A Novel QoS-Oriented Intrusion Detection Mechanism for IoT Applications

Abdulfattah Noorwali, Ahmad Alvi, Mohammad Khan, Muhammad Javed, Wadii Boulila, Priyadarshini Pattanaik

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9962697, 10 pages
https://doi.org/10.1155/2021/9962697

Research Article

A Novel QoS-Oriented Intrusion Detection Mechanism for IoT Applications

Abdulfattah Noorwali,[1] **Ahmad Naseem Alvi**,[2] **Mohammad Zubair Khan**,[3] **Muhammad Awais Javed**,[2] **Wadii Boulila**,[4] **and Priyadarshini A. Pattanaik**[5]

[1]*Department of Electrical Engineering, Umm Al-Qura University, Makkah 21961, Saudi Arabia*
[2]*Department of Electrical and Computer Engineering, COMSATS University Islamabad, 45550, Pakistan*
[3]*Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia*
[4]*RIADI Laboratory, National School of Computer Science, University of Manouba, Tunisia*
[5]*Image and Information Processing Department, IMT Atlantique, LaTIM Inserm U1101, Brest 29238, France*

Correspondence should be addressed to Wadii Boulila; wadii.boulila@riadi.rnu.tn

Received 3 April 2021; Accepted 4 June 2021; Published 18 June 2021

Academic Editor: Nawab Muhammad Faseeh Qureshi

Wireless sensor network (WSN) is an integral part of Internet of Things (IoT). The sensor nodes in WSN generate large sensing data which is disseminated to intelligent servers using multiple wireless networks. This large data is prone to attacks from malicious nodes which become part of the network, and it is difficult to find these adversaries. The work in this paper presents a mechanism to detect adversaries for the IEEE 802.15.4 standard which is a central medium access protocol used in WSN-based IoT applications. The collisions and exhaustion attacks are detected based on a soft decision-based algorithm. In case the QoS of the network is compromised due to large data traffic, the proposed protocol adaptively varies the duty cycle of the IEEE 802.15.4. Simulation results show that the proposed intrusion detection and adaptive duty cycle algorithm improves the energy efficiency of a WSN with a reduced network delay.

1. Introduction

Internet of Things (IoT) applications use wireless sensor networks (WSNs) to implement several applications in the fields of healthcare, military, environmental monitoring, smart cities, agricultural engineering, etc. WSNs collect sensing data from different areas, generate large data sets, and share it with remote servers for intelligent processing and valuable insights. The data dissemination for IoT applications is shared locally using sensor nodes, then passed to the nearby computing nodes, and finally reached the centralized server, thus forming a reliable multihoming network. WSNs comprise tiny wireless nodes that operate autonomously on a battery with limited energy, so they are required to be energy efficient. Besides, sensor nodes have limited computational capabilities along with low data rates and low processing.

At the data link layer, many medium access control (MAC) algorithms have been proposed in literature that consider these limitations to meet application requirements. The main concerns in these MAC protocols include energy efficiency, delay minimization, and better throughput. These MAC protocols also offer nodes scalability, reliability, and adaptability [1–3].

IEEE 802.15.4 standard was developed to transmit data using low transmit power and low data rate to nearby nodes. It is widely accepted and embedded in the majority of the WSNs [4]. The standard has two operating modes: first is the beacon-enabled mode and second is the non-beacon-enabled mode. The first mode, i.e., beacon-enabled mode, is mostly used for IoT applications. Figure 1 shows the superframe diagram of IEEE 802.15.4. The duty cycle of IEEE 802.15.4 standard is controlled using two variables: first is

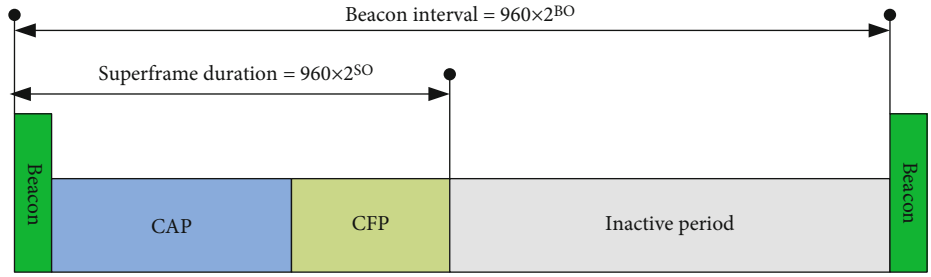

Figure 1: IEEE 802.15.4 standard superframe.

the beacon order (BO) and second is the superframe order (SO). A higher value of BO increases the duration of the beacon known as beacon interval (BI). The active portion of the superframe is controlled by SO. The superframe structure can work in a hybrid manner, using both contention-free access mechanism and also contention-based access technique. Slotted carrier sense multiple access (CSMA/CA) is used for coordinating multiple access during contention-based period. On the other hand, guaranteed time slots are allocated for data transmission without contention.

Most WSN applications use the IEEE 802.15.4 standard due to its hybrid capabilities. Some applications are sensitive in nature, and vulnerability in data delivery is unacceptable [5–7]. Due to its wide utility, the beacon-enabled mode of the standard remains in prime research. Its contention-based and contention-less modes are examined and evaluated in different prospects, such as efficient slot allocation for better link utilization [8–10].

Security issues are the main concern in sensitive WSN and IoT applications such as remote healthcare, traffic safety, and home security; that is why many security measures have been proposed [11, 12]. Most of the solutions are related to encryption to ensure that the intruders should not understand the data. For this purpose, cryptographic techniques are widely used to ensure security of IoT applications and provide data integrity, confidentiality, and privacy [13]. Adversaries try to disturb a wireless network to disrupt communications, especially in highly sensitive applications. Most of these attacks target physical and MAC layers. That is why the IEEE 802.15.4 standard remains a high target point of these adversaries, especially during the contention-based or contention-less periods. These attacks not only reduce the network efficiency of the standard but also decrease the network lifetime.

There are several techniques in the literature to determine the intruder's attacks in different MAC protocols of WSNs. Yu et al. [14] provide a solution to detect spoofing attacks by examining network characteristics. Intrusion attacks that do not occur often are hard to detect, and authors in [15] propose a technique to detect these attacks efficiently. Authors in [16, 17] introduce mechanisms to detect continuous wave jamming signals in the IEEE 802.15.4 standard. Besides these, many other recent techniques focused on intrusion detection [18–20]. Security and intrusion detection is a key component of future IoT applications and 6G technologies [21–23].

Most of the research about intruder's attack detection is based on jamming and spoofing attacks and does not identify the intruder's attacks causing collisions and packet exhaustion. In this paper, an intrusion detection technique is proposed to detect adversaries' attacks in the IEEE 802.15.4. Besides, an adaptive duty cycle algorithm is proposed to meet the QoS. The salient features of our proposed work include the following:

(1) A soft function is developed to compute the probabilities of the collision, successful transmission, and packet exhaustion

(2) An intrusion detection mechanism is developed to detect the collision and exhaustion attacks from this soft function

(3) An adaptive duty cycle algorithm is proposed that works for IEEE 801.5.4 standard and achieves required QoS in a variable traffic scenario

The paper starts by describing the working of IEEE 802.15.4 standard in Section 2, followed by an intrusion detection mechanism in Section 3. The network performance with and without intrusion detection is presented in Section 4. The conclusion of the paper is given in Section 5.

2. IEEE 802.15.4 Working

IEEE 802.15.4 standard is designed for applications that work on low transmission powers and data rates. The standard can work on three frequency bands: first is the 868 MHz, second is the 915 MHz, and last one is the 2.4 GHz. The first two spectrum bands do not need license and offer 1 and 10 frequency channels, respectively. 868 and 915 MHz use the BPSK modulation scheme and data rates of 20,000 and 40,000 bits/sec, respectively. However, 2.4 GHz comprises 16 different frequency channels and uses an O-QPSK modulation scheme by offering a 250,000 bits/sec data rate. A comparative table of all these frequency bands is given in Table 1.

The standard offers both ad hoc and centralized controlled network. In an ad hoc manner, nodes send their information with each other using an unslotted CSMA/CA-based multiple access algorithm. In a centralized network, a superframe architecture is used that has active and inactive periods. The coordinator issues a beacon frame, and IoT nodes turn on their transceivers to receive the message and

Table 1: Frequency spectrum of IEEE 802.15.4 standard.

Frequency spectrum (MHz)	Modulation scheme	Symbols rate	Symbols rate	Number of channels	Bit duration (sec)
868	BPSK	20k	20k	1	$50 * 10^{-6}$
915	BPSK	40k	40k	10	$25 * 10^{-6}$
2400	O-QPSK	62.5k	250k	16	$4 * 10^{-6}$
868	BPSK	20k	20k	1	$50 * 10^{-6}$

keep them synchronized. The active period known as superframe duration (SD) contains 16 equal duration slots. SD includes transmission of the beacon frame, transmission of data using contention access period (CAP), and data dissemination in the contention-free period (CFP). Out of these 16 time slots, beacon and CAP can use 9 or more slots, whereas CFP can be allocated at most 7 slots.

The coordinator periodically generates beacon frames. Nonmember nodes that intend to become a member of the network must wait for the beacon to know the CAP period to transmit their joining requests to the coordinator. The data requests of IoT nodes are processed during CAP, and the coordinator then allocates guaranteed time slots (GTS) to these IoT nodes. Those nodes that are not allocated GTS can transfer their data during CAP by following the multiple access slotted CSMA/CA protocol. That is why the superframe structure has a mandatory portion of CAP where nodes send their requests and data by applying a slotted CSMA/CA algorithm.

2.1. Slotted CSMA/CA Working. During CAP, the coordinator keeps its radio on to receive and respond to all the requests originated by the nodes. All nodes that intend to send any requests or transmit data during CAP use the slotted CSMA/CA protocol to confirm the idleness of the medium. The slotted CSMA/CA comprises three main parameters, named NB, BE, and CW.

Parameter NB is the maximum number of times a node can check medium availability for transmission. The default value of NB is in the range of 0 to 4, which means the maximum attempts to assess the medium availability is 5 when NB is 4. If a node does not find medium free even after NB, it informs the upper layer about channel access failure.

Parameter BE is backoff exponent, and its default value ranges from 3 to 5. It determines a random wait time that the node takes before checking the medium availability for transmission. The random range of the backoff period is always in the range of 0 to $2^{BE} - 1$. In case the medium is busy, it increments its value by 1 until the maximum value is reached. For an initial value of 3, a node should wait for any random value of backoff periods between 0 and 7. The maximum default backoff period for a node to wait before checking medium availability in this standard is 31 backoff periods.

Parameter CW stands for the contention window with a default value of 2. It decrements by 1 whenever finding the channel idle and reset to its initial value of 2 by finding the channel busy. Nodes can send their data when the value of CW becomes 0. This allows the nodes to confirm the channel idle by applying the clear channel assessment (CCA). CSMA/CA flow diagram of CSMA/CA is presented in Figure 2.

When data is transmitted, then the node waits for the acknowledgment. Suppose it could not receive within a specified time. In that case, the same frame is transmitted again until it exceeds the maximum frame retries limit, which has been defined in a MaxFrameRetries parameter.

Most of the adversaries do not follow the algorithm and do not follow the standard policies, severely disturbing the network quality by transmitting the smaller or longer stream of packets in the medium. A description of different adversary attacks on IEEE 802.15.4 standard is given in the following section.

2.2. Attacks on the IEEE 802.15.4 Standard. This section describes some of the intruder's attacks on the standard, which ultimately affects the WSN performance. The following three attacks are quite common and disturb either CAP, CFP, or both.

(i) Exhaustion attack (CAP)

(ii) Collision attack (CAP+CFP)

(iii) Unfairness attack (CFP)

2.2.1. Exhaustion Attack. In most WSN applications, legitimate nodes are deployed in an open environment. In the IEEE 802.15.4 standard, each member node applies a slotted CSMA/CA algorithm before sending its packet to other nodes or coordinator. Suppose it could not send its packet due to the channel busy after exceeding its threshold limits as described in the algorithm. In that case, it reports the channel access failure to its upper layer, and the coordinator gets this information through an indirect data transfer method. After completing their backoff counter, each requesting node detects the channel availability by performing a clear channel assessment (CCA). Adversaries keep the channel busy by sending a long stream of messages. Due to these attacks, legitimate nodes always find the channel busy in each CCA operation and find channel access failure after exceeding its retry limits. Besides, when a node transmits its packet and could not receive its acknowledgment, it must resend the packet repeatedly till its maximum limit and then finally declares that the packet cannot be transmitted.

2.2.2. Collision Attack. The collision occurs when a node communicates with another node while the third node sends packets on the same frequency channel. In the IEEE 802.15.4

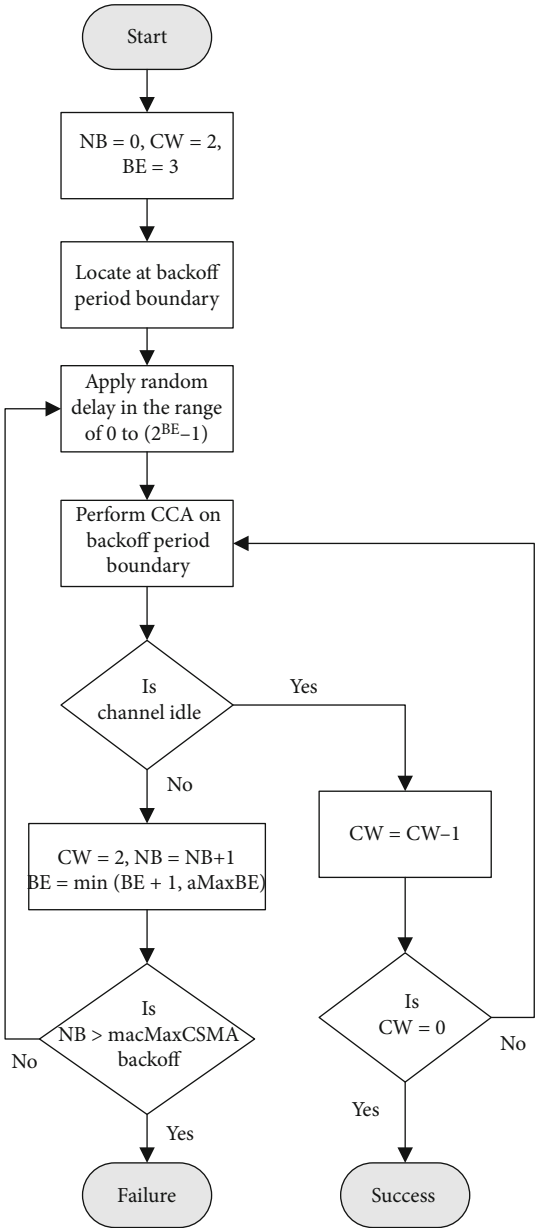

Figure 2: CSMA/CA mechanism of IEEE 802.15.4 standard.

standard, nodes transmit their information with and without contending the medium with other nodes during CAP and CFP, respectively. Adversaries intentionally transmit small packets during these transmissions that cause the collision, and nodes must resend their packets from scratch. This retransmission consumes energy and increases the transmission delay, and ultimately, the quality of service is compromised.

2.2.3. Unfairness Attack. The standard allocates GTS to data requesting nodes on a first-come, first-served basis. All the data requesting nodes have equal chances of generating their request during CAP as they are required to observe the clear channel availability after decrementing the backoff period. The adversary node does not follow the backoff period and sends its data request soon after the beacon frame. The coordinator receives GTS requests from the adversaries before other legitimate requests and allocates GTS before the adversaries compared to the legitimate nodes.

Most of the adversary attacks are during CAP because they cannot be determined easily. In this work, an intrusion detection mechanism is proposed specifically for CAP of the IEEE 802.15.4 standard by identifying collision and exhaustion attacks. Besides, an adaptive duty cycle algorithm is proposed that allows the coordinator to adjust its duty cycle to meet the QoS.

3. Proposed Scheme

This work helps the coordinator to determine the intruder's attack and satisfies the QoS by introducing two different algorithms. The first algorithm checks whether the QoS is compromised due to an intruder's attack or not. In case there are no intruder's attacks, the second algorithm allows the coordinator to adjust its duty cycle to satisfy its QoS.

3.1. Intrusion Detection Mechanism. In this section, a mechanism for intrusion detection in the IEEE 802.15.4 standard is proposed based on the following inputs:

(1) Collision ratio (CR): number of collisions detected against the total packets transmitted by a node per second

(2) Packet successful transmission ratio (PST): ratio of packets received at destination to the packets transmitted by the source node

(3) Request ratio (RR): ratio of the number of requests generated by the nodes to the coordinator's requests per second

A soft function is designed to find out the probability of collision (PC), probability of successful transmission (PS), and probability of exhaustion (PE) from input values of CR, PST, and RR, respectively, as follows:

$$Y(V) = \frac{1}{1 + \exp\{-E * (V - F)\}}. \quad (1)$$

Here, $Y(V)$ gives the probability of collision, successful transmission, and exhaustion from this soft function when we input CR, PST, and RR values by putting these values against V in the soft function. E in this soft function is the slope parameter, and F is the center of the curve.

The shape of the curve depends upon the values of E and F, and their values can be determined by a cost function as follows:

$$J(V) = (Y_D - Y)^2. \quad (2)$$

Here, Y is the actual value and Y_D is the desired value.

Input: Collision Ratio *CR*, Packet Successful Transmission ratio *PST*, Request Ratio *RR*
Calculate $PC = 1/[1 + exp\{-E\times(CR - F)\}]$
Calculate $PS = 1/[1 + exp\{-E\times(PST - F)\}]$
Calculate $PE = 1/[1 + exp\{-E\times(RR - F)\}]$
Calculate $Z_1 = (PS\times\varphi) + (PC\times\theta)$
Calculate $Z_2 = (PS\times\varphi) + (PE\times\theta)$
if $Z_1 > Th$
Collision attack found
else
No Collision attack
if $Z_2 > Th$
Exhaustion attack found
Else
No Exhaustion attack

Algorithm 1: Intruder detection algorithm.

Values of E and F change periodically. If E_N and F_N are their current values, then their next stages E_{N+1} and F_{N+1} can be determined from their current values as follows:

$$E_{N+1} = E_N + \varnothing * \frac{\partial J}{\partial E}, \tag{3}$$

where $\varnothing$ ranges from 0 to 1 and $\partial J/\partial E$ is calculated as follows:

$$\frac{\partial J}{\partial E} = 2(Y_D - Y)\frac{E_N}{[1 + \exp\{-E_N * (V - F_N)\}]^2}. \tag{4}$$

And F_{N+1} is calculated as follows:

$$F_{N+1} = F_N + \varnothing * \frac{\partial J}{\partial F}. \tag{5}$$

Here, $\partial J/\partial F$ is calculated as follows:

$$\frac{\partial J}{\partial F} = 2(Y_D - Y)\frac{-E_N * \exp[-E_N * (V - F_N)]}{[1 + \exp\{-E_N * (V - F_N)\}]^2}. \tag{6}$$

The more the number of iterations to find out the next stages of E and F, the steeper the curve will be.

After finding out the probabilities of collisions, successful transmissions, and exhaustion from input values of CR, PST, and RR, respectively, intruder's attacks can be determined as shown in Algorithm 1. This algorithm detects collisions and exhaustion attacks of the intruders.

3.1.1. Collision Attack Detection. Algorithm after determining collisions and successful transmission probabilities from the soft function scale them by φ and θ, respectively. Both scaled values are summed up and then compared with the threshold value. In case the summed value is greater than the threshold value, an attack is found; else, no attack is found.

3.1.2. Exhaustion Attack Detection. Adversary exhaustion attacks are detected from the probability of exhaustion and successful transmission probability. Like the above criteria, the probability of success is summed individually with the probability of exhaustion and compared with the threshold. The threshold is set, and then, this summation result is compared with the threshold. If the sum is greater than the threshold, an attack is found; else, no attack is found.

3.2. Duty Cycle Adjustment Algorithm. In case the intruder detection algorithm could not detect the adversary's involvement and the system still feels that QoS is compromised, the coordinator's duty cycle needs to be adjusted to satisfy the QoS. This algorithm allows the coordinator to adjust its duty cycle to meet the QoS. In case the member of nodes is increased and requires more data requests, an increase in the active period is achieved. Similarly, when there is less data in a network, then the active period needs to shrink. IEEE 802.15.4 standard does not discuss the adaptation in the duty cycle according to the QoS requirement. This algorithm allows the coordinator to adjust its duty cycle to meet the QoS of the network.

The algorithm improves the data transmission by improving the throughput and reduces the number of collisions. The algorithm allows the coordinator to test QoS during the last BI and make proper adjustments in the next BI. It is expected that the data required to receive by the coordinator is half of its maximum capacity. In case the received data is less than this threshold value, then it may be due to an increased number of collisions, as shown in Figure 3.

If QoS is compromised only due to low throughput, then the algorithm allows the coordinator to adjust the duty cycle as follows:

(i) If the difference between BO and SO is more than 1 and SO is greater than 0, then the BO and SO's parameter value will be reduced in the next BI. This decreases the active duration that allows nodes to send their data in less time, resulting in increased throughput

(ii) In case the difference between BO and SO is greater than 1, however SO is 0, then BO will be reduced without any change in SO. This decrease in BO reduces the inactive period, and consequently, nodes' waiting time is reduced

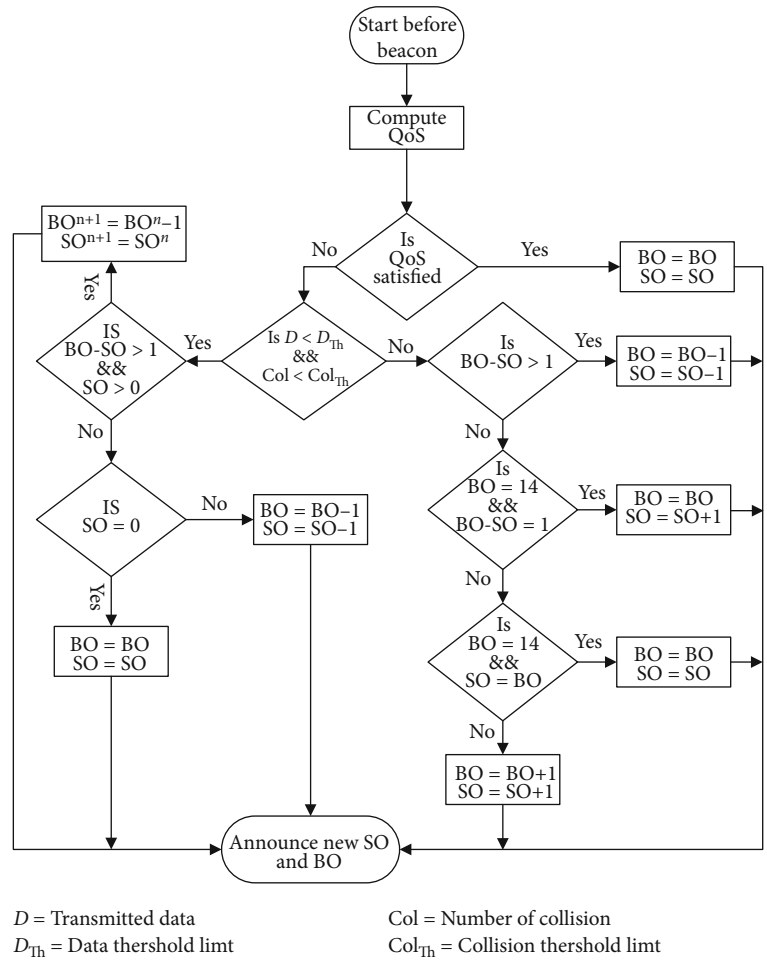

Figure 3: Proposed adaptive duty cycle adjustment.

(iii) If the difference between BO and SO is 0 and SO is greater than 1, then SO's next value is decremented without any change in BO. The decrease in SO results in a reduced active period, and hence, the throughput is increased

(iv) If the difference in BO and SO is 0 and SO's value is 0, then they remain unchanged during the next BI. This is the scenario when data traffic in a network is very small

If there is an increased number of collisions during BI, it may reduce the throughput. This increase in the collision may occur due to insufficient active duration, and there is a requirement to increase the active period so that nodes have more time to send their data requests. Following are the criteria for adjusting the parameter values of SO and BO.

(i) If the difference between BO and SO is greater than 0 and BO is less than 14, then both SO and BO will be increased in the next BI

(ii) In case BO approaches its maximum limit of 14, and the difference between BO and SO is 0, then SO will be increased without any change in BO value

Table 2: Parameter values.

Parameters	Values
Number of nodes	10
Network size	100
Data rate (kbps)	250
Legitimate nodes	15
Intruder nodes	5
Sink node	1
Superframe duration (msec)	122.88
Beacon interval (msec)	245.76
Duty cycle (%)	50
Transmitting energy (mJ)	50
Receiving energy (mJ)	30
Idle energy (mJ)	5
Offered load (kbytes)	1 : 1 : 10

(iii) If both SO and BO are 14, then the next SO and BO value will remain unchanged as it is already on its maximum limit

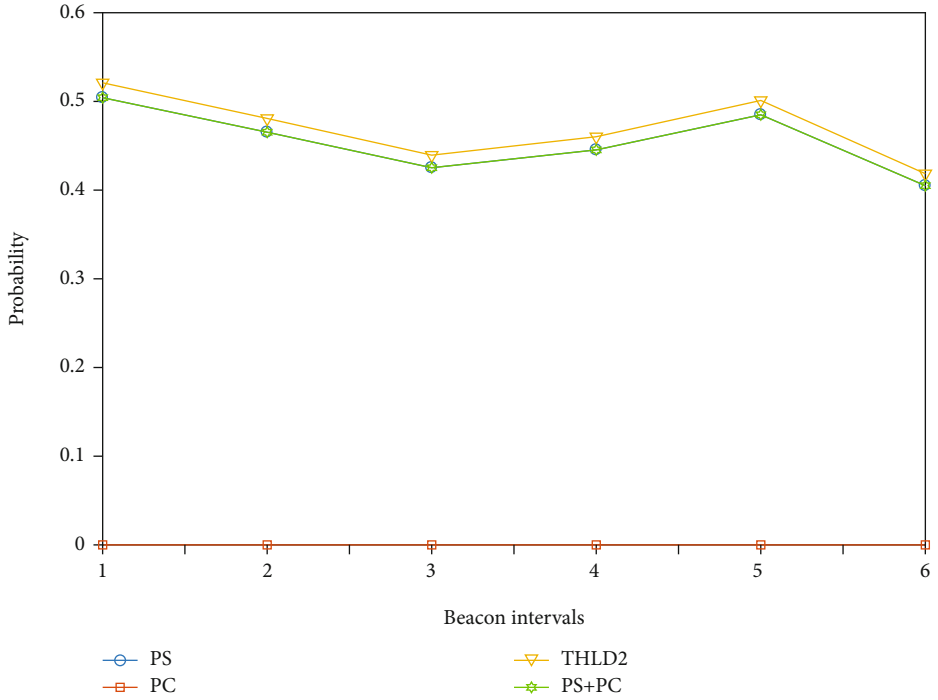

Figure 4: Scenario when no attack found against beacon intervals.

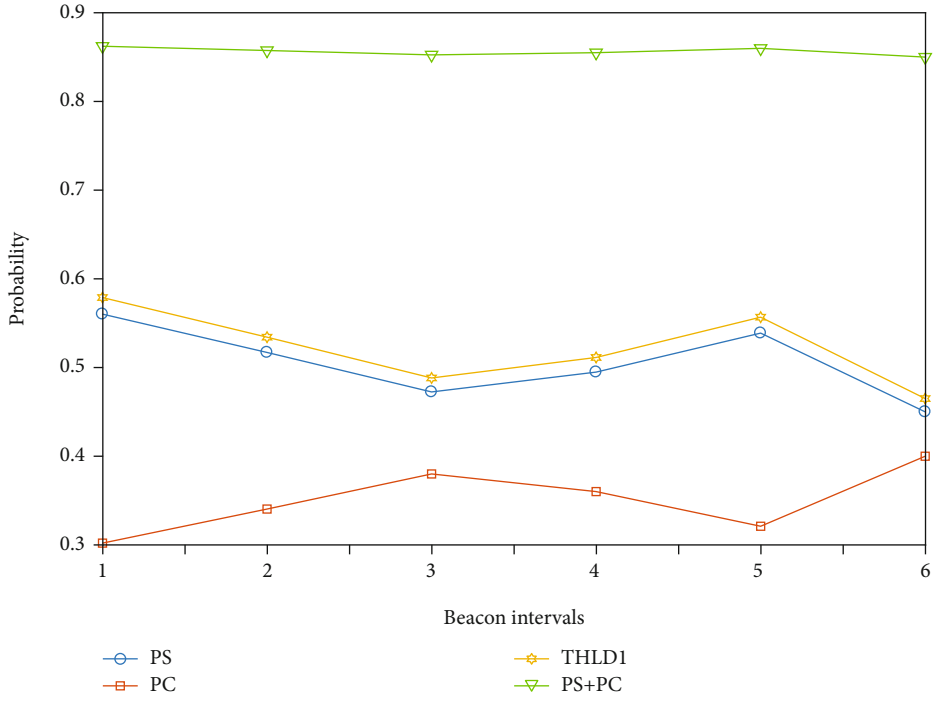

Figure 5: Collision attack detection against beacon intervals.

(iv) If BO is less than 14 with a 100% duty cycle, then we have the flexibility to increase the SO. However, we must increase the value of BO to meet the standard permissible requirements

4. Analysis and Results

In this section, the proposed scheme is evaluated by developing a simulation environment in MATLAB, as shown in

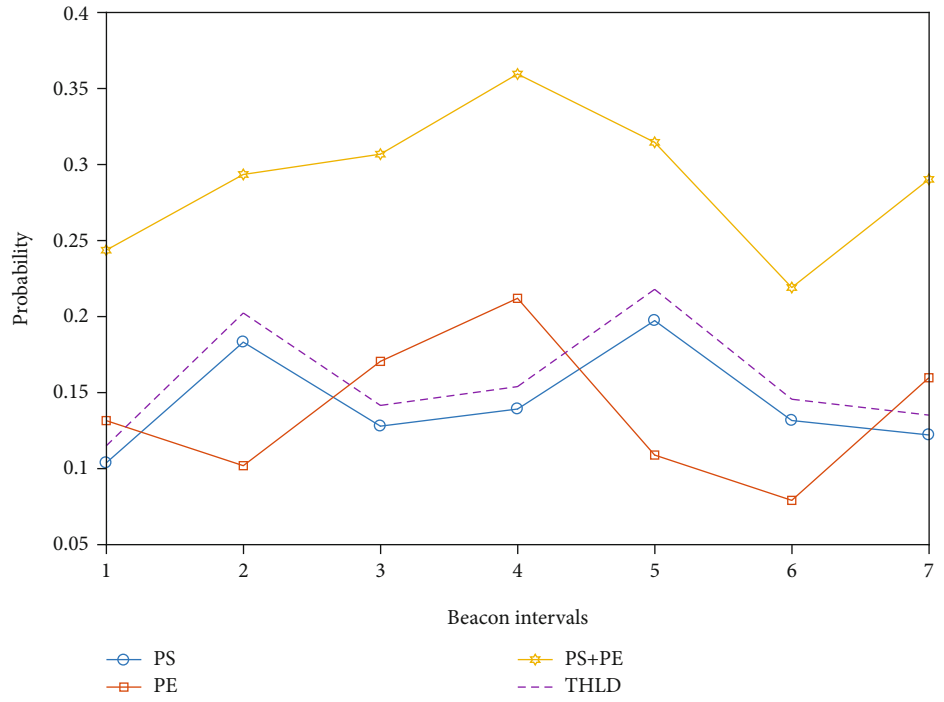

Figure 6: Exhaustion attack detection.

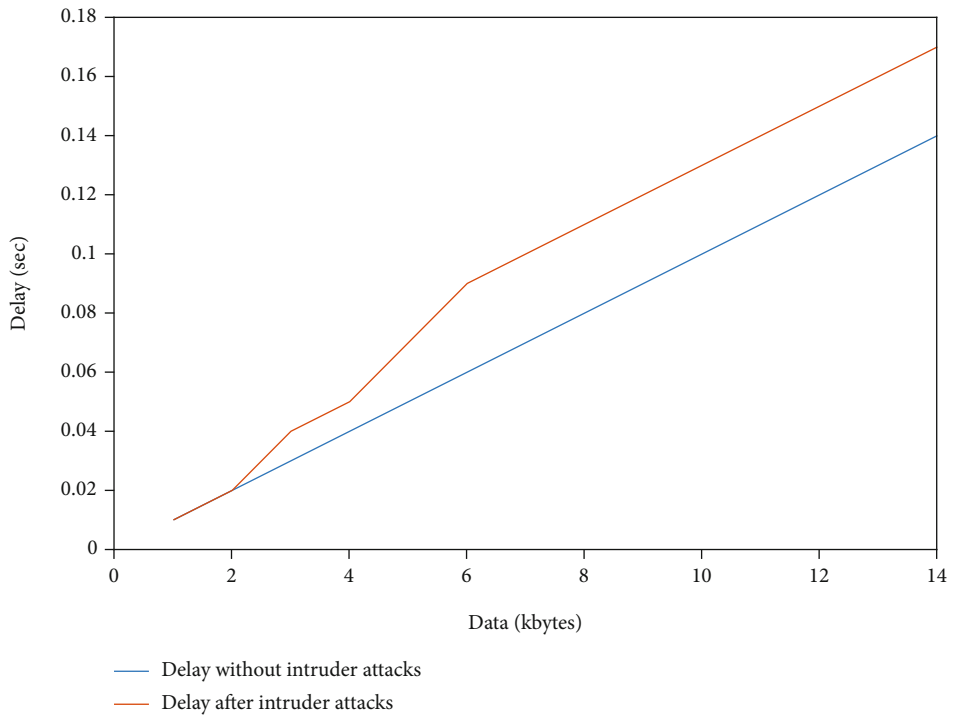

Figure 7: Transmission delay with and without intruder's attack.

Table 2. The proposed scheme detects intruder's attack by exposing collision and exhaustion probabilities as described in Section 3.

Results shown in Figure 4 describe the scenario when there is no intruder's attack found. In this case, the probability of successful transmission is maximum, and the probability of collision is 0. The sum of both probabilities is less than the threshold, and hence, no collision detection is found in this case. However, the probability of collision and successful transmission increases in the presence of an intruder's attack

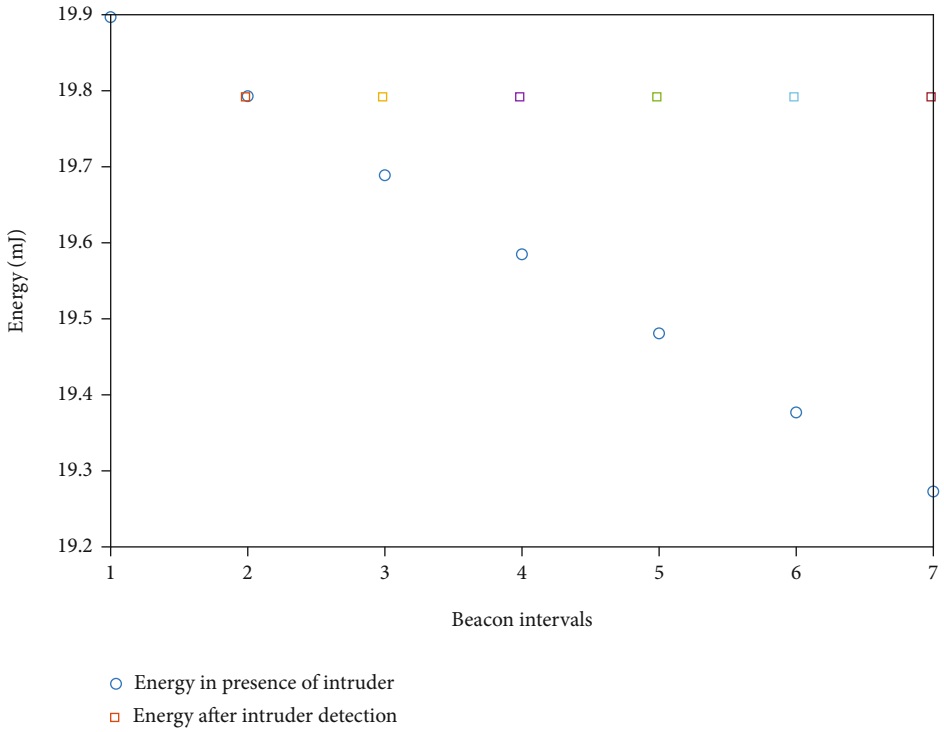

Figure 8: Energy consumed by the node for intrusion detection.

and is verified by the results shown in Figure 5. It is evident from the results that the probability of successful transmission depends upon the probability of collisions. In the 3rd and 5th beacon intervals, the probability of successful transmission decreases with the increase in collision probability.

Figure 6 shows the probabilities of exhaustion attack in the presence of intruders for different beacon intervals. It is evident from the results that whenever exhaustion probabilities increase from the threshold, our proposed scheme detects the presence of intruders.

Delay transmission is calculated as the time duration when a node has data to transmit and successfully transmits its data to the coordinator or sink. Network delay is the accumulated delay of all the nodes in a network. Figure 7 shows the amount of delay experienced by the nodes in the presence and absence of an intruder's attack. It is evident from the results that network delay in the presence of an intruder's attack is much more than the delay without an intruder's attack. This is due to the retransmission of the crushed packet.

Figure 8 shows a comparative analysis of energy consumed by a node, when it detects intruder's attacks and stops transmission, and when it could not detect an intruder and keep on transmitting packets again and fruitlessly wasting its energy.

5. Conclusion

IoT applications generate big data for remote sensing applications and thus vulnerable to adversaries, and server attacks which can severely damage the network performance and QoS may be compromised. In this work, an intrusion detection mechanism is proposed to detect intrusion possibilities by developing a soft function for the IEEE 802.15.4 standard. The proposed intrusion detection mechanism detects the collision and exhaustion attacks during different stages of the standard's superframe. Besides, if QoS is compromised due to generation of large data, then the duty cycle adaptation algorithm is proposed to meet the QoS requirements. The results verify that the proposed scheme successfully detects these intrusions, and this detection minimizes the WSN delay and energy consumption. Although the proposed intrusion detection mechanism detects the most common intruder's attacks, it does not work when adversaries attack the IoT nodes unfairly. The future work will explore efficient intrusion detection mechanisms for unfair attacks.

Data Availability

Data is available on request from the corresponding author.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: 19-ENG-1-01-0015.

References

[1] S. Khan, A. N. Alvi, M. A. Javed, B. Roh, and J. Ali, "An efficient superframe structure with optimal bandwidth utilization and reduced delay for Internet of Things based wireless sensor networks," *Sensors*, vol. 20, no. 7, p. 1971, 2020.

[2] M. Zheng, C. Wang, M. du, L. Chen, W. Liang, and H. Yu, "A short preamble cognitive MAC protocol in cognitive radio sensor networks," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 6530–6538, 2019.

[3] S. Khan, A. N. Alvi, M. A. Javed, S. H. Bouk, and S. H. Bouk, "An enhanced superframe structure of IEEE 802.15.4 standard for adaptive data requirement," *Computer Communications*, vol. 169, pp. 59–70, 2021.

[4] A. N. Alvi, S. Khan, M. A. Javed et al., "OGMAD: optimal GTS-allocation mechanism for adaptive data requirements in IEEE 802.15.4 based Internet of Things," *IEEE Access*, vol. 7, pp. 170629–170639, 2019.

[5] R. Zhu, M. Yu, Y. Li, J. Wang, and L. Liu, "Edge sensing-enabled multistage hierarchical clustering deredundancy algorithm in WSNs," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6664324, 14 pages, 2021.

[6] H. Wang, L. Wu, Q. Zhao, Y. Wei, and H. Jiang, "Energy balanced source location privacy scheme using multibranch path in WSNs for IoT," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6654427, 12 pages, 2021.

[7] W. Zhang, W. Fang, Q. Zhao, X. Ji, and G. Jia, "Energy efficiency in Internet of Things: an overview," *Computers, Materials & Continua*, vol. 63, no. 2, pp. 787–811, 2020.

[8] S. Gong, X. Liu, K. Zheng, X. Tian, and Y. Zhu, "Slot-hitting ratio-based TDMA schedule for hybrid energy-harvesting wireless sensor networks," *IET Communications*, vol. 14, no. 12, pp. 1949–1956, 2020.

[9] Y. Li, X. Zhang, J. Zeng, Y. Wan, and F. Ma, "A distributed TDMA scheduling algorithm based on energy-topology factor in Internet of Things," *IEEE Access*, vol. 5, pp. 10757–10768, 2017.

[10] R. A. Lara-Cueva, R. Gordillo, L. Valencia, and D. S. Benítez, "Determining the main CSMA parameters for adequate performance of WSN for real-time volcano monitoring system applications," *IEEE Sensors Journal*, vol. 17, no. 5, pp. 1493–1502, 2017.

[11] E. B. Hamida, M. A. Javed, and W. Znaidi, "Adaptive security provisioning for vehicular safety applications," *International Journal of Space-Based and Situated Computing*, vol. 7, no. 1, pp. 16–31, 2017.

[12] M. A. Javed, E. B. Hamida, A. al-Fuqaha, and B. Bhargava, "Adaptive security for intelligent transport system applications," *IEEE Intelligent Transport Systems Magazine*, vol. 10, no. 2, pp. 110–120, 2018.

[13] A. Haider, M. Adnan Khan, A. Rehman, M. U. Rahman, and H. Seok Kim, "A real-time sequential deep extreme learning machine cybersecurity intrusion detection system," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1785–1798, 2021.

[14] J. Yu, E. Kim, H. Kim, and J. H. Huh, "Design of a framework to detect device spoofing attacks using network characteristics," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 34–40, 2020.

[15] E. Yang, G. Prasad Joshi, and C. Seo, "Improving the detection rate of rarely appearing intrusions in network-based intrusion detection systems," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1647–1663, 2021.

[16] M. Eskandari, Z. H. Janjua, M. Vecchio, and F. Antonelli, "Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6882–6897, 2020.

[17] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.

[18] M. Mittal and S. Vijayal, "Detection of attacks in IoT based on ontology using SPARQL," in *2017 7th International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 206–211, Nagpur, India, 2017.

[19] M. Mittal, L. K. Saraswat, C. Iwendi, and J. H. Anajemba, "A neuro-fuzzy approach for intrusion detection in energy efficient sensor routing," in *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp. 1–5, Ghaziabad, India, 2019.

[20] M. Mittal, C. Iwendi, S. Khan, and R. Javed, "Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system," in *Transactions on Emerging Telecommunications Technologies*, John Wiley & Sons, Ltd., 2020.

[21] U. M. Malik, M. A. Javed, S. Zeadally, and S. U. Islam, "Energy efficient fog computing for 6G enabled massive IoT: recent trends and future opportunities," *IEEE Internet of Things Journal*, 2021.

[22] N. U. H. Lodhi, A. Malik, T. Zulfiqar, M. A. Javed, and N. S. Nafi, "Performance evaluation of Wi-Fi finger printing based indoor positioning system," in *2018 IEEE Conference on Wireless Sensors (ICWiSe)*, pp. 56–61, Langkawi, Malaysia, 2018.

[23] M. A. Javed and S. Zeadally, "RepGuide: reputation-based route guidance using Internet of Vehicles," *IEEE Communications Standards Magazine*, vol. 2, no. 4, pp. 81–87, 2018.