Impact of RTS/CTS jamming attacks in IEEE 802.11ah dense networks

Abdelhak Moussa
SM@RTS Laboratory
Digital Research Center of Sfax (CRNS)
Tunisia
e-mail: abdelhak.moussa@enis.usfax.tn

Issam Jabri
College of Engineering and architecture
Al Yamamah University
Kingdom of Saudi Arabia
e-mail: issam.jabri@enig.rnu.tn

2021 International Wireless Communications and Mobile Computing (IWCMC) | 978-1-7281-8616-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/IWCMC51323.2021.9498705

***Abstract*—IoT, a cornerstone in the development of the 21st century's city, has presented different use cases with a multitude of challenges. In response to these challenges mainly characterized by the ubiquitous connectivity and the large-scale deployment, IEEE 802.11 committee issued the AH version of the standard. The main enhancements featured in this amendment are the support of up to 8000 stations interconnected within a 1 km radius. Despite the promising large coverage and the high number of stations that an IEEE802.11ah access point can handle, Wi-Fi HaLow still faces many security challenges. This paper studies the response of a network to jamming attacks based on control packets. It provides an overview of the introduced features within this amendment of the standard and presents alarming results showing how it is not fit to mitigate jamming attacks.**

***Index Terms*—IEEE 802.11ah, IoT, Security, Availability, Denial of Service, RTS/CTS**

I. Introduction

The user market penetration of WLAN technologies has experienced great success since the first standardization of WLAN in 1997. The widespread use of Wi-Fi devices has led to the case of ubiquitous access to information by everyone in the world, with office, industry or even personal wireless access to the Internet. Meanwhile, internet connectivity is more and more available to "things" enabling the emergence of IoT. Actually, more than 26 billion IoT units are deployed globally [1]. Wireless connectivity of IoT needs to consider the limited battery life and low processing power available in the deployed devices. Hence, it is mandatory to come up with newer techniques in the management of nodes alongside ubiquitous and efficient transmission and dissemination of data packets. Deployment of large number of devices on a large-scale has led to the introduction of the IEEE 802.11ah standard[2]. On the other hand, the critical nature of data makes its protection against numerous attacks an obligation.

Jamming attacks using control packets has been a serious threat to the availability of wireless connectivity. In fact, this type of attacks, mainly based on control packets such as RTS/CTS, has been exploited in numerous vector strikes which impact is subject to many research work[3], [4], [5]. Besides, the use of RTS/CTS mechanism is controversial in the AH version of IEEE 802.11 standard. In fact, the contention mechanism proposed in the standard does not use legacy DCF mechanism but a new scheme called Restricted Access Window (RAW). Meanwhile, recent research on the efficiency of RAW mechanism showed that the use of RTS/CTS is beneficial in terms of throughput, latency, and energy efficiency[6], [7]. Accordingly, this work investigates the security threats implied by the use of these mechanisms and studies the trade-off between usability and security in such cases.

In the rest of this paper, an overview of the IEEE 802.11ah is presented. Then, section III discusses the vulnerabilities related to the control frames. Section IV presents the simulation results of the jamming attacks. Finally, potential future directions are presented in the concluding section.

II. Overview of IEEE 802.11ah

The existence of unused wireless channel resources in the sub-1GHz radio band might be helpful in designing an outdoor long-range WLAN. In fact, radio frequencies below 1 GHz are characterized by a long range and an easy penetration of obstacles that could offer an increase in the wireless coverage of a WLAN. Another typical feature that sub-1GHz radio bands is the use of narrower band wireless channels that are less affected by frequency fading that characterizes the 5 GHz and above frequencies. Thus, S1G can gain in matter of wireless coverage. So using frequencies below 1 GHz has its advantages in increasing the coverage in a WLAN but let's not forget that it also has its drawbacks with significant throughput limitations compared to the other frequency bands above the 1 GHz.

Due to the drawbacks encountered by the current versions of the standard in response to the large demands for ubiquitous wireless access, IEEE 802.11 working group has triggered a new Task Group: TGah, with the new project of developing an IEEE 802.11 standard at sub 1GHz license-exempt bands for large-scale wireless networks. The scarcity of the available spectra in the sub-1GHz Industrial, Scientific and Medical (ISM) bands. The use of frequencies below the 1 GHz would liberate the large-scale deployment from the congested wireless access in the 2.4 and 5 GHz radio bands. Although S1G carrier frequencies for proprietary WLAN has already existed, the IEEE 802.11 LAN/MAN standards committee started the

TABLE I
KEY FEATURES IN IEEE 802.11AH AND IEEE 802.15.4E

Feature	IEEE 802.11ah	IEEE 802.15.4e
Frequency band	Unlicensed 900 MHz	Unlicensed 868/915 MHz and 2.4 GHz
Data rate	150Kbsp-300Mbps	<200 Kbps
Coverage range	<1.5 Km	<100 m
Power consumption	Low	Low
Number of supported devices	8000	65000

works on enhancing the features on the PHY and MAC layers in order to support license-exempt operations in the S1G band with a new task group TGah charged with developing the IEEE 802.11ah standard [1], [8].

The standardization process gained in popularity with the focus on the IoT and M2M trending topics. And the opportunity to develop a new WLAN protocol to support services with long-range and short-burst traffic attracted many big corporations, such as Nokia, Huawei and Qualcomm to this new platform of innovation and to unite their efforts and come up with the IEEE 802.11ah. The IEEE 802.11ah (Wi-Fi HaLow) and the IEEE 802.15.4e (ZigBee) are the main contenders for being the protocol of the IoT, and the high throughput feature as presented in Table I weighs in favor of the IEEE 802.11 solution [9]. TGah wants to appeal the need for large wireless coverage range, low power consumption and rich data rates which are the main needs in wireless sensor networks. Most importantly, the IEEE 802.11ah standard offers a wide range of new wireless technology that is intended to take over 802.15. To do so, this new standard has to provide the same features as ZigBee in terms of power consumption and long-range coverage.

The design of this standard is based on many use cases:

- Smart sensors and meters. This use case is the most obvious one because of the characteristics of S1G frequencies that would help in covering IoT applications for indoor and outdoor spaces in urban, suburban and rural environments.
- Back-haul aggregation. In this scenario, the routers and gateways gather data from the stations and forward it to servers with long range communications.
- Extended range hot-spot and cellular offloading. The high throughput and the long transmission-range make S1G communications very attractive for delivering the data that was originally targeted for cellular networks.

The key features of the PHY and MAC layers are presented in the following paragraphs.

A. IEEE 802.11ah PHY

The technological developments on the PHY layer of the IEEE 802.11ac standard influenced the standardization of 802.11ah PHY, since they were conducted in parallel. The 802.11ah standardization process aimed for providing a user experience similar to that of 2.4 and 5 GHz WLANs. The features of the PHY in the 802.11ah standard are based on the down-clocked operation of 802.11ac's PHY .

It is designed for transmission characteristics which are proper S1G radio frequencies with keeping in mind that the goal is to arrive one day to deploying one single AP with triple or quadruple band capabilities that can operate on the three bands of the ISM spectrum. Being a 10-times-down-clocked version of 802.11ac, 802.11ah defines 2, 4, 8, and 16 MHz channels alongside with an additional 1MHz channel that has the purpose of achieving long-range transmissions[2].

Channelization: The available S1G license-exempt bands are different depending on local regulations in each country. The channelization defined in IEEE 802.11ah was based on the available wireless spectrum in China, South Korea, Japan, Singapore, Europe and the United States. The main idea in the channelization techniques in 802.11ah is to split the radio band in multiple 1 MHz small channels and use the channel bonding techniques in order to achieve the wide channel bandwidths. However, channel bandwidths obtained through channel-bonding could be different according to local regulations and more work is investigating on how to optimize obtaining maximum bandwidths [9].

Transmission modes: Every station in IEEE 802.11ah has to support the reception of 1MHz and 2MHz as these channel bandwidths depict the transmission into two categories. The category of the 2 MHz channel bandwidth has its design exactly like the PHY of IEEE 802.11ac with the use of OFDM, MIMO and DL-MU-MIMO. Durations are ten times longer, and hence, the data rates are exactly one tenth of those found in the 802.11ac. Further information about the channelization and its impact on duration and transmission times is found in Khorov et al. [8].

As for the 1MHz bandwidth mode, the tone spacing is exactly the half of that in the other category which results in small data rates but a longer transmission-range.

B. IEEE 802.11ah MAC

The designing of this version presented the difficulty of supporting a large number of stations associated to an AP. These stations are battery powered and transmitting short packets, thus, the need for power saving MAC protocols and medium access novel mechanisms alongside other legacy technologies . In this paragraph we will detail the grouping of stations and the channel access in IEEE 802.11 ah.

Grouping of stations: As described above, the AP in IEEE 802.11ah is required to support larger numbers of station than in the legacy 802.11 WLANs. In order to increase the number of supported stations by one access point, a new hierarchical AID is defined. The idea is to group the stations according to a four-level structure. At the top level, the stations are divided into 4 pages of 32 blocks each. A block includes 8 subblocks of 8 stations each. This 13 bits representation allows to address 8191 stations based on several characteristics such as the nature, role and location of the station. Since a characteristic is not permanent, dynamically assigning and changing this grouping is required.

Channel access: The access to the channel in IEEE 802.11ah is contention based. In order to decrease collision

TABLE II
KEY MAC FEATURES WITHIN EACH AMENDMENT

Feature	802.11	802.11n	802.11ac	802.11ah
Backward compatibility	X	X	X	
DCF	X			
PCF	X			
HCCA	X	X		X
EDCA	X	X	X	X
TXOP Forward	X	X	X	X
TXOP RD		X	X	X
TXOP BDT				X
Dynamic Bandwidth Management			X	X
RID				X
Frame Aggregation		X	X	X
Block Ack	X	X	X	X
MU-MIMO			X	X
Group ID			X	X
TIM	X	X	X	X
Delivery TIM		X	X	X
Targe Wakeup Time				X
Grouping of Stations				X
Hierarchical AID				X
RAW				X
Low power mode operations				X

probability in such large-scale networks, the standardization committee introduced the *Restricted Access Window mechanism* (RAW). The main idea of RAW is to limit the set of stations that are accessing the channel and spread their contention over a long period of time, but this could raise other problems related to power consumption. The information about the group which is required to access the channel at a specific time is broadcast by the AP within a special beacon called Raw-Parameters-Set. During a RAW, only a set of stations that belong to the same page are required to contend for the channel. This solution relies heavily on the accuracy of the dynamic grouping of stations[8].

While this new mechanism is still trying to prove its accuracy, many other efforts have focused on developing RTS/CTS sector based techniques to overcome the problems with RAW [10], [11].

The amendments as it is shown in Table II were mainly driven by the demands of the market for higher throughput and ubiquitous access and we have remarked that the standardization always supposes a cooperative behavior from the all participating nodes of the network which leads to security vulnerabilities.

III. MAC SECURITY VULNERABILITIES IN IEEE 802.11AH

The information security refers to the techniques which are used in order to protect any form of confidential, private or sensitive information from any kind of unauthorized access. The security of numeric information is a great dilemma in our world. The data is flooding everywhere and the need to secure the application's flows of data is greater than any time before.

The first step with going forward and ensuring the security nowadays is to understand its main concepts, notably, the confidentiality, the integrity and the availability. This model is known as the *CIA triad* that guides the policies of information security within any organization. Data confidentiality stands for making data available exclusively to the entities accredited to have it, while data integrity is about ensuring that the information can not be corrupted or altered. The third component and the basis one in the security triad is the data availability, it requires that the data or the system providing it is always ready when required.

Now we focus on the security vulnerabilities related to the MAC level and more specifically the Denial of Service attacks and we try to show how the attacks work in order to proceed to the tests with the newer version of the standard.

Many works have been concluded in order to investigate the DoS attacks in 802.11 and proposed solutions to this problem. Since we assume that there is a single channel that is reused, keeping it busy in the reach of a node leads to a DoS attack on that node. Also, by using a particular node to continually send data can lead to the extinction of the battery life of that node. Even with the use of authentication, we can not radically prevent these attacks. The DoS attacks are mainly related to control frames, namely the RTS/CTS and ACK frames [12], [13], [14].

The RTS/CTS mechanism is used by the IEEE 802.11 in the MAC layer in order to mitigate the hidden node problem. The main idea for this mechanism is for a node to transmit a Ready To Send (RTS) packet to the nodes that are in its reach informing its neighbors that it has packets to send. When the receiver node receives the RTS packet, it responses by a Clear To Send (CTS) packet to the sender in order to inform its neighbors and especially those not in the reach of the transmitter that a transmission is about to start.

A. Vulnerabilities related to RTS/CTS

The major vulnerability within IEEE 802.11 is its nature and what makes it very successful; the communication medium. Because communications take place through the open air using radio waves at different frequencies, the risk of interception is greater than with the wired medium. If the message is not encrypted, or is encrypted with a weak algorithm, the security threat is serious and can damage the network and even the reputation of the standard. Especially if we remark that through the standardization process and in the notes and comments published by the Task Groups, the security concern is not seriously enough debated.

We can say that the efficiency of the IEEE 802.11 standard requires a cooperative behavior from all the participating stations in a network. Hence, it is very vulnerable to misbehaviour or malicious attacks based on altering the information and calculations required for a certain case to happen properly and as planned. Moreover, many hidden vulnerabilities that are mainly related to the formats of the control and management frames may be exploited by attackers for different malicious threats. The RTS/CTS exchange can be exploited by the attacker in order to jam its neighboring by deliberately sending RTS or CTS packets.

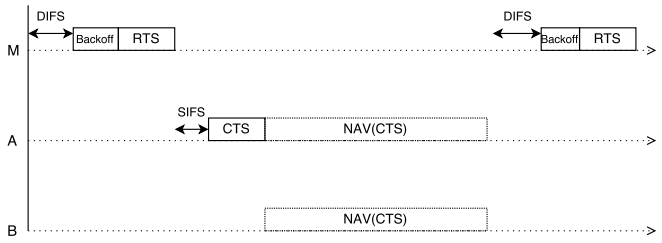

Fig. 1. False RTS attack

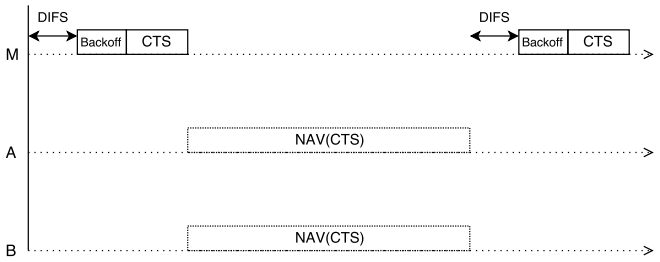

Fig. 2. False CTS attack

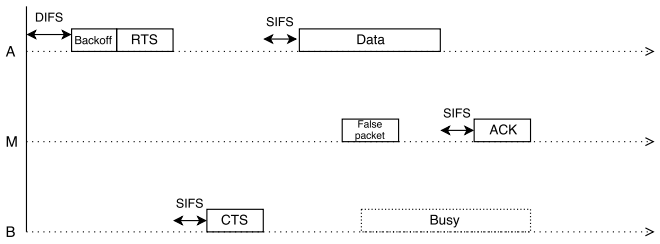

Fig. 3. False ACK attack

In the next paragraphs, we describe the hidden vulnerabilities within the RTS/CTS mechanism. During the standardization, the address of the transmitter node was considered irrelevant, since upon sending an RTS packet by the transmitter, all the nodes in its transmission range become silent except the destination that is supposed to answer by a CTS. Thus, in order to optimize the packets sizes, the CTS and ACK packet do not have a source address field. An attacker can exploit these vulnerabilities by producing some simple attacks without being identified by the monitoring process.

Jamming based on the false RTS: In this attack the sender is the attacker that tries to jam the reach of its antenna in the network. The adversary can send the packet with the source address field containing its address or an other address it spoofed from a previous packet it received. The success of this attacks relies on the frequency of sending the false RTS packet and the variation of the addresses and the duration in order to escape the monitoring process. Many works have tried to find solutions to this problem but they always end with proposing some mitigation techniques and they do not arrive to overcoming the problem.

Figure 1 illustrates the scenario of a false RTS attack.

Jamming based on the false CTS: The false CTS packet can be generated by the attacker station in order to create a false blocking situation. When the stations in the transmission range of the adversary receive a false CTS packet, they block their transmission for the duration specified in the received malicious packet, even if it did not receive the RTS, it considers itself as a hidden node.

In this attack, the attacker senses the channel status. If it is busy, it will wait for a DIFS+Back-off, otherwise, it will create the false CTS packet with a false destination address and then will starts the attack. The success of this attack relies on the misbehaving in the DCF mechanism in order to gain access to the medium at every time. This could be done by minimizing the Back-off or even changing the DIFS value. The success of the attacker relies also on varying the duration and the addresses of the forged CTS packets in order to escape the monitoring process.

All of the two above attacks can block transmissions in their range ,but also, they block the transmissions in the regions of the network reached by the its neighbors because of the altering of the duration fields. We can say that these attacks are extended to the interference range of the attacker node.

Figure 2 illustrates the scenario of a false CTS attack.

False packet validation based on false ACK: The false ACK packet can be forged and exploited by the attacker in order to disturb the network operations such as the routing process or monitoring mechanism. The goal of this attack is to validate a Data packet although the packet is not properly received at the receiver station. The false ACK can not be detected and its impact is more significant. In fact, the sender will not retransmit the packet because is has received the ACK packet. This attack is more complex than the two previously mentioned attacks. The attacker station needs to know the addresses of the sender and receiver of the legitimate Data exchange, it also needs to know the NAV(RTS) or the NAV(CTS). Thus, the spoofing of the addresses is obligatory for this attack to succeed. This attack is divided into two parts, in the first part, the attacker sends a false packet to the receiver station in order to create a collision at this station. In the second part, the attacker sends the false ACK to the sender station as if everything went normal and the Data packet was delivered successfully.

The durations at which the attacker sends the false packet and the false ACK are determined based on the RTS overheard at the beginning, so are the addresses of the sender and receiver stations.

The False ACK attack is limited to the transmission range of the attacker but its serious negative impact is related to the escape from the monitoring process and the other mechanisms that require an ACK packet.

Figure 3 illustrates the scenario of the false ACK attack.

IV. Impact of the attacks

In this section, we describe the simulations we have driven and present the results. First, we present the simulated topology and the appropriate parameters. Then, show and discuss the obtained results.

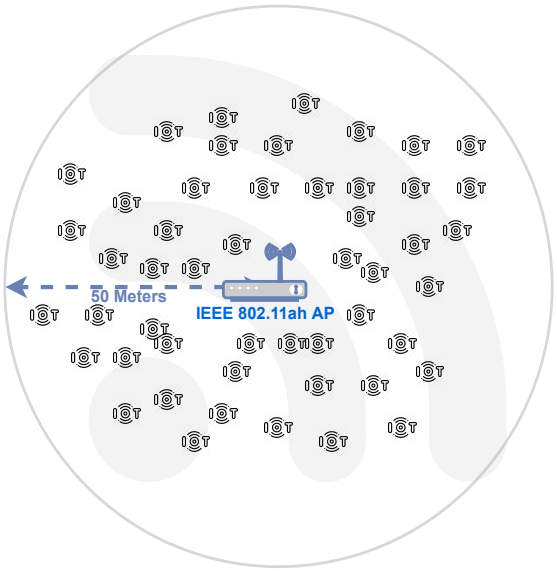

Fig. 4. Network topology of the IoT scenario

A. Simulation scenario

The scenarios we chose to implement is the IoT scenario which is the one that had driven the development of the IEEE 802.11ah standard. In this scenario, the network consists of 50 stations and one AP. All the stations are sending UDP packets to the AP. Here we are not testing in saturation mode, because in IoT use cases, the size of the data packets is reasonably small.

The stations are situated randomly within 50 meters from the AP as shown in the screenshot from NetAnim presented in Figure 4.

a) Simulation parameters: The simulations on this version are conducted through the 802.11ah module developed by Le Tian et al. [15] based on NS-3.24. We need here to present this module and the introduced new parameters.

Every station generates data packets during the 30 seconds of simulation time, and the simulation stops when there are no more queued packets waiting for transmission. The main simulation parameters are presented in Table III.

B. Results Analysis

Lastly, we implement the IoT uses case in order to study the impact of the attacks on the IEEE 802.11ah version.

Figure 5 stresses out the importance of the attack's duration. We remark that the network responds in the same manner to all three attacks. The longer the attack gets, the lower the throughput is, until it reaches a total 100 Kbytes/Second. It shows that if an attack lasts around 30 seconds, the throughput would drop to almost null and the recovery of lost packets would not be possible especially in this scenario characterized by short packets' waiting duration. This is a breaking point for the network.

Moreover, we study the response of the network to the different attacks by pulling the statistics from the Wireshark

TABLE III
SIMULATION PARAMETERS WITH IEEE 802.11AH

Parameter	Value [unit]
Number of stations	50
Number of RAW stations	50
Maximal distance	50 meters
Number of RAW groups	5
RAW slot count	0
NRAWSlotCount	8
Number of slots per RAW group	6
Frequency	0.9 GHz
MCS	8
Bandwidth	1 MHz
Short Guard Interval	Disabled
UDP inter-arrival	200 milliseconds
Payload size	500 bytes
Maximal delay	400 milliseconds
RTS/CTS	Enabled
Simulation time	30 seconds

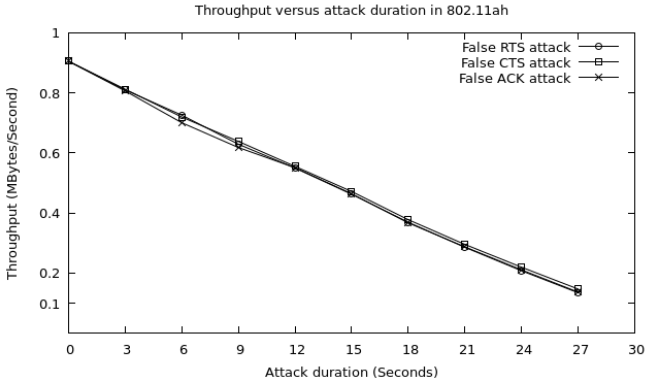

Fig. 5. Throughput versus duration of the attack in IEEE 802.11ah

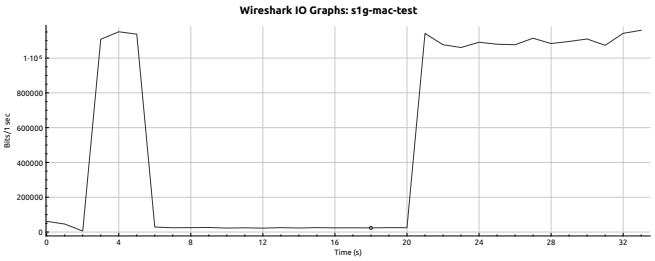

Fig. 6. Total throughput versus time during False RTS attack in IEEE 802.11ah

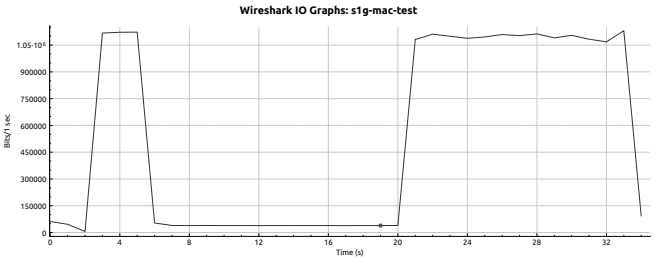

Fig. 7. Total throughput versus time during False CTS attack in IEEE 802.11ah

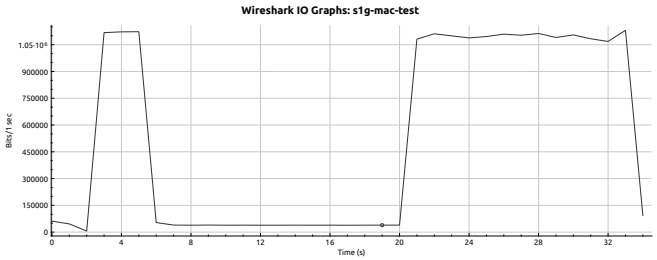

Fig. 8. Total throughput versus time during False ACK attack in IEEE 802.11ah

tool. In these tests we tried to drive the attacks away from the association to the AP process, thus, the attacks start at 6 seconds and stop at 21 seconds.

Figure 6 shows how throughput drops during the False RTS attack and similarly does during the False CTS and ACK attacks shown in Figure 7 and Figure 8 respectively. This drop in throughput results in high numbers of dropped packets which affects the delivery of critical data and drains battery storage.

Since attacks exploiting RTS/CTS resulted in serious damage to the network, we weigh in favor of not using this mechanism within RAW despite the fact that it was proved to be efficient in [16], [17]. Considering the small size of payloads, we believe that implementing a mitigation technique within RTS/CTS would result in more overhead and a questionable trade-off between security and efficiency. Moreover, lightweight authentication and trust mechanisms introduced at the grouping phase of RAW is critical to the large adoption of Wi-Fi HaLow.

V. Conclusions and Future Directions

In this work, we have carried an investigation on the impact of jamming attacks related to the control packets in IEEE 802.11ah standard through simulation. The obtained results show that the impact of these attacks is very serious and can reduce the reputation of the standard. It is better to drop the optional use of RTS/CTS and work on solving the hidden node problem through the optimization of RAW. Security enhancing goes through ensuring trust since the formation of RAW groups. We aim for the use of Blockchain in trust management between RAW groups in order to make the medium access scheme lighter and more efficient whilst maintaining secure communications.

References

[1] S. Aust, R. V. Prasad, and I. G. M. M. Niemegeers, "IEEE 802.11ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi," in *2012 IEEE International Conference on Communications (ICC)*. Ottawa, ON, Canada: IEEE, Jun. 2012, pp. 6885–6889. [Online]. Available: http://ieeexplore.ieee.org/document/6364903/

[2] "IEEE Standard for Information technology–Telecommunications and information exchange between systems - Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation," *IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016)*, pp. 1–594, May 2017, conference Name: IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016).

[3] M. Wang and B. Xu, "Guaranteed Cost Control of Cyper-Physical Systems Under Periodic DoS Jamming Attacks," in *2018 37th Chinese Control Conference (CCC)*, Jul. 2018, pp. 6241–6246, iSSN: 1934-1768.

[4] H. B. Salameh and M. Al-Quraan, "Securing Delay-Sensitive CR-IoT Networking Under Jamming Attacks: Parallel Transmission and Batching Perspective," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7529–7538, Aug. 2020, yang.

[5] H. Yang, M. Shi, Y. Xia, and P. Zhang, "Security Research on Wireless Networked Control Systems Subject to Jamming Attacks," *IEEE Transactions on Cybernetics*, vol. 49, no. 6, pp. 2022–2031, Jun. 2019, r.

[6] E. Coronado, V. Valero, L. Orozco-Barbosa, M.-E. Cambronero, and F. L. Pelayo, "Modeling and simulation of the IEEE 802.11e wireless protocol with hidden nodes using Colored Petri Nets," *Softw Syst Model*, Jul. 2020. [Online]. Available: https://doi.org/10.1007/s10270-020-00817-2

[7] O. Raeesi, J. Pirskanen, A. Hazmi, J. Talvitie, and M. Valkama, "Performance Enhancement and Evaluation of IEEE 802.11ah Multi-Access Point Network Using Restricted Access Window Mechanism," in *2014 IEEE International Conference on Distributed Computing in Sensor Systems*, May 2014, pp. 287–293, iSSN: 2325-2944.

[8] E. Khorov, A. Lyakhov, A. Krotov, and A. Guschin, "A survey on IEEE 802.11ah: An enabling networking technology for smart cities," *Computer Communications*, vol. 58, pp. 53–69, Mar. 2015. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0140366414002989

[9] N. Ahmed, H. Rahman, and M. Hussain, "A comparison of 802.11ah and 802.15.4 for IoT," *ICT Express*, vol. 2, no. 3, pp. 100–102, Sep. 2016. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2405959516300650

[10] S. Aust, R. V. Prasad, and I. G. Niemegeers, "Sector-based RTS/CTS access scheme for high density WLAN sensor networks," in *39th Annual IEEE Conference on Local Computer Networks Workshops*. Edmonton, AB, Canada: IEEE, Sep. 2014, pp. 697–701. [Online]. Available: http://ieeexplore.ieee.org/document/6927723/

[11] H. Nabuuma, E. Alsusa, and M. W. Baidas, "AID-based backoff for throughput enhancement in 802.11ah networks," *Int J Commun Syst*, vol. 32, no. 7, p. e3923, May 2019. [Online]. Available: http://doi.wiley.com/10.1002/dac.3923

[12] A. Rachedi and A. Benslimane, "Smart Attacks Based on Control Packets Vulnerabilities with IEEE 802.11 MAC," in *2008 International Wireless Communications and Mobile Computing Conference*. Crete Island, Greece: IEEE, Aug. 2008, pp. 588–593. [Online]. Available: http://ieeexplore.ieee.org/document/4600001/

[13] ——, "Impacts and solutions of control packets vulnerabilities with IEEE 802.11 MAC," *Wirel. Commun. Mob. Comput.*, vol. 9, no. 4, pp. 469–488, Apr. 2009. [Online]. Available: http://doi.wiley.com/10.1002/wcm.690

[14] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proceedings of the 12th conference on USENIX Security Symposium - Volume 12*, ser. SSYM'03. USA: USENIX Association, Aug. 2003, p. 2.

[15] L. Tian, S. Deronne, S. Latré, and J. Famaey, "Implementation and Validation of an IEEE 802.11 ah Module for ns-3," in *Proceedings of the Workshop on ns-3*. ACM, 2016, pp. 49–56.

[16] C.-C. Hu, Z.-B. Liu, Y.-M. Lin, and G.-J. Xu, "An Efficient and Effective Regrouping Algorithm for Minimizing Hidden Pairs in 802.11ah Networks:," in *Proceedings of the International Conference on Advances in Computer Technology, Information Science and Communications*. Xiamen, China: SCITEPRESS - Science and Technology Publications, 2019, pp. 191–196. [Online]. Available: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0008097301910196

[17] R. Gao, X. Lei, and Q. Hu, "An Adaptive Contention Window Scheme for 802.11ah WLANs," *ITM Web Conf.*, vol. 17, p. 01016, 2018. [Online]. Available: https://www.itm-conferences.org/10.1051/itmconf/20181701016