International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 3, June 2020, pp. 2589~2599
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i3.pp2589-2599

Security-aware fair transmission scheme for 802.11 based cognitive IoT

Hayoung Oh
DASAN University College, Ajou University, South Korea

Article Info

Article history:

Received Mar 29, 2019
Revised Nov 24, 2019
Accepted Dec 9, 2019

Keywords:

Cognitive IoT
DCF (distributed coordination function)
IEEE 802.11
Queue management
Security-aware fair transmission

ABSTRACT

Cognitive IoT is exponentially increased because of various real time and robust applications with sensor networks and big data analysis. Each IoT protocol of network layer can be RPL, COAP and so on based on IETF standards. But still collision problems and security-aware fair transmission on top of scalable IoT devices were not solved enough. In the open wireless LAN system based cognitive IoTs, IoT node that is continuously being stripped of its transmission opportunity will continue to accumulate packets to be sent in the butter and spoofing attacks will not allow the data transfer opportunities to be fair. Therefore, in this paper, we propose a method to reduce the average wait time of all packets in the system by dynamically controlling the contention window (CW) in a wireless LAN based cognitive IoT environment where there are nodes that do not have fair transmission opportunities due to spoofing attacks. Through the performance evaluation, we have proved that the proposed technique improves up to 80% in terms of various performance evaluation than the basic WLAN 802.11 based IoT.

Corresponding Author:

Hayoung Oh,
DASAN University College, Ajou University,
Suwon 16499, South Korea.
Email: hyoh79@gmail.com

1. INTRODUCTION

With the development of cognitive IoTs (CIoTs) [1] with sensors and big data analysis [2], real time and robust applications are exponentially attended all over the world [3-8]. Even though those techniques were famous with the reflection of IETF standards such as Orchestra [9], RPL (IPv6 Routing Protocol for Low power and Lossy Networks) [10], TSCH (Time Slotted Channel Hopping MAC) [11] and COAP enough years ago, the exact and strict solutions for secure wireless transmission of cognitive IoTs were not provided in the research and other areas in practice.

In the 802.11 protocol, the concept of a fundamental mechanism for accessing media is DCF. The DCF is a standard CSMA/CA access mechanism, back-off time is used to avoid collisions by checking whether the wireless channel is empty before the transmission. In DCF, the more nodes competing, the more likely it is that collisions will occur and the transmission will not be fair. Many researches has been done to solve this problem. But those were not considered in CIoTs environment enough. For example, when a collision occurs, the backoff of the corresponding node exponentially increases, the backoff of other nodes increases linearly [12, 13], and when the transmission is completed, a new backoff algorithm that linearly reduces the backoff of all nodes. A method of allocating different CW values according to the number of collisions occurring in the nodes is proposed [14].

Figure 1 shows Media Access Control (MAC) Layer 2 attacks in 802.11 based CIoT. An attacker of MAC can transmit packets using a spoofed source MAC address of an access point at any time. The recipient of these spoofed frames has no way of identifying if they are legitimate or illegitimate requests and will process them. The ability to transmit spoofed management frames causes MAC layer DoS attacks on an open

wireless 802.11 network. In case of the node of recipient of the spoofed frames, it cannot utilize the 802.11 channel fairly different from those of recipient of the spoofed frames. In this paper, we improve a performance by giving the fair transmission of 802.11 based CIoT node with the highest score the opportunity to transmit the packet. That is, the higher score is considered with the number of packets in the output queue as well as the longer the waiting time of the packet in the output queue on top of the probability of recipient of the spoofed frames.

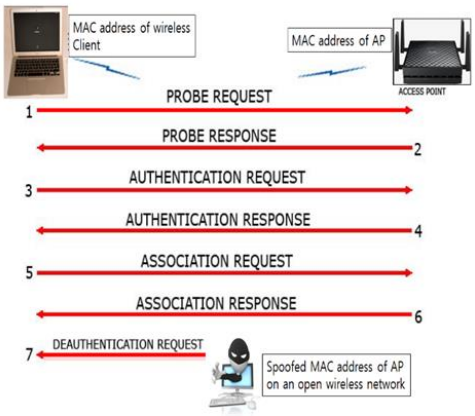


Figure 1. Media access control (MAC) Layer attacks in 802.11 based CIoT

2. RELATED WORK

2.1. IoT (internet of thing)

Internet of things (IoT) not only push the nodes to sense radio channel for hearing wireless medium, it also does provide an opportunity to learn and adapt about the radio and neighborhood. As number of IoT nodes cherish, spectrum scarcity and interference management becomes very important. As 802.11 radios are vital frontrunners to realize IoT technology, 802.11 channel access algorithms at MAC layer in IoT nodes play a vital role to attain maximum achievable throughput [5].

Authors of [5] proposed a novel interference and spectrum aware channel access mechanism for 802.11 infrastructure and adhoc network based on perceived RSSI, RCPI and SNR metrics by generating signal-strength-snr graph to combat interference. The method also uses concept of adaptive channelization to address effective spectrum management. Authors of [6] introduced the concept of Green Internet of Things (G-IoT) as one of the most important roles on the way to create a green and sustainable place for living with the big data analysis. It is essential in achieving valuable insights from voluminous and various G-IoT generated data in the process of creating cities where the quality of life toward the fruition of smart and sustainable city vision.

Compared with the representative IoT related various protocols such as RPL[10], TSCH [11], Orchestra achieves local and autonomous scheduling without a centralized and a distributed scheduler [9]. The Wireless HART [15, 16] and ISA100.11a [17] are rely on a centralized scheduling entity. Different from the IETF 6TiSCH working group [18] on top of the negotiation between neighbor nodes, Orchestra IoT nodes employ simple periodic schedules and update the schedules automatically and temporally considering the routing topology.

In LLSF (Low Latency SF) [19], the authors focus on the proper time of a node schedule/ unschedule timeslots to its neighbor and which timeslots usage. The SF daisy-chains timeslots consider a multi-hop path when a node receives a packet in a slot with an immediate retransmission in the next slot. The LLSF reduces the end-to-end latency on a 5-hop path by 82.8% compared to SF0, with no additional overhead. In [20], the authors exploit the statistical information of CR licensed users' activities, fading conditions, and jamming attacks over idle channels. They use a security- availability- and quality-aware channel assignment with providing communicating CR pair with the most secured channel of the lowest invalidity ratio. Authors of [21] proposed the methodology for spectrum sharing and access problem in a multidevice single-transceiver CR IoT network with time-critical applications under jamming attacks. They maximize the number of simultaneous served IoT devices over all available idle channels while ensuring delay requirement, hardware, link quality, security attacks, and spectrum utilization constraints. In [22], they define an Edge Centric Context Sharing Architecture for providing context-aware security by

using shared context information and discuss the challenges in the context-aware security area in detail. The authorsof [23] cover the Internet of Things security and examine IoT conventions, potential dangers, vulnerabilities, misuse, information breaks, security system and alleviation. The authors of [8] introduce the definition of cognitive IosT first as shown in Figure 2. Similar to the sensor nodes, surely IoT node can sense the environment such as the remaining wireless resources on top of the cognitive components. Different from IoT, IosT means Internet of small Things. It considers the more distance with the small usage of energy when the IosT node (re)transmits or store the data in a specific area. In this paper, in 802.11 environments based IoT, we first consider the cognitive function of IoT for recognizing the self queue and propose Self-Dynamic Tx Control based Security-Aware Fair Transmission in 802.11 based on Cognitive IoT.

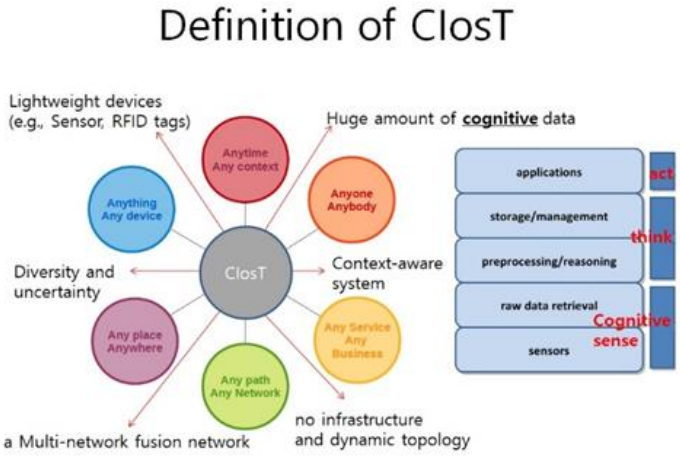


Figure 2. Definition of CIosT

2.2. DCF (distributed coordination function)

In the 802.11 protocol, the underlying mechanism for accessing the medium is called Distributed Coordination Function (DCF). This is a random access scheme, a protocol based on CSMA/CA, and the re-transmission of collided packets is subject to discrete Backoff Timer rules. DCF uses two techniques for packet transmission. The first is a two-way handshaking technique. This technique is characterized by the fact that the ACK signal is transmitted immediately from the destination station that transmitted it, which means that it successfully received the packet sent by the sender station. The second technique is the optional four way handshaking technique known as the RTS/CTS mechanism. This technique reserves a channel by sending a RTS frame before transmitting a packet. When a destination station receives a RTS frame, it notifies the CTS frame that it has received an RTS frame. After that, normal packet transmission can occur and an ACK response can also be generated. The RTS/CTS mechanism is used to solve the Hidden Terminals problem, and the Hidden Terminals problem is that multiple pairs of nodes can not hear each other.

More specifically, DCF is described as follows. A station with a new packet monitors whether the channel is empty or not, and if the channel is empty for a period of time called DIFS, the station transmits the packet. However, if you know that the channel is busy (either immediately or through DIFS), the station will wait for the DIFS to monitor until the channel is empty. And to avoid channel capture, the station must wait for a random backoff time, even though the channel is empty during DIFS between two consecutive new packet transmissions. DCF uses a binary exponential backoff scale for efficiency. Immediately after DIFS, the time is slotted, which is the amount of time that any station can detect if another station has sent a packet, and this time depends on the physical layer.

DCF is selected between (0, w-1) for the backoff time in packet transmission. This w value is called the Contention Window and is related to the number of failures to send a packet. When attempting to transmit a packet for the first time, w is chosen as CWmin and w increases by an exponential power of 2 as the number of failed transmissions increases, and can increase to CWmax. The backoff timer is decremented when the channel is detected to be empty, and the backoff timer stops when it detects that the channel is transmitting. If the channel is found to be empty than one DIFS, the backoff timer operates again and the packet is transmitted when the timer becomes 0 again.

In CSMA/CA, a destination broadcasts an ACK when it successfully receives a packet to detect a collision. ACK is sent immediately after a short time, called SIFS, at the end of the packet, and since SIFS is shorter than DIFS, other stations can not determine that the channel is empty until the end of the ACK. If the station that sent the packet does not receive an ACK for a certain amount of time or another packet transmission is detected on the channel, it is reschedule by the backoff rule.

Figures 3 and 4 show a packet transmission process between A and B with DCF and RTS/CTS mechanism, respectively. When the backoff timer of STATION A becomes zero, it is a process of sending a packet after DIFS time and receiving an ACK from the destination. If the data is successfully sent, A randomly selects a value to proceed with the timer and B will also resume the timer process that was frozen. Then the timer of B becomes 0 and B transfers the packet. However, when the node of recipient of the spoofed frames responses ACK to the access point (AP) with an original MAC address, the AP realized the spoofing attack in the network. Due to the spoofing attack, the node lost the channel utilization change. Therefore, we need to design security aware fair scheme in unsaturated 802.11.

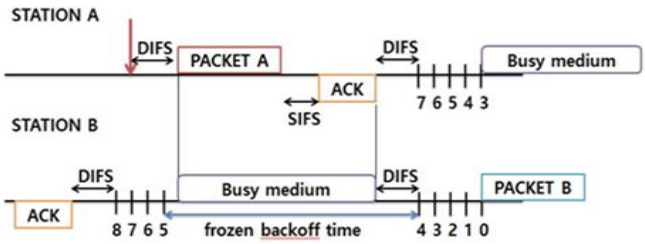


Figure 3. DCF mechanism

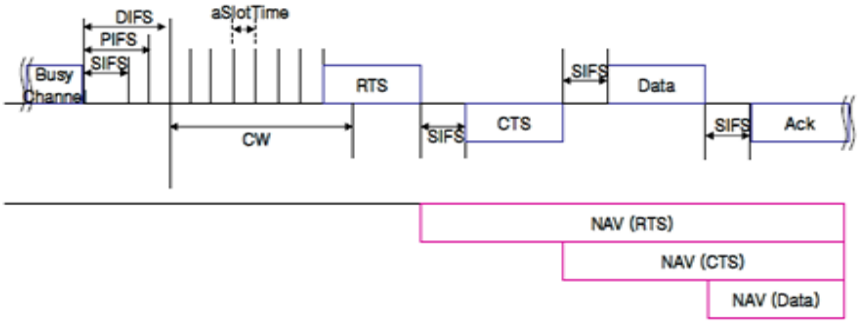


Figure 4. RTS/CTS mechanism

2.3. RTS/CTS mechanism

The node that has generated the shortest random backoff time successfully accesses the medium and transmits the RTS frame first. The RTS frame contains the address of the source node to which data is to be transmitted and the duration field used to set the network allocation vector (NAV). Among the nodes receiving the RTS frame, the destination node transmits the CTS frame as a response to the RTS frame, and the remaining nodes setting their NAV as the value of the duration field included in the RTS frame postpone access. When the transmission of the RTS/CTS frame is completed, the transmitting node starts data transmission and the receiving node transmits an ACK frame. All frames contain a duration field, and the nodes update the NAV only if they receive a duration field that is greater than the current NAV. When the NAV is zero, the nodes determine that the medium is idle, wait for DIFS, and then attempt to access the medium while reducing their backoff time. Since the DCF scheme can instantaneously confirm the transmission packet loss due to the RTS and CTS exchange collision, the RTS/CTS scheme is effective in an environment having a large average packet size or a high probability of collision due to a large number of nodes.

The purpose of exchanging RTS/CTS packets is to reduce performance degradation caused by hidden terminals. Various studies are under way to prevent performance degradation due to various factors such as collision with hidden terminal. The VBS algorithm [24] that adjusts the initial value of the backoff

stage variably in order to prevent a large possibility of collision when there are more than a certain number of stations in the same channel, and by assigning different CW values according to the number of collisions generated in each station. In order to solve the problem of performance degradation in terms of throughput and delay when there are many nodes participating in competition, it is necessary to increase the contention window to the maximum contention window in the event of a collision after the packet transmission (m, k) [25], to improve the MAC performance by selectively using the DCF and PCF protocols according to the result.

In order to solve the problem of degradation in performance from the point of view of throughput and delay in case of many nodes participating in the competition, the method increases the contention window to the maximum contention window in case of a collision after the packet transmission and gradually reduces the contention window if the contention does not occur [25], a technique that improves the MAC performance by selectively using the DCF and PCF protocols according to the result of measuring the network state of the wireless LAN [16].

In order to reduce the possibility of collision and to minimize the delay and increase the reliability, an algorithm that uses a slot time that is not used in fixed CW when a successful terminal attempts continuous transmission. We propose an alternative transmission method of RTS and CTS frames according to the data frame length and propose a calculation method that can have the maximum capacity. In addition, Performance analysis of IEEE 802.11 DCF MAC was performed through mathematical analysis or simulation. Various mathematical analysis methods have been used. Bianchi proposed a Markov chain technique to model CSMA / CA characteristics. DCF described two channel approaches [24].

2.4. PCF (point coordination function)

PCF stands for Point Coordination Function and is one of the 802.11 media approaches. Unlike the DCF (Distrubuted Coordination Function) that is currently used, it means a WLAN MAC Sublayer protocol centralized in wireless LAN. The PCF uses a centrally controlled polling function. Unlike the DCF, the centralized polling function is a feature that directly controls services for all stations in the central AP. The polling method in the PCF is performed as shown in Figure 5. First, an access point (AP) waits to acquire a channel during a PIFS (PCF Inter-Frame Space) period. The AP then sends a CF-Poll Frame that allows frame transmission to all stations in the area covered by the PCF. That is, each station is asked whether there is frame to send. This means Polling only for stations that are allowed within the PCF period. If the station does not have a frame to transmit, the station returns a null frame.

The process in Figure 5 is as follows. The AP transmits a CF-Poll Frame. STA1 receives the data and transmits CF-Ack Frame for Data and CF-Poll Frame. The AP then sends a CF-Ack Frame for CF-Ack and a CF-Poll Frame for Polling again. After receiving CF-Poll Frame from STA2, data is sent. The AP receives the data and sends the CF-End Frame in order to terminate the CF-Ack frame and the PCF in response to the end of the PCF. In Figure 4, the time zone controlled by the PCF is called a contention free period (CFP). In Figure 4, 'B' in the frame means Beacon, and it has a meaning to indicate the head of CFP. Using CF-Poll Frame of PCF, we can consider security for identifying the original AP. But we did not consider control packet overhead.

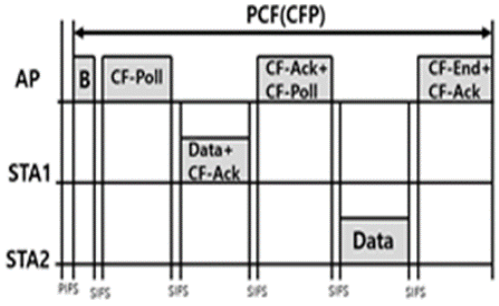


Figure 5. PCF mechanism

3. PROPOSED SCHEME

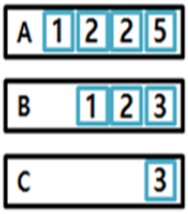
3.1. Priority setting by output queue and number of recipient of the spoofed packets in CIoTs environment

The proposed scheme gives the opportunity to send a packet to the CIoT node with the highest score by converting the number of spoofed packets in the output queue and the time of the oldest packet waiting in the output queue. Each CIoT node will have a table that lists the number of (un)spoofed packets waiting to be

sent and the time of the longest waiting packet, calculated in a certain ratio. Each CIoT node records an additional information when it sends a packet, plus the time of the oldest packet as well as information of (un)spoofed packets. Each time a packet is transmitted, the nodes in the range update the table with the additional information contained in the packet.

3.2. A system model

Figure 6 shows the scenarios of the proposed scheme where CIoT nodes A, B, and C are present and the (un) spoofed packets in each node's Output Queue and the time at which they were stored in the queue are arbitrarily assumed. In the table above, there are CIoT nodes A, B, and C (simply, number of packets * 3 + robust time * 7), and the score is calculated for each node based on (1). Isp and Iup are the indicator functions about the existence of spoofed and un-spoofed packets in the queue and Ir is an indicator function about the robustness of the each epoch in the system. pi and pi are each packet in the queue of each node and ri is the robust time duration of each node in the system composed of the discrete epochs. Therefore, the more node has packets and robust durations, the more node has transmission chances.



	A	B	C
# of packets	4	3	1
time	5	2	3
score	47	23	24

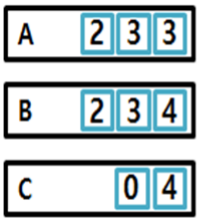
Figure 6. Scenarios of the proposed scheme in 802.11 based CIoTs

$$score_n = \alpha . \sum_{f-1}^{n} I_{sp} \, . p_i + \beta \, . \sum_{f-1}^{m} I_{up} \, . p_j + \sum_{k-1}^{l} I_r \, . r_j \quad (1)$$

For example, when calculating the scores of nodes A, B, and C, A has the highest chance of transmitting a packet because A scores the highest. So, when the backoff time of A node becomes 0 and A has a transmission opportunity.

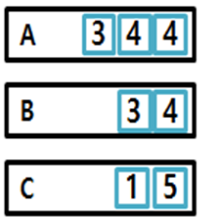
Figure 7 shows the case of hidden Tx of the specific CIoT node. For example, CIoT node A successfully transmitted, and a new packet was added to C while the node A was transmitting. CIoT B and C nodes who heard the packet sent by A will modify their table with information about the number and time of A's packet. When you make a modification, assume that A took 1 time epoch to transmit, so we need to increase the time value of each CIoT node by 1 and then calculate the score. Each node updated about the latest information of the node A since they overheard about the Tx of node A. However, since the other CIoT nodes have not yet transmitted, the information of the other nodes is not updated. Therefore, even though packets are added to C, but each node thinks that there is still one packet of C node and do not update of that. However, naturally node C broadcast the secure control packet with the latest updated information to all neighbor nodes based on (2). Or the node C can transmit the packet with the latest updated information to all neighbor when it has a chance to transmit the packet with the highest score with DCF as shown Figure 8. The description of tfair part of (2) is shown in performance evaluation part.

$$Tx_{\theta e} - control = \min(t_{fair}, t_{Dc\theta}) \quad (2)$$



A	B	C
3	3	1(2)
3	4	4
30	37	31

Figure 7. The case of hidden Tx of the specific node in unsaturated 802.11



A	B	C
3	2	1(2)
4	4	5
37	34	38

Figure 8. The case of fair Tx of control packet in the specific CIoT node

Tx chance of secure control packet is given to all nodes fairly in common when each node has enough secure duration with the third part of (1). But the less the node has robustness of security, the less it has chances of control packet.

Figure 9 shows a situation where a new CIoT node 'D' has been brought in while C is transmitting. A, B, and C nodes have learned a new node by energy detection give the new node a chance to send a packet for the first time in order to know the information of this new node 'D'. If D succeeds, A, B, and C nodes know the information of D and can also score D. Figure 10 shows a situation where CIoT node A, which existed during the transmission of a packet, was dropped for some reason, i.e., Denial of Service (DoS). The other nodes that have empty channels for transmission of A have the highest score and know that node A has been dropped because the packet is not transmitted. Then other nodes removes A related information from each table, and B transmits the packet with the highest priority.

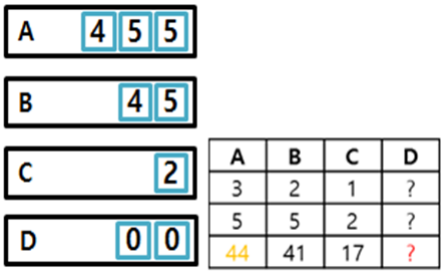


Figure 9. Join case of a new CIoT node in the system

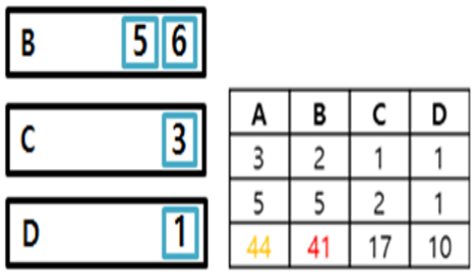


Figure 10. The case of CIoT node A with denial of service (DoS)

4. PERFORMANCE EVALUATION

This paper is based on the IEEE 802.11 DCF aware robust CIoT scheme and aims to improve performance by reducing the number of collisions between the nodes with the spoofed packets and the nodes with the un-spoofed packets fairly. In order to evaluate the performance, we compare the number of collisions by using C ++, and confirmed that the number of collisions of the proposed method is considerably small. For the description of tfair part of (2) we present a simple idea to change the selection of backoff time by keeping the other conditions the same as before. The proposed scheme of security aware fair transmission in unsaturated 802.11 can be achieved by using more equitable use of network resources by each node. First, the idea of modifying the backoff time algorithm is as follows as shown in Figure 11. By taking the method of selecting the backoff time within the range of [CW / 2, CW], the collision frequency could be reduced to less than half. It can be seen that the width of the circle is considerably narrowed.

In this paper, we set backoff time from CW/2 instead of setting the backoff time within the range of CW (Contention Window). It can naturally reduce the number of collisions between the nodes with the spoofed packets and the nodes with the un-spoofed packets fairly. After monitoring the IFS system and Busy medium, it selects random integer among [2/CW, CW], starts the process to determine the backoff time, decreases continuously and transmits the instant the backoff counter becomes zero as shown Figure 12. If transmission is successful, CW is initialized to CWmin. If transmission fails, CW is exponentially increased to CWmax.

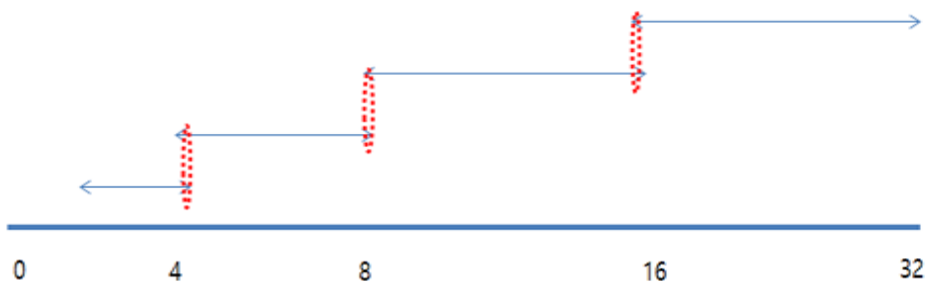


Figure 11. Secure collision range of the proposed scheme

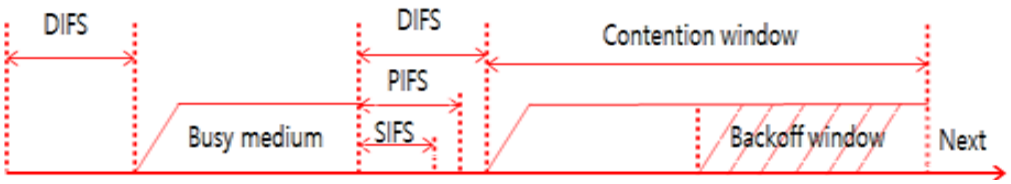


Figure 12. Dynamic control of CW in the proposed scheme

Figure 13 shows the scheme diagram for the proposed scheme. Start with CWmin in the initial Stage0 step. If a collision occurs, randomly select Backoff counter within [CW/2, CW] as Stage1. In case of continuous collision, CW exponentially increases to CWmax like Stage n. If the transmission succeeds, the CW value is initialized to CWmin, and the process returns to the stage 0.

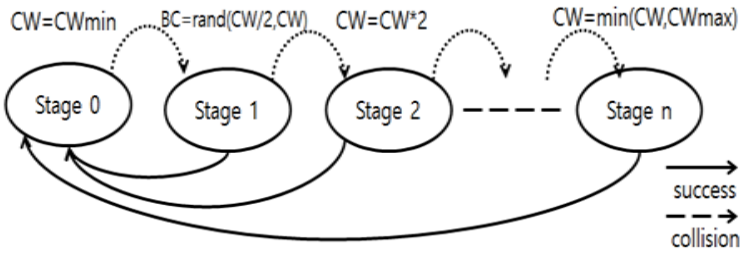


Figure 13. CW changes of CIoT in the proposed scheme

We constructed the simulation with C++ code and configured the CW value of each node to be arbitrarily selected from 32 to 1024 as shown in Figure 14. We also changed the number of CIoT nodes from 5 to 25 by 5 increments. As the number of nodes increases, it is found that the number of collisions is less than half of the number of collisions. The backoff time algorithm proposed in this paper does not increase the range of selecting backoff time cumulatively as the number of collision increases. Instead, it selects a value between CW/2 and CW to reduce the number of collisions between the CIoT nodes with the spoofed packets and the nodes with the un-spoofed packets fairly. As CWmax increases and the number of node with spoofed packets, the probability of collision decreases significantly as shown in Figures 15 and 16, respectively. Also, even when CWmax is small, the number of collisions is not large compared to the conventional technique, and the number of collisions is small in all cases.

In the existing IEEE 802.11 DCF based CIoT, the possibility of collision is high because the range of overlapping backoff time selection is wide. This can cause serious performance degradation unfairly in the node with (un)spoofed packets. On the other hand, when the proposed scheme is used, the possibility of collision can be reduced because each CIoT node greatly reduces overlapping range in selecting backoff time.

```
if last transmission was successful Then
    CW = CWmin
else /*Fail to transmission*/
    CW = 2(CW+1) - 1
    CW = min(CW, CWmax)
    Backoff = rand(CW/2,CW) x (slot)
if CW reaches a CWmax Then
    Backoff = rand(0,CW) x (slot)
```

Figure 14. pseudo code

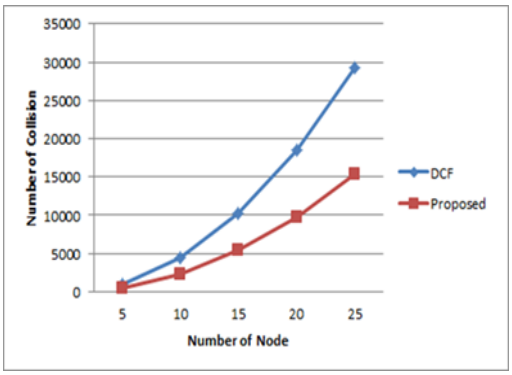


Figure 15. Number of collision with number of node

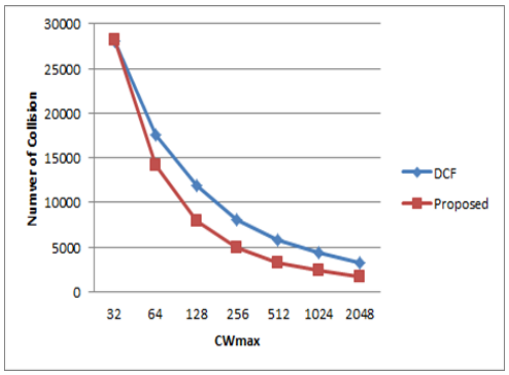


Figure 16. Number of collision with CWmax

Figure 17 is a graph comparing the DCF based IoT with the proposed system, 802.11 based CIoT, in terms of the number of successful transmissions until all nodes transmit at least once according to the number of packets and the WaitTime ratio. Figure 18 is a graph comparing the DCF based IoT with the proposed system of this paper for the number of cumulative collisions occurring in 100 transmissions.

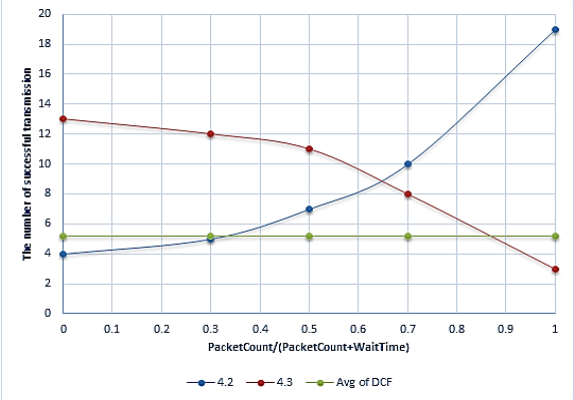


Figure 17. The number of successful transmissions

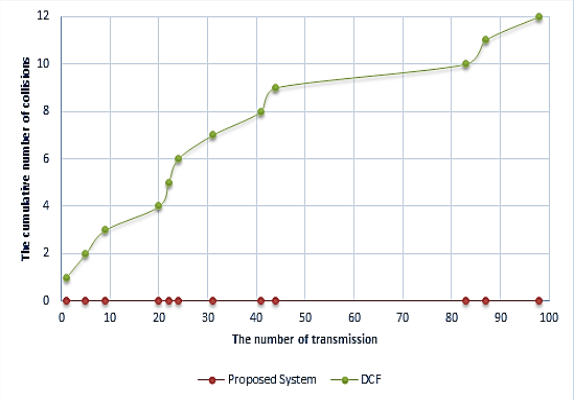


Figure 18. The number of cumulative collisions occurring in 100 transmissions

In an existing dcf, an average of about five successful transmissions were required so that all nodes could send packets at least once. When successfully transmitted about 5 times, the channel idle and wasted for an average of about 22 slot time. On the other hand, when using the method proposed in the above paper, there was no time for the channel to be wasted. In addition, it is possible to fairly transmit the backoff time by setting the backoff time in consideration of the number of (un)spoofed packets waiting for transmission.

5. CONCLUSION

The existing DCF based IoT is a method of setting backoff at random. At this time, if the collision continues, a IoT node on top of 802.11 that cannot send packets for a long time has occurred. Specifically if the IoT nodes with spoofed packets from attack, the fair changes of the transmission among system nodes are broken easily. Therefore, in this paper we set the backoff with the number of packets in the output queue and the time of the longest (un)spoofed packet waiting in the node. In addition, we modify the range of selecting backoff time by maintaining existing algorithm of IEEE 802.11 DCF opportunistically in CIoT environment. As a result, the CIoT nodes that have long waits or have a lot of (un)spoofed packets to send can now have transmission opportunities. Simulation results show that the simulation results show half the number of collisions compared with the conventional method.

ACKNOWLEDGEMENTS

This work was supported by the Ajou University research fund and Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035557) and Ajou University.

REFERENCES

[1] Qihui Wu, *et al*., "Cognitive Internet of Things: A New Paradigm beyond Connection," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 129-143, Apr. 2014.
[2] Mohammad Saeid Mahdavinejad, "Machine Learning for Internet of Things Data Analysis: A Survey," *Digital Communications and Networks*, Oct. 2017.
[3] Saurabh K Pandey, "*Event Localization in the Internet of Things Environment*," *7th International Conference on Advances in Computing & Communications, ICACC-2017*, 22-24, Cochin, India, Aug. 2017.
[4] Roadmap for IoT Spectrum Access, 2017. [Online], Available: https://www.itu.int/en/ITU-D/Regional-Presence/Africa/Documents/IoT-ICTA-trilok-Dabeesing.pdf.
[5] A Rakesh Kumar, "Smart network access for 802.11 based internet of things," *2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, 2015.
[6] Mirjana Maksimovic, "The Role of Green Internet of Things (G-IoT) and Big Data in Making Cities Smarter, Safer and More Sustainable," *IJCDS Journal*, vol. 6(4), pp. 2210-142, Jul. 2017.
[7] GSMA, "Air Quality Monitoring Using IoT and Big Data," Feb. 2018.
[8] Hayoung Oh, Rong Ran, "CIosT: Cognitive Internet of small Things Framework for Eco-friendly Network," Jan. 2019.
[9] Simon Duquennoy, *et al*., "Orchestra: Robust Mesh Networks Through Autonomously Scheduled TSCH," *SenSys'15*, Nov. 2015.
[10] T. Winter, P. Thubert, and RPL Author Team, "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," *RFC 6550*, Mar. 2012.
[11] 802.15.4e Task Group. 802.15.4e-2012: IEEE Standard for Local and metropolitan area networks, Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer, 16 April 2012.
[12] Giuseppe Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE Journal on Selected Areas in Communications*, vol. 18(3), pp. 535–547, Mar. 2000.
[13] Deng, Jing, Varshney, Pramod K. and Haas, Zygmunt J., "A New Backoff Algorithm for the IEEE 802.11 Distributed Coordination Function," *Sixth International Conference on Fuzzy Systems and Knowledge Discovery*, pp. 1-8, Dec. 2009.
[14] Mohammad Hossein Manshaei, Jean-Pierre Huaux, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function: Bianchi Model," *Mobile Networks*, pp. 1-8, 2007.
[15] Zhifei Li, *et al*., "Performance Analysis of IEEE 802.11 DCF: Throughput, Delay, and Fairness," *wireless comm*., pp. 1-13, 2017.
[16] H. C. Foundation, "WirelessHART Speci_cation 75: TDMA Data-Link Layer," HCF SPEC-75, 2008.
[17] ISA. ISA-100.11a-2011, "Wireless Systems for Industrial Automation: Process Control and Related Applications," Nov. 2013.
[18] X. Thubert, T. Watteyne, R. Struik, and M. Richardson, "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4e," draft-ietf-6tisch-architecture-06, Mar. *IETF Draft*, 2015.
[19] Tengfei Chang, Thomas Watteyne, Qin Wang, Xavier Vilajosana, "LLSF: Low Latency Scheduling Function for 6TiSCH Networks," *IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2016.
[20] Haythem Bany Salameh, Sufyan Almajali, Moussa Ayyash and Hany Elgala, "Security-aware Channel Assignment in IoT-based Cognitive Radio Networks for Time-Critical Applications," *2017 Fourth International Conference on Software Defined Systems (SDS)*, 2017.
[21] Haythvem Bany Salameh, Sufyan Almajali, Moussa Ayyash and Hany Elgala, "Batch-based security-aware spectrum sharing with simultaneous assignment decisions in time-critical IoT networks with cognitive radio capabilities," in *Transactions on Emerging Telecommunications Technologies*, May 2018.
[22] Everton de Matos, Ramão Tiago Tiburski, Leonardo Albernaz Amaral and Fabiano Hessel, "Providing Context-Aware Security for IoT Environments Through Context Sharing Feature," *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, pp. 1711-1715, 2018.
[23] Mostafizur Rahman Masum, "IoT Security Training, IoT Security Awareness," *IoT Security Training, IoT Security Awareness*, Jan. 2019.
[24] S. K. Kang, Y. Y. Choo, "Variable Backoff Stage (VBS) Algorithm to Reduce Collisions in IEEE 802.11 DCF," *J. Korea Inst. Inf. Commun. Eng*., 19(6), pp. 1333-1340, 2015.
[25] BJ. and H. Nam, "Backoff Algorithm to improve DCF functionality in IEEE 802.11," *J. H. Nam, Backoff Algorithm to improve DCF functionality in IEEE 802.11, IJCA*, vol. 7(5), 2014.

BIOGRAPHY OF AUTHOR

Hayoung Oh received the the Ph.D. degree in Computer Science from Seoul National University in 2013. From 2002 to 2004, she joined Shinhan Financial Group as a developer in applied research. In 2010, she was with U.C. Berkeley as a researcher. From 2013 to 2016, she has been with Soongsil University as a professor in the School of Electronic Engineering. Since 2016, she has been with Ajou University as a professor. Her research interests include social and computer networks, and security.