Performance Evaluation of Centralized and Distributed Control Methods for Efficient Registration of Massive IoT Devices

Nurullah Shahin, Rashid Ali, Seung Yeob Nam, and Young-Tak Kim
Dept. of Information and Communication Engineering, Yeungnam University, Gyeongsan, South Korea
Email: {nurullah, rashid, synam}@ynu.ac.kr, ytkim@yu.ac.kr

***Abstract*— The IEEE 802.11ah Wi-Fi HaLow allows thousands of devices being connected to a single access point (AP) with several improved functionalities compared to existing WiFi, such as restricted access window (RAW), target wake time (TWT), and traffic indication map (TIM). However, such functionalities are applicable only after successful registration process (exchanges of authentication and association information). In the registration process, a large number IoT devices are simultaneously trying to connect to a single centralized AP and inevitably imports severe contentions that bring a long registration time. In IEEE 802.11ah standards, the problems have been addressed through Centralized Authentication Control (CAC) and Distributed Authentication Control (DAC) protocols. Both CAC and DAC are proposed to reduce severe contentions by allowing an optimal number of devices requests for the registrations. However, the standard does not define the way to select the optimal operational parameters. In this paper, we evaluate and compare the performances of CAC and DAC protocols and provide two modified CAC-based algorithms that achieve substantial improvement overall existing IEEE 802.11ah schemes to reduce the registration time.[1]**

***Index Terms*—M2M networks, IEEE 802.11ah, Internet of Things (IoT), authentication, association.**

I. INTRODUCTION

One of the widely used communication technology for the Internet of Things (IoT) is the IEEE 802.11ah Wi-Fi HaLow standard supports a large number of battery-powered sensors/actuators with improved transmission probability, energy consumptions, long range, and efficient spectrum usage [1]. In IEEE 802.11ah, a single access point (AP) serves up to 8000 power-limited devices with the additional functionalities of Restricted Access Window (RAW), Target Wake Time (TWT), and Traffic Indication Map (TIM) [1]. The novel functionalities, however, can be applied only after successful completion of registration process. Therefore, some proper mechanisms are strongly required to handle the severe contentions by a large number of IoT devices that are trying to connect to a single AP.

The AP serves a large number of IoT devices, therefore, at any time the network may have some situations to restart or re-initialize for any unavoidable circumstances such as a sudden power outage, an AP reboot, and a system crash. Once the AP faces one of the above situations, all the IoT devices simultaneously start to contend for the channel access to send requests to reconnect with the AP. Since the IEEE 802.11ah uses CSMA/CA for the channel access mechanism, it generates high collisions and retransmissions specifically in the dense network, and therefore each IoT device consumes much time and energy for the registration process.

In the IEEE 802.11ah [2], the registration procedure includes two handshakes: authentication and association. The authentication performs the exchange of identity and security attributes (e.g., MAC addresses and security keys); the device sends an Authentication Request (AuthReq) and the AP confirms by an Authentication Response (AuthResp). On the other hand, the association resolves the capabilities attributes (e.g., supported transmission rates, association IDs, and channels); the device sends an Association Request (AReq) and the AP reply with an Association Response (AResp). Specifically, the AResp frame includes a short identifier referred to as Association ID (AID) that is used to identify the device for delivery of data frames after a successful registration procedure.

To enhance the registration procedure, the IEEE 802.11ah standard provides the methods to control the number of the allowed devices to start connection establishment with the AP. Since a registration requires multiple handshake procedures, the dynamic control of the number of devices provides an opportunity to reduce the severe collisions and to speed up the overall registration process in the network. The IEEE 802.11ah standard proposes centralized authentication control (CAC) and distributed authentication control (DAC) methods to control the traffic at an optimal level [3]. In CAC, the CAC-based parameters centrally control the contentions; the updated CAC parameters are broadcasted at every beacon interval. On the other hand, in DAC the DAC-based parameters control the contentions in a distributive way, where the AP sets the DAC parameters at initialization and does not need any dynamic adjustment algorithm. The AP broadcasts the fixed values of the parameters in every beacon interval. The standard, however, does not define the optimal parameters for these methods, and to the best knowledge of authors, there are no research reports that compare the performances of the CAC and the DAC with same operational environments.

In this paper, the performance of CAC and DAC methods are compared with optimal parameters. Moreover, we propose two enhanced CAC-based algorithms and compare with existing schemes by extensive simulation experiments to provide an insight to choose the best operational parameter selection that significantly reduces the registration time in dense IoT networks.

The rest of this paper is organized as follows. Section II briefly reviews related works. In Section III, we provide the description of CAC and DAC methods. Simulation results of

[1] This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2016-0-00313) supervised by the IITP (Institute for Information & communications Technology Promotion).

CAC and DAC are given in Section IV. Section V concludes the paper.

II. Related Work

The registration time of a massive number of devices becomes an important issue, especially in dense IoT networks, where many devices are simultaneously trying to connect to a centralized AP. Therefore, a large number of requests of the registrations increase collisions that result in increased retransmissions and increased registration time that degrades the overall network performance. To control the severe contentions in registration procedures, the IEEE 802.11ah TGah has introduced two authentication control mechanisms to limit the contentions at an optimal level to reduce the required registration time: centralized authentication control (CAC) and distributed authentication control (DAC) mechanisms [3].

Sthapit et al. [4] proposed an analysis of CAC parameters. Instead of using the authentication control threshold (ACT), the large number of devices is divided into equal sub-groups and only one specific sub-group is allowed to exchange the registration frames. The registration time can be reduced by allowing a specific number of sub-groups. However, the equal size of the sub-groups can be applied only when the AP has the knowledge about the number of devices in the network. Therefore, this mechanism is not applicable until all IoT devices are successfully registered. Moreover, the assumptions of the experiments are less practical due to the consideration of a small number of active devices at one time, which is not a realistic scenario in real M2M communications for massive numbers IoT devices.

Tian et al. [5] implemented the IEEE 802.11ah MAC and PHY in the network simulator-3 (ns-3) [6]. In terms of the association procedure, the authors evaluate the performance of the IEEE 802.11ah and develop an algorithm based on [2]. The results show that the average authentication time grows linearly with the number of connecting devices. As in [2], the given algorithm chooses the ACT based on the fixed step size and management queue threshold.

Another study and mathematical analysis of CAC is given in [7]. The authors proposed a contention-free transmission (CFT) scheme with several additional algorithms—Optimal Solution (OPT), Empty Slot Statistics (ESS), Decision Changing Algorithm (DCA), and Adaptive Threshold Algorithm (ATA)—to optimally adjust the ACT in order to reduce the overall registration time. The results show that 8000 devices can complete registration within 80 seconds.

One of our previous studies proposed an enhanced registration procedure with a network allocation vector (NAV) to mitigate contention in dense IoT networks [8] that reduces the time required for the registration process by implementing additional features, Firstly, the devices use EDCA to transmit AuthReq frame, and then transmit AuthRep, AReq, ARep, an acknowledgment (ACK) frames separated by Short Inter-Frame Space (SIFS). For this purpose, the device specifies the time until the end of the ACK for ARep in the Duration/ID field in AuthReq. When a device successfully sends AuthReq to the AP, and all other devices consider the channel virtually busy for the time specified in Duration/ID field. If the AP refuses to associate with the device, the AP sets 0 in Duration/ID field of AuthRep. Finally, the CAC method limits the number of devices from the total number of devices in dense IoT network. In the registration procedure, only the AuthReq faces contention to access the channel, and therefore, the combined scheme cuts contention by half, compared to the conventional 802.11ah. However, the performance of the combined scheme is not sufficient due to the inefficiency of the non-optimized CAC algorithm, so the registration requires rather a long time.

All of the above-mentioned approaches have several limitations: Firstly, the current version of IEEE 802.11ah standard clearly states that the devices should pick the random value at initialization and is re-picked only after a successful authentication procedure [2]. More specifically, the devices pick their random values only at initialization, and therefore, in the end, the AP can update the V_{ACT} to its maximum value to ensure that all the devices have the opportunity to be connected. Secondly, the use of a fixed step size provides an exponential growth of authentication time according to the number of connecting devices, depending on different sizes of networks [9]. Finally, an efficient optimized CAC based algorithm must adapt to the network dynamics and perform efficiently in congestion scenarios. These modifications affect the performance enhancement of the proposed algorithms.

Bankov et al. [9] proposed a fast centralized authentication (FCA) scheme with up and down algorithms, which adaptively adjust the ACT and step size based on the management queue. The up and down algorithms are very efficient in dense IoT network. Moreover, the performances of the up and down algorithms are compared with the optimal condition under the assumption that the AP knows the exact number of connecting devices. In the simulation with realistic conditions, the up and down algorithms provide authentication times just exceeding 22% and 20% more than the optimal condition, respectively.

Another solution to limit contention is the DAC mechanism that is described in IEEE 802.11ah standard [3]. The amendment introduces the basic procedures of the DAC method. Bankov et al. [10] proposed a mathematical model of link set-up process with DAC method and showed that the link set-up time in DAC depends linearly on the number of connecting devices, while without the DAC method the registration time is almost exponential.

In our previous work [11], we have proposed a hybrid slotted-CSMA/CA–time-division multiple access (TDMA) (HSCT) medium access control (MAC) protocol for efficient massive registration of dense IoT network. The registration time has been dramatically reduced by several steps: Firstly, the logical frame is divided into two parts: i) a contention-based slotted-CSMA/CA period (SCP) that is further divided into multiple CSMA/CA access windows (i.e., C-slots), and ii) a contention-free slotted-TDMA period (STP) that is further divided into multiple T-slots. The SCP allows each device to select a backoff slot in a geometric probability distribution to send the AuthReq. On the other hand, the STP is used to exchange AuthResp-AReq-AResp frames between devices and the AP through individually allocated T-slots. Secondly, the algorithm adaptively adjusts the SCP and STP to enable efficient channel utilization. Finally, two modified algorithms (Smart-up and Smart-down) are provided to select optimal CAC parameters.

In this paper, we compare the performances of the CAC and the DAC methods with detail analysis. The channel access mechanism in 802.11ah is fully based on CSMA/CA. We analyze the performance enhancement with consideration of the backward compatibility and less complexity of the current implementation. Moreover, the network simulation

// V_{ACT}: the authentication control threshold
// v_{ACT_old}: the previous authentication control threshold
// Δ: step size of the ACT
// $maxACT$: maximum authentication control threshold
// Q_L: management queue size of the AP
// S_A: number of successful AuthReq/AssocReq in the previous BI
// $mode$: assign the specific mode
// $init\_stage$: flag that is used to find more optimal Δ
// $change\_\Delta$: flag that is used to set more precise Δ

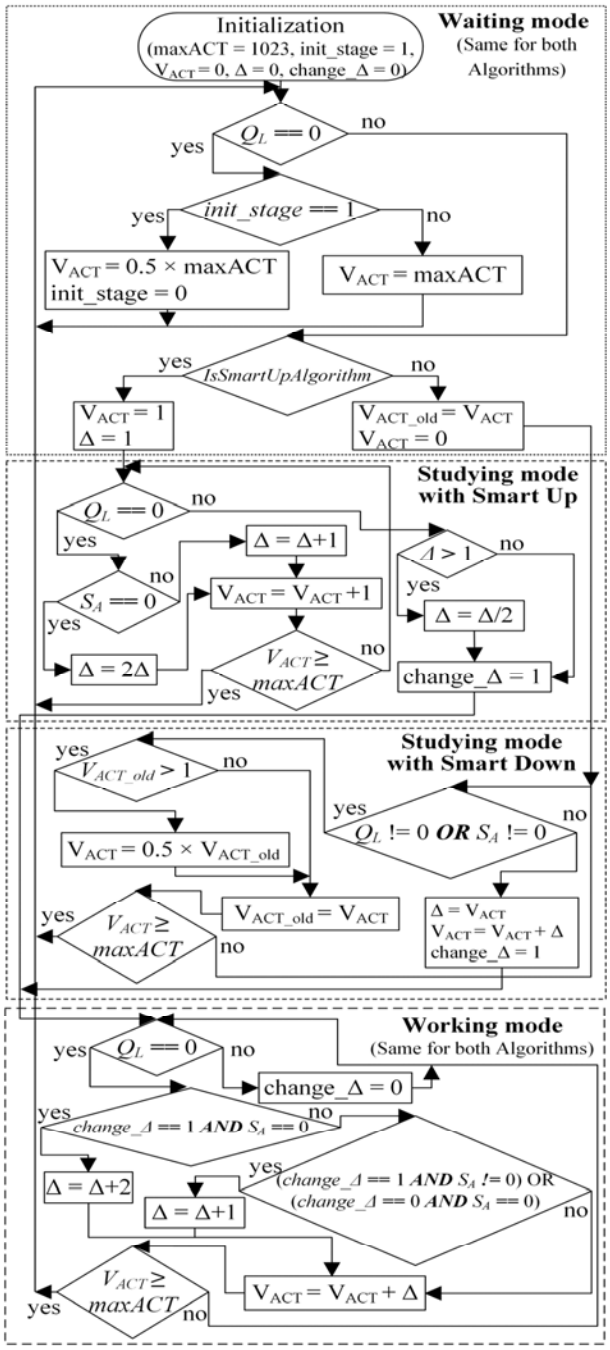

Fig. 1 Flowchart of "Smart Up" and "Smart Down" algorithms.

environments provide the higher fidelity in terms of MAC protocol behavior and performance evaluation. Finally, we compare the proposed algorithms and mechanisms with different network sizes to afford more insight of selecting suitable operational parameters for the dense IoT networks.

III. Centralized And Distributed Control Method

In this paper, we consider a dense IoT network with N devices and an AP, where devices can simultaneously try to connect with the AP, using either the CAC or the DAC protocol. We assume that all the devices are located in the transmission range of each other. Both CAC and DAC method follows the basic EDCA channel access mechanism.

A. Centralized Authentication Control (CAC)

The CAC mechanism in IEEE 802.11ah [3] specifies the optimal selection of authentication control threshold (V_{ACT}) based on the management queue (MQ) (Q_L) that buffers the response frames (i.e., AuthResp and AResp). In detail, the authentication control threshold (ACT) is updated or remained the same. The updated ACT allows the amount of a fixed step size (Δ) in every beacon interval (BI). If the queue size (Q_L) is greater than the fixed management queue threshold (Q_T), the ACT is decreased by a fixed step size. Otherwise, it is increased. However, IEEE 802.11ah standard does not define how to select the optimal values of step size and management queue threshold. The mechanism in [2] describes the selection of the optimal V_{ACT}, however, it provides the fixed step size instead of optimal adaptive selection of step size that significantly affects the performance of the registration process as it is shown in [9].

In the CAC method, the network can provide the maximum average number of successful AuthReqs in one BI (A_{OPT}) that can be obtained from the optimal setting of the actual number of contenders (N_{OPT}), authentication control threshold (V_{ACT_OPT}), and step size (Δ_{OPT}), if AP knows the actual network size as in [9]. Therefore, the optimal V_{ACT_OPT} and step size (Δ_{OPT}) provides the optimal number of contenders (N_{OPT}) among the total number of devices (N) in the network, defined as:

$$V_{ACT\_OPT} = V_{ACT\_OPT} + \Delta_{OPT} \quad (1)$$

$$N_{OPT} = \frac{V_{ACT\_OPT}}{1023} N \quad (2)$$

where the Δ_{OPT} can be determined through the simulation by taking the different value of step size (Δ).

Two efficient CAC-based smart up and smart down algorithms are provided to increase the efficiency of the performance in the registration procedure [11]. The smart up and smart down algorithms adaptively select both the ACT and the step size based on the management queue size and the number of AuthReqs/AReqs at the previous beacon. The smart up and smart down algorithms describe in detail in the flowchart of Fig. 1. Both algorithms execute in one of the three modes (*waiting*, *studying*, and *working* modes) in a BI. The working principle of the *waiting* and *working* modes are the same, but the *studying* mode is different for the smart up and smart down algorithms.

B. Distributed Authentication Control (DAC)

In the DAC method [3], the AP periodically broadcasts beacon frames that include the DAC information fields about the parameters: authentication control slot (ACS) duration (T_{ac}), the minimum transmission interval(TI_{min}), and the maximum

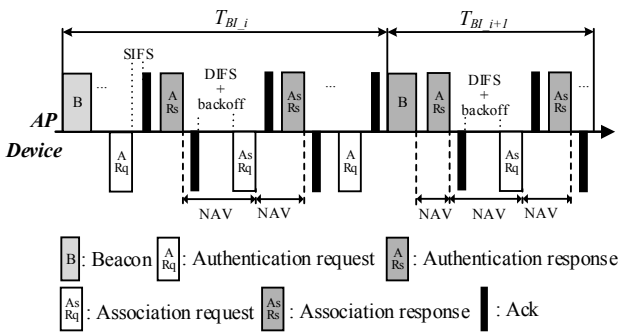

Fig. 2 Channel Reservation (CR) scheme for the registration process.

transmission interval (TI_{max}). The standard defines the values of T_{ac}, TI_{min}, and TI_{max} as 10 time units (TUs), eight BIs, and 256 BIs, respectively. Each device maintains a transmission interval (TI) in BI units, and a TI is initialized with an integer number uniformly distributed in the range from 0 to $TI_r - 1$, where TI_r is the transmission interval window and r is the number of authentication retries. At the initialization, the retry counter (r) is set to zero and TI_0 to the minimum TI (TI_{min}). When a device is allowed to send a AuthReq, it sets a fixed time duration called *AuthenticationRequestTimeout*. If no AuthResp arrives during *AuthenticationRequestTimeout,* the device considers that the AuthReq is lost, and it increases the retry counter and selects a new value of transmission interval (TI) from a new transmission interval window (TI_r) defined as:

$$TI_r = \begin{cases} TI_{min} & r = 0 \\ min\{2 \times TI_{r-1}, TI_{max}\} & 0 < r < R_{TI} \end{cases} \quad (3)$$

where R_{TI} is the maximum number of authentication retries. If $r \geq R_{TI}$, then the device sets the TI_r to TI_{min} to re-send the AuthReq. Each device chooses the number of BI, m, from the uniformly distributed the range $[0, TI_r - 1]$. Once more, the BI is equally divided into L authentication control slots, where $L = T_{BI} / T_{ac}$. The authentication control slot number, l, is uniformly selected from the range $[0, L - 1]$. The device attempts to send an AuthReq in authentication control slot l of BI m. If the AuthReq attempt is failed, the device increases the number of authentication retries (r) and re-picks m and l. Inside the ACS, the device attempts to access the channel according to the enhanced distributed channel access (EDCA) mechanism.

C. Channel Reservation (CR) Scheme for CAC and DAC

In CAC and DAC methods, the devices use the EDCA mechanism to transmit the frames. If a device is allowed to send a frame for the transmission, the frame enters into the transmission queue. Since multiple devices share one channel, each device joins in the contention. Therefore, before starting the transmission, each device senses the channel, and if it is idle the device transmits this frame. If the channel is busy, the device uniformly picks a backoff counter (k) that is initialized with an integer number uniformly distributed in the range from 0 to $CW_r - 1$, where CW_r is the contention window and r is the retry counter. At the initialization, the retry counter (r) and CW_0 is set to zero and the minimum CW (CW_{min}), respectively. The backoff counter is freezed when the channel is busy. Once the channel stays idle for time interval AIFS, the device resumes the backoff countdown, decrementing at every empty slot δ. When the backoff counter reaches zero, the device transmits the frame, and the receiver sends an ACK to the sender after a SIFS. If the ACK is received, the device considers the frame was successfully transmitted, and starts serving a new frame if the queue is not empty. If ACK is not arrived within *AckTimeout*, the device considers that the frame is lost. In this case, the device increases the retry counter and re-selects a new value of backoff counter from a new window by the following equation:

$$CW_r = \begin{cases} CW_{min} & r = 0 \\ min\{2 \times CW_{r-1}, CW_{max}\} & 0 < r < R_{CW} \end{cases} \quad (4)$$

where CW_{max} is the maximal value of the contention window (by default, equal to 1024). If the retry counter reaches the maximum retry limit R_{CW} (by default equal 7), the frame is dropped from the queue. In the EDCA scheme, since multiple devices simultaneously try to access the same channel, there is a possibility of more contention or dropping of frames due to the collision that increases the number of unsuccessful transmission attempts.

The channel reservation (CR) scheme is the extension of the contention-free transmission (CFT) scheme [7], which is based on virtual carrier sensing to provide contention-free access for the registration frames as shown in Fig. 2. The CR differs from CFT in that:

1) both AuthResp and AResp use the same values of the EDCA parameters as the beacon frame, where *CW* is set to zero.
2) the Duration/ID field of the AuthResp frame is set to zero if the AP refuses to authenticate the device.

The duration of a full registration (T_{REG}) process is about 6.684 ms, which is required to accommodate at least one registration as follows:

$$T_{\text{REG}} = 6\text{SIFS} + 4\text{ACK} + \text{AIFS} + CW_{\min} \times T_{\text{slot}} + T_{\text{AuthReq}} + T_{\text{AuthResp}} + T_{\text{AReq}} + T_{\text{AResp}} \approx 6.684 \text{ milliseconds} \quad (4)$$

where T_{AuthReq}, T_{AuthResp}, T_{AReq}, and T_{AResp} are the transmission time of the AuthReq, AuthResp, AReq, and AResp frame, respectively.

Bankov et al. [9] analyze the DAC method that shows the optimal selection of L minimizes the average registration time. The registration time grows almost linearly with large numbers of connecting devices. Unlike CAC, the DAC reduces contention in a distributed way based on traffic conditions. Since the IEEE 802.11ah proposed both CAC and DAC for the dense environment, it is necessary to compare their performances in the same operational environment. In this paper, we analyze and compare the performance of both CAC and DAC methods in the same environment from 1000 to 8000 IoT devices.

The collision probability becomes high as the number of contending devices grows, therefore, successful exchanges of a large number of registration frames spend a long time. As a result, devices can fail to receive authentication and association responses before the timing parameters *AuthenticationRequestTimeout* and *AssociationRequestTimeout* and require re-sending the new AuthReq and AReq, respectively. In CAC method, the AP manages the number of devices simultaneously sending the registration frames and thus

it controls the V_{ACT} in such a way that allows a maximal number of successful registrations within a BI. Therefore, the proposed algorithm tries to provide the optimal value of V_{ACT} to minimize the average registration time for the networks. On the other hand, in the DAC method, the AP does not periodically adjust the operation parameters that are set only at the initialization as compared to CAC method.

IV. Performance Evaluation

The algorithms are executed based on the implementation in [5] that is prepared for the 802.11ah MAC and PHY in network simulator-3 (ns-3) version 3.24 [6]. We compare our proposed Channel Reservation (CR) smart up (CR_Smart Up) and CR smart down (CR_Smart Down) algorithm with IEEE 802.11ah [2], combined authentication/association (CAA) procedure [8], No Channel Reservation with optimal CAC (No_CR_OPT), contention-free transmission (CFT) with Adaptive Threshold Algorithm (CFT_ATA) [7], CFT with Up algorithm (CFT_Up), CFT with Down algorithm (CFT_Down) [9], CFT with DAC method (CFT_DAC) [10], and CR with optimal CAC (CR_OPT) in the same operational conditions. Due to the consideration of the low-power nature of the battery-powered sensors in IoT applications, the transmission power is limited to 3 dBm. The simulation uses 650 Kbps physical data rate using a 2 MHz channel bandwidth, and the PHY and MAC layer parameters is set according to the IEEE 802.11ah [3] and [12] as shown in Table I. The 8000 devices randomly placed in a circle around the AP within a radius of, at most, half of the transmission range to avoid the influence of the hidden terminal problem [13].

Fig. 1 depicts the comparisons of the proposed CR_Smart Up and CR_Smart Down algorithms with different schemes to evaluate the registration process at the number of devices range from 0 to 8000. The proposed CR_Smart Down algorithms achieves substantial improvement over all existing methods and algorithms by an efficient registration procedure that requires, on average, 75%, 68.5%, 45%, 41%, 37% and 11% less time, compared to the No_CR_OPT, CFT_ATA, CFT_Up, CFT_Down, CFT_DAC, and CR_Smart Up schemes, respectively. The CFT_ATA takes longer registration time, because of no *waiting* mode. Therefore, if V_{ACT} reaches to its maximum value it could not overcome its optimal value. As we can see, both the conventional IEEE 802.11ah registration and the CAA scheme show the exponentially increasing registration time as the number of connecting devices grows. Although the IEEE 802.11ah and the CAA mechanism use several techniues to enhance the performance, the absence of *waiting* mode and fixed step size (Δ) make the big difference in the performance efficiency compared to the CR_Smart Up and CR_Smart Down schemes. Even at a large network size with a total number of devices of up to 8000, the CR_Smart Up and CR_Smart Down require only 24% and 15% more registration time than the CR_OPT that can provide the best V_{ACT}, if AP knows the actual network size. The optimal (OPT) algorithm provides the best performance among others. Because we assume that, the "OPT" algorithm knows the exact number of devices before starting the registration procedure. The AP can provide the optimal Δ_{OPT} to get the maximal registration in a BI according to Eqs. (1) and (2). In the real situation, however, the AP could not know the network size before registration process. On the other hand, the DAC method does not need to provide any upates of operational parameters in each BI, except the AP sets an optiamal value of

TABLE I
MAC LAYER PARAMETERS USED IN SIMULATIONS [3][12]

Parameters	Value
AP's transmission range	1000 meters
Device's transmission range	500 meters
PHY header + preamble	20 μs
Beacon length	67~100 bytes
Authentication request (AuthReq) length	26 bytes
Authentication response (AuthResp) length	28 bytes
Association request (AReq) length	43 bytes
Association response (AResp) length	33 bytes
Authentication/Association request timeout	500 ms
Acknowledgement (ACK) length	14 bytes
Back-off slot duration (δ)	52 μs
Short Inter-Frame Space (SIFS)	160 μs
Arbitration Inter-Frame Space (AIFS)	264 μs
Air propagation delay	3 μs
Beacon interval (BI)	100 ms
Minimum contention window (CW_{min})	16
Maximum contention window (CW_{max})	1023
Maximum retry limit in *EDCA* (R_{CW})	7
Minimum number of BI interval (IT_{min})	8
Maximum number of BI interval (IT_{max})	256
Maximum retry limit in *DAC* (R_{TI})	5

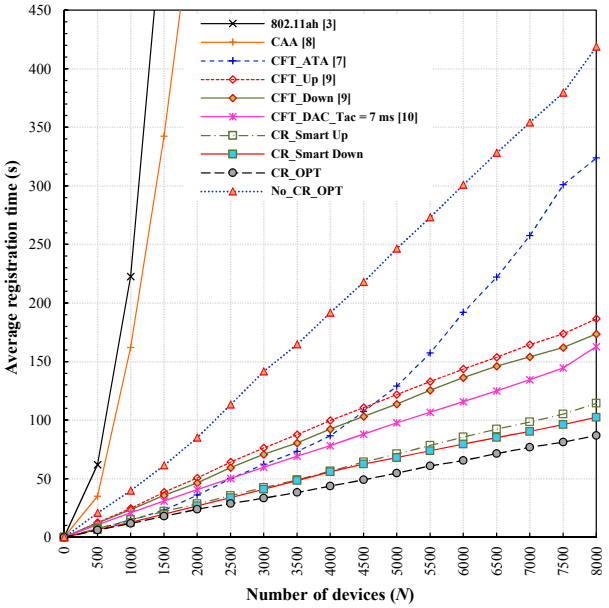

Fig. 1. The average registration time under different protocols and algorithms with number of devices range from 0 to 8000.

ACS duration T_{ac} at the initialization and periodically broadcasts in every beacon. We have taken the best parameters for the each protocol.

Fig. 2 (a) and (b) shows the results with 1000 and 4000 devices for all schemes. In this analysis, the CR_Smart Up and CR_Smart Down algorithm outperform the CFT_DAC, CFT_Up, and CFT_Down algorithms in small, medium, and large IoT networks. The reasons behind are as follows. Firstly, the *waiting* mode initializes the V_{ACT} by the half of the maximum value instead of the maximum value. The less value of V_{ACT} allows a moderate number of devices to send the AuthReqs. Therefore, it takes less convergence time to switch from *waiting* mode to *studying* mode. Secondly, in *studying* mode, the consideration of both condition of Q_L and S_A allows more registrations during the selection of optimal Δ. Finally, the updates of V_{ACT} during the *working* mode also allows more

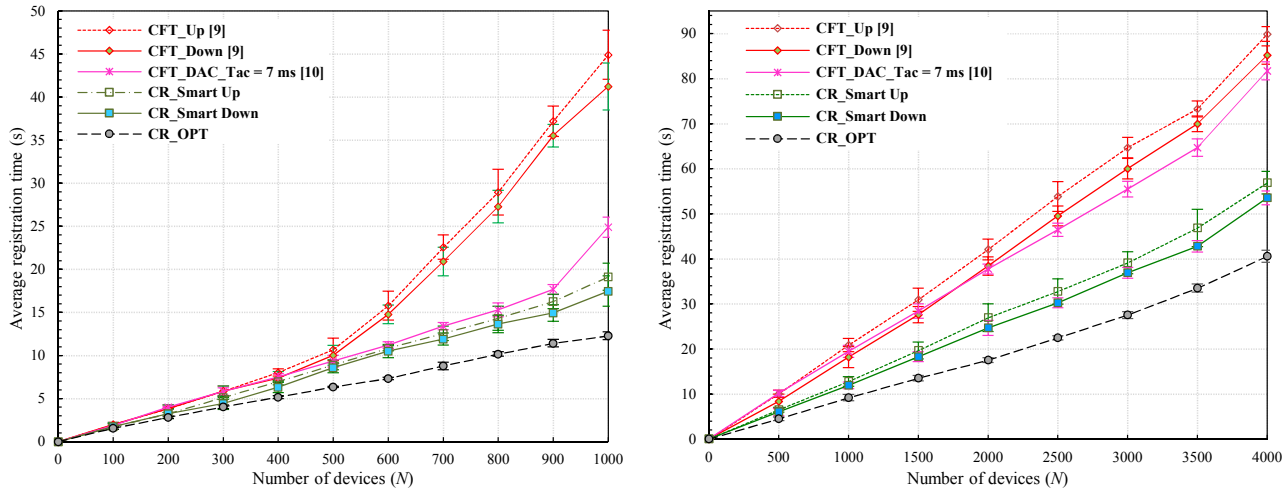

Fig. 2. The average registration time under different protocols and algorithms with number of devices (a) range from 0 to 1000; (b) range from 0 to 4000.

number of registrations with the consideration of both request and response traffic. There are small performance gaps among the CFT_DAC, CFT_Up, and CFT_Down algorithms at 4000 devices. Oppositely, if the network size is about 1000 devices, both the CFT_Up and CFT_Down algorithms require almost the same registration time for a small number of devices (e.g., 500 or less), however, after that there is an exponential increase with the connecting devices. This is because both the CFT_Up and CFT_Down algorithms consume more time to reach the value of V_{ACT} to its maximum during the working mode. In Fig. 2 (a), the CR_OPT takes 73%, 70%, 50%, 38%, and 29% less time compared with the CFT_Up, CFT_Down, CFT_DAC, CR_Smart Up, and CR_Smart Down algorithms, respectively at 1000 devices. In Fig. 2 (b), the registration time of the CR_OPT is 54%, 52%, 50%, 28%, and 24% lower than the CFT_Up, CFT_Down, CFT_DAC, CR_Smart Up, and CR_Smart Down algorithms, respectively at 4000 devices. In any size of the networks, the CR_Smart Up and CR_Smart Down have a small performance gap between them due to the allowing of more registrations at *studying* mode in CR_Smart Down than at the *studying* mode in CR_Smart Up algorithm.

V. Conclusion

We evaluated and compared the Centralized Authentication Control (CAC) and the Distributed Authentication Control (DAC) protocols, and their optimal parameter settings to reduce the registration time in dense IoT networks. In CAC, the AP controls the network traffic through a centralized algorithm. In DAC, oppositely the contentions are controlled in a distributive way, therefore, the AP sets the DAC parameters at initialization and does not need dynamic adjustment. Moreover, the optimal duration of authentication control slot (ACS) significantly affects the efficiency of the DAC performance. However, the standard does not provide any way to select optimal parameters. In this paper, we provide Smart Up and Smart Down algorithms that outperform the existing solutions under any size of the networks and requires a slightly higher registration time than the optimal one that has the knowledge about the network size. We provided the optimal duration of ACS through extensive simulations. Since more in-depth study is necessary in the comparisons of CAC and DAC methods with various considerations such as registration with interfering data nodes, error-channel conditions, and the mathematical analysis, we put these issues as our future work.

References

[1] E. Khorov, A. Lyakhov, A. Krotov, A. Guschin, "A survey on IEEE 802.11ah: An enabling networking technology for smart cities", Computer Communications, Volume 58, 2015, Pages 53–69, ISSN 0140-3664.

[2] H. Wang, Supporting Authentication/Association for Large Number of Devices, 2012. <http://mentor.ieee.org/802.11/dcn/12/11-12-0112-04-00ahsupporting-of-the-authentication-association-for-large-number-of-devices.pptx>.

[3] 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, in *IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016)*, pp.1–594, May 5 2017.

[4] P. Sthapit, S. Subedi, G. R. Kwon, and J. Y. Pyun, "Performance Analysis of Association Procedure in IEEE 802.11ah," in *The Tenth International Conference on Systems and Networks Communications*, 2015, pp. 70–73.

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

[6] The Network Simulator— ns-3. [Online]. Available: https://www.nsnam.org/.

[7] D. Bankov, E. Khorov, and A. Lyakhov, "The Study of the Centralized Control Method to Hasten Link Set-up in IEEE 802.11 ah Networks," in *Proceedings of European Wireless Conference 21th*, 2015, pp. 1–6.

[8] N. Shahin, T. Libea, and Y.-T. Kim, "Enhanced Registration Procedure with NAV for Mitigated Contentions in M2M Communications," in Proc. of *18th Asia-Pacific Network Operations and Management Symposium (APNOMS) 2016*, Kanazawa, Japan, 2016.

[9] D. Bankov, E. Khorov, A. Lyakhov and E. Stepanova, "Fast centralized authentication in Wi-Fi HaLow networks," in *2017 IEEE International Conference on Communications (ICC)*, Paris, 2017, pp. 1–6.

[10] D. Bankov, E. Khorov, and A. Lyakhov, "The Study of the Distributed Control Method to Hasten Link Set-up in IEEE 802.11ah Networks," in *Problems of Redundancy in Information and Control Systems (REDUNDANCY)*, 2016 XV International Symposium, 2016, pp.13–17.

[11] N. Shahin, R. Ali, and Y.-T. Kim, "Hybrid Slotted-CSMA/CA-TDMA for Efficient Massive Registration of IoT Devices," in *IEEE Access*, vol. 6, pp. 18366–18382, 2018. doi: 10.1109/ACCESS.2018.2815990

[12] A. Hazmi, J. Rinne, and M. Valkama, "Feasibility study of IEEE 802.11ah radio technology for IoT and M2M use cases," in *2012 IEEE Globecom Workshops*. IEEE, 2012, pp. 1687–1692.

[13] M. Park, "IEEE 802.11ah: Energy efficient MAC protocols for long range wireless LAN," in *2014 IEEE International Conference on Communications (ICC)*. IEEE, 2014, pp. 2388–239.