the latter among all the nodes in the network in a confidential manner. This problem should be addressed according to application and situation.

SWARD (Secure WAke-up RaDio)

Montoya et al. proposed an improvement named SWARD (Secure WAke-up RaDio) to generate wake-up tokens [26]. In SWARD, a WuT for the $n+1$-th wake-up is generated from the n-th WuT and the k-th message exchanged by main transceivers between the two nodes during the n-th wake-up according to:

$$WuT_{n+1,long} = hash(WuT_{n,long} \,||\, Msg_{n,k})$$
$$WuT_{1,long} = hash(ScrtKey \,||\, NodeAdrs)$$
$$WuT_n = trunc(WuT_{n,long})$$

where "||" is the concatenation of its two operands. Then the WuT is truncated for authentication. To generate WuT, SWARD includes message data exchanged by main transceivers, assuming that the messages are encrypted when being exchanged. This assumption is not a strong limitation.

As its authors claimed, first, SWARD generates an unpredictable new WuT at every wake-up of a node; second, the token computation is recursive, requiring only local node information; and third, the method is more secure than related ones because it relies on several secret elements rather than only one.

METHODOLOGY

The original proposal of SWARD discussed its design only on a single-hop star-shaped network such that a single central sink node is surrounded by some device nodes. Wireless IoT networks in reality often have a multi-hop (hop-by-hop) structure. ZigBee [31] over IEEE 802.15.4 [32] is a well-known example. To evaluate the feasibility and performance of SWARD more generally, we should try to apply it to some multi-hop IoT networks. Therefore, we selected two multi-hop routing protocols used in practice, GPSR [28] and AODV [29], each of which is one of the most used in each category.

GPSR is a position-based greedy protocol for a network in which each node has its own location information. The outline of the GPSR protocol is as follows. A node forwards a message to the neighbor closest to the destination (Greedy Forwarding). If there is no closer node in the neighbors and the greedy forwarding fails, the "right-hand rule" is applied, in which the node forwards the message to the rightmost neighbor (Perimeter Forwarding). GPSR requires every node to have some reliable GPS or positioning hardware. Also, it requires periodic beaconing to share position data among neighbors. This protocol does not include message broadcasting; therefore, it is highly scalable. However, it does not guarantee end-to-end reachability.

AODV is a topology-based on-demand protocol for a network in which a node does not have its location information. The outline of the AODV protocol is as follows. When a source node needs a route, it broadcasts an RREQ (Route Request) message. Its neighbors who receive the RREQ forward (broadcast) it and set up reverse paths to the source. The destination or an intermediate node with a fresh route sends (unicasts) an RREP (Route Reply) back through the reverse path. AODV, as opposed to GPSR, does not require any positioning hardware or beacon to share position data. Every node maintains routes to guarantee end-to-end reachability.

Each message, including the one for greedy forwarding and perimeter forwarding in GPSR, and the RREQ and RREP in AODV, is accompanied by a WuT of SWARD between the sender and the receiver. There have already been some studies on multi-hop protocols for WuRs and WuCs without authentication [33-35]. They proposed skipping of intermediate hops of WuRs and WuCs in a hop-by-hop sequence of message forwarding for performance improvement. However, a WuT including SWARD requires authentication between the sender and the receiver; therefore, their proposals of the skipping cannot be applied.

We implemented two simulators, one for GPSR and the other for AODV, and conducted some experiments to evaluate the multi-hop SWARD. In the GPSR and AODV networks, respectively, we compared results between the networks using the WuT of the SWARD and the one not using WuT but only WuC. In each simulation cycle, each node performed the procedure outlined as below:

WuC (without authentication) case:

```
if the node has a message to send:
  communicate WuC with its receiver;
  send the message to its receiver;
if the node receives a WuC:
  wake up;
  wait a message and receives it;
estimate power consumption.
```

WuT (with authentication) case:

```
if the node has a message to send:
  communicate WuT with its receiver;
  send the message to its receiver;
if the node receives a WuT:
  authenticate;
  if approved:
    wake up;
    wait a message and receives it;
  otherwise:
    ignore;
estimate power consumption.
```

The common scenario was: a virtual field for the experiments was 300 × 300 square meters (in a virtual sense) wide; in the field, there were 150 device nodes at random locations, a single sink node at the center, and one or more attacker(s) at random locations; and each node had a communication range of 50 meters. Major parameters regarding power consumption are listed in Table 1. Their values were assigned based on previous related studies, including Ullah et al. [14] and Montoya et al. [26].

Table 1. Experiment parameters and assigned values.

Parameter	Value
Initial battery power	0.5 J
Power consumed in active state	13.5 mW
Power consumed in sleep state	0.0015 mW
Power consumed for WuR	54.3 μW
Power consumed in waking-up	0.0043 mW

RESULTS AND DISCUSSION

Figures 1 and 2 examine the number of surviving nodes. The number of attackers is one in Figure 1 and two in Figure 2, respectively. The purple curve represents the GPSR network without WuT, the green is GPSR with WuT, the blue is AODV without WuT, and the yellow is AODV with WuT, respectively.

As the numbers of surviving nodes indicates, AODV consumes more battery power than GPSR when the network is dense because AODV includes RREQ broadcasts. However, in the last stage when the network becomes sparse, AODV outperforms GPSR, due to the so-called "void problem" of GPSR where no closer neighbor exists to the destination.

The WuT improves the battery power consumption both on GPSR and on AODV. Moreover, the WuT brings greater improvement to GPSR than to AODV. This implies that AODV is more durable against the denial-of-sleep attacks. The reason must be that AODV uses RREQ broadcast, and can find a detour route when any neighbor node is dead. As the number of attackers increased, GPSR was getting worse than AODV. This is another sign that GPSR is more prone to denial-of-sleep attacks than AODV, and that the WuT is more effective for GPSR than for AODV. Particularly, both GPSR and AODV networks without WuT in the initial phase until the 1,500th cycle suffer sharp decreases in the numbers. This is because in this phase, the networks establish all the initial routes to deliver data from every node to the sink, and the networks are more prone to the denial-of-sleep attacks.

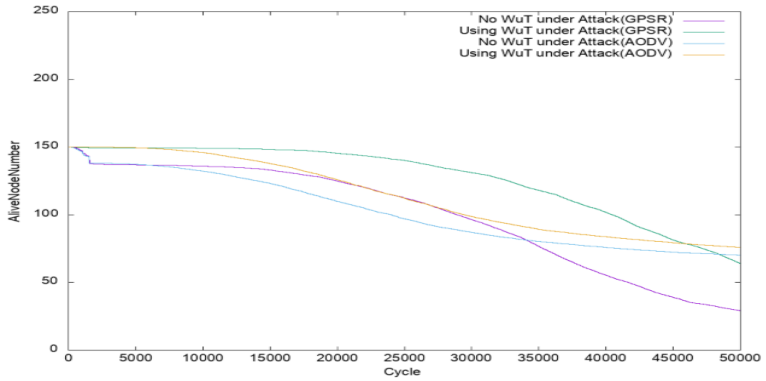

Figure 1. The number of surviving nodes: one attacker case.

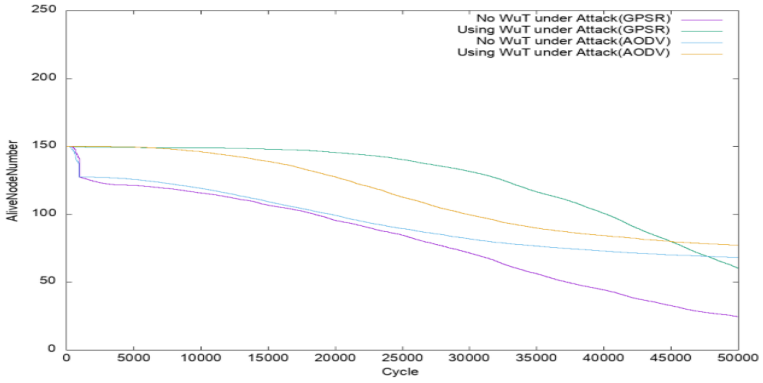

Figure 2. The number of surviving nodes: two attacker case.

Figure 3 and 4 evaluate the message delivery (collection) ratio; the number of attackers is one in Figure 3 and two in Figure 4, respectively. The number of surviving nodes is less in AODV than in GPSR, and this must affect the delivery ratio. The WuT brings improvement to both GPSR and AODV.

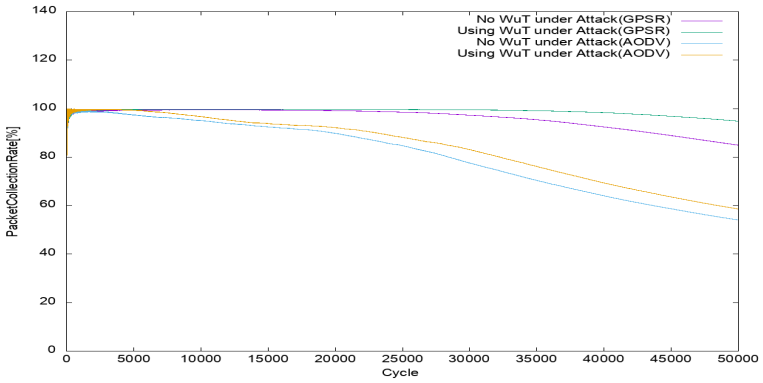

Figure 3. Delivery ratio (%): one attacker case.

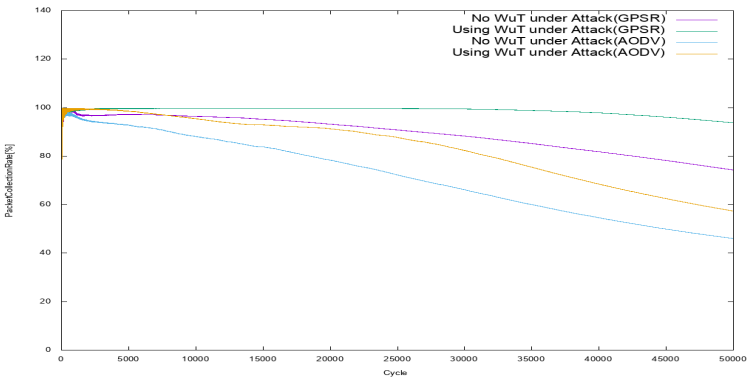

Figure 4. Delivery ratio (%): two attacker case.

CONCLUSION AND FUTURE RESEARCH

This paper applied the WuT method to two kinds of multi-hop networks, and evaluated its effects by comparison. As far as we know, there have been no studies on applying WuT to a position-based routing like GPSR. Our contribution is that this study might be the first attempt to apply the WuT to position-based routing, and consequently the first comparison between it and topology-based routing like AODV. As the result implies, the WuT is more effective for position-based routing than for topology-based routing.

We have obtained some preliminary, yet promising results; however, we are still at the beginning of this research, and there are still many issues that should be addressed. As we mentioned in Section 1, there have been many other methods, including machine learning for example, proposed thus far that are stronger but more computationally intensive. It must be worth investigating the hybrid combination of these new proposals deployed on a central cloud and the lightweight WuT scheme deployed on distributed device nodes. It would also be interesting to combine the software-based WuT and the hardware-based method with the physical unclonable functions.

ACKNOWLEDGMENT

This work was supported by JSPS Grants-in-Aid 23K11071 and 25K15086.

REFERENCES

[1] R. C. Carrano, D. Passos, L. C. S. Magalhaes, and C. V. N. Albuquerque, “Survey and Taxonomy of Duty Cycling Mechanisms in Wireless Sensor Networks”, IEEE Comm. Surveys Tutorials, 16(1), 181-194, 2014.

[2] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”, Proc. 33rd Annual Hawaii Int. Conf. on Sys. Sci., 2, 1-10, 2000.

[3] J. Oller, I. Demirkol, J. Casademont, J. Paradells, G. U. Gamm, and L. Reindl, “Has Time Come to Switch from Duty-Cycled MAC Protocols to Wake-up Radio for Wireless Sensor Networks?” IEEE/ACM Trans. on Networking, 24(2), 674-687, 2016.

[4] M. A. Spohn, C. M. Ranieri, A. R. d. Silva, and J. Ueyama, “A Systematic Review on Wake-Up Radios Applied to Wireless Sensor Networks”, J. of Comp. Sci., 21(3), 566-583, 2025.

[5] F. Z. Djiroun and D. Djenouri, “MAC Protocols with Wake-up Radio for Wireless Sensor Networks: a Review”, IEEE Comm. Surveys Tutorials, 19(1), 587-618, 2017.

[6] D. Ghose, F. Y. Li, and V. Pia, “MAC Protocols for Wake-Up Radio: Principles, Modeling and Performance Analysis”, IEEE Trans. on Industrial Info., 14, 2294-2306, 2018.

[7] Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks”, IEEE Comm. Surv. Tutorials, 8, 2-23, 2006.

[8] F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco, and A. Castiglione, “Energy-Oriented Denial of Service Attacks: an Emerging Menace for Large Cloud Infrastructures”, J. of Supercomp., 71, 1620-1641, 2015.

[9] J. K. Lee, Y. R. Choi, B. K. Suh, S. W. Jung, and K. I. Kim, "A Survey on Energy Drainage Attacks and Countermeasures in Wireless Sensor Networks", App. Sci, 15, 2213, 2025.
[10] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midki, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols", IEEE Trans. on Vehicular Tech., 58, 367-380, 2009.
[11] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of Service Defense for Resource Availability in Wireless Sensor Networks", IEEE Access, 6, 6975-7004, 2018.
[12] A. Gallais, T. H. Hedli, V. Loscr, and N. Mitton, "Denial-of-Sleep Attacks against IoT Networks", Proc. of 6th Int. Conf. on Control, Decision and Info. Tech., 1025-1030, 2019.
[13] N. Ullah, M. S. Chowdhury, M. A. Ameen, and K. S. Kwak, "Energy Efficient MAC Protocol for Low-Energy Critical Infrastructure Monitoring Networks Using Wakeup Radio", Int. J. of Distrib. Sensor Net., 8(4), 15 pages, 2012.
[14] M. Mukhtar, M. H. Lashari, M. Alhussein, S. Karim, and K. Aurangzeb, "Energy-Efficient Framework to Mitigate Denial of Sleep Attacks in Wireless Body Area Networks", IEEE Access, 12, 122918-122928, 2024.
[15] S. Patil and S. Chaudhari, "DoS Attack Prevention Technique in Wireless Sensor Networks", Procedia Comp. Sci., 79, 715-721, 2016.
[16] M. Gunasekaran and S. Periakaruppan, "GA-DoSLD: Genetic Algorithm Based Denial-of-Sleep Attack Detection in WSN", Security and Comm. Networks, 2017, 1-10, 2017.
[17] Z. Yang, L. Li, F. Gu, X. Ling, and M. Hajiee, "TADR-EAODV: A Trust-Aware Dynamic Routing Algorithm Based on Extended AODV Protocol for Secure Communications in Wireless Sensor Networks", Internet of Things, 20(4), 100627, 2022
[18] T. B. Yaseen, A. Tahat, K. Kastell, and T. A. Edwan, "Denial-of-Sleep Attack Detection in NB-IoT Using Deep Learning", J of Telecomm and the Digital Economy, 10(3), 14-38, 2022.
[19] I. Dissanayake, A. Welhenge, and H. D. Weerasinghe, "A Machine Learning Approach to Detect Denial of Sleep Attacks in Internet of Things", IoT, 6(4), 71, 2025.
[20] R. Falk and H. J. Hof, "Fighting Insomnia: A Secure Wake-up Scheme for Wireless Sensor Networks", Proc. 2009 3rd Int. Conf. on Emerging Security Info., Sys. and Tech., 191-196, 2009.
[21] A. Kavoukis and S. Aljareh, "Efficient Time Synchronized One-time Password Scheme to Provide Secure Wake-up Authentication on Wireless Sensor Networks", Int. J. of Adv. Smart Sensor Network Sys, 3(1), 1-11, 2013.
[22] O. Stecklina, S. Kornemann, and M. Methfessel, "A Secure Wake-up Scheme for Low Power Wireless Sensor Nodes", Proc. of 2014 Int. Conf. on Collaboration Tech. and Sys., 279-286, 2014.
[23] R. Fotohi, S. F. Bari, and M. Yusefi, "Securing Wireless Sensor Networks against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol", Int. J. of Comm. Sys., 33, e4234, 2019.
[24] H. Ning, F. Farha, A. Ullah, and L. Mao, "Physical Unclonable Function: Architectures, Applications and Challenges for Dependable Security", IET Circuits, Dev. & Sys., 14(4), 407-568, 2020.
[25] H. T. Lin and Y. Y. Liang, "A PUF-Based Secure Wake-Up Scheme for Internet of Things", Comp. & Security, 110(4), 102415, 2021.

[26] M. Montoya, S. B. Min, A. Molnos, and J. J. A. Fournier, "SWARD: Secure WAke-up RaDio against Denial-of-Service on IoT Devices", Proc. 11th ACM Conf. on Security & Privacy in Wireless and Mobile Net., 190-195, 2018.
[27] R. R. Jenifer and V. S. J. Prakash, "Detecting Denial of Sleep Attacks by Analysis of Wireless Sensor Networks and the Internet of Things", Scientific Temper, 14, 1412-1418, 2023.
[28] B. Karp and H. T. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks", Proc. 6th Annual ACM/IEEE Int. Conf. on Mobile Comp. and Net., 243-254, 2000.
[29] C. Perkins and E. Royer, "Ad-Hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Workshop on Mobile Comp. Sys. and App., 90-100, 1999.
[30] R. H. Jhaveri and N. M. Patel, "Mobile Ad-Hoc Networking with AODV: A Review", Int. J. of Next-Gen. Comp., 6(3), 165-191, 2015.
[31] Connectivity Standards Alliance, Zigbee the Full-Stack Solution for All Smart Devices, 2026.
[32] IEEE C/LAN/MAN-LAN/MAN Standards Committee, IEEE 802.15.4-2024: IEEE Standard for Low-Rate Wireless Networks, 2024.
[33] T. Kumberg, M. Schink, L.M. Reindl, and C. Schindelhauer, "T-ROME: A Simple and Energy Efficient Tree Routing Protocol for Low-Power Wake-Up Receivers", Ad Hoc Net., 59, 97-115.
[34] A. Pegatoquet, T.N. Le, and M. Magno, "A Wake-Up Radio-Based MAC Protocol for Autonomous Wireless Sensor Networks", IEEE/ACM Trans. on Net., 27(1), 56-70, 2019.
[35] N.E.H.Djidi, S. Sampayo, J. Montavont, A. Courtay, M. Gautier, O. Berder, and T. Noel, "The Revenge of Asynchronous Protocols: Wake-Up Radio-Based Multi-Hop Multi-Channel MAC Protocol for WSN", Proc. IEEE Wireless Comm. Net. Conf., 6 pages, 2022