IEEE VTC2018-Fall , Chicago, IL, USA, August 27-30, 2018

Comparison of Slotted Aloha-NOMA and CSMA/CA for M2M Communications in IoT Networks

Asim Mazin, Mohamed Elkourdi, and Richard D. Gitlin, *Life Fellow, IEEE*
Innovation in Wireless Information Networking Lab (*i*WINLAB)
Department of Electrical Engineering, University of South Florida, Tampa, Florida 33620, USA
Email:{ asimmazin,elkourdi}@mail.usf.edu, richgitlin@usf.edu

***Abstract*—The Internet of things (IoT), which is the network of physical devices embedded with sensors, actuators, and connectivity, is being accelerated into the mainstream by the emergence of 5G wireless networking and the support of Machine-to-Machine (M2M) communications. Due to the simplicity of IoT devices and their sporadic traffic in such application, a simple medium access control (MAC) protocol is needed to connect M2M devices to the Internet through a hub (IoT gateway). This paper compares two MAC protocols namely: the newly introduced slotted Aloha-NOMA protocol and the well-known carrier sensing multiple access with collision avoidance (CSMA/CA) protocol. The comparison is based on two metrics, the throughput and the average delay. Simulation results show that the throughput of slotted Aloha-NOMA is higher than CSMA/CA at low probability of transmission at the cost of increased average delay caused by novel power level selection mechanism.**

***Index Terms*—Slotted-Aloha, M2M communication, multiple hypothesis testing, NOMA, CSMA/CA, IoT.**

I. Introduction

The rapid growth of both the number of connected devices and the data volume that is expected to be associated with the IoT applications, has increased the popularity of Machine-to-Machine (M2M) type communication within 5G wireless communication systems [1]. Uncoordinated random access schemes have attracted lots of attention in the standards of cellular network as a possible method for making massive number of M2M communication possible with a low signaling overhead [2], [3]. This paper compares the newly introduced slotted Aloha-NOMA protocol, which is matched to IoT/M2M applications and which is scalable, energy efficient and has high throughput and CSMA/CA, which is used as MAC for wireless sensor networks (WSN) such as ZigBee technology [4].

The slotted Aloha-NOMA protocol exploits the simplicity of slotted Aloha and the superior throughput of non-orthogonal multiple access (NOMA) [5] and its ability to resolve collisions via use of a successive interference cancellation (SIC) receiver [6], [7]. The recently introduced Aloha-NOMA protocol [8] and subsequent enhancements [9] are a promising candidate MAC protocol that can be utilized for low complexity IoT devices. In [10] NOMA is applied to multichannel slotted Aloha to enhance the throughput with respect to conventional multichannel slotted Aloha without the need for any bandwidth expansion [10]. The slotted Aloha-NOMA protocol is a promising method for not requiring any scheduling, apart from time slot and frame synchronization, in which all IoT devices transmit to the gateway at the same time on the same frequency band and has high throughput as will be demonstrated in this paper.

The contribution of this paper are: (1) This paper presents an enhancement to the slotted Aloha-NOMA protocol where the receiver adaptively learns the number of active devices (which is not known a priori) using a form of multi-hypothesis testing [11] and (2) a comparison of Slotted Aloha-NOMA with CSMA/CA in terms of throughput and average delay is presented. Simulation results are performed to show that the slotted Aloha-NOMA protocol performs better than the CSMA/CA in the low probability regime of transmission in terms of throughput.

The paper is organized as follows. Section II discusses the slotted Aloha-NOMA protocol, Section III presents the carrier sense multiple access with collision avoidances (CSMA/CA) and Section IV, simulation results are presented to compare the success probability and average delay of both protocols. The paper is concluded with some remarks in Section V.

II. Slotted Aloha-Noma Protocol

A. *Slotted Aloha-NOMA overview*

NOMA has emerged as a promising technology in 5G networks for many applications [5] and the slotted Aloha-NOMA protocol is a synergistic combination of the low complexity slotted Aloha protocol with the high throughput feature of NOMA. The main bottleneck of slotted Aloha systems is the low throughput caused by the high number of collisions, which can be addressed by NOMA. In slotted Aloha-NOMA the signaling overhead is reduced in the detection phase of the proposed protocol where the number of active IoT devices are detected by the gateway using a form of multiple hypotheses testing, which is further explained in Section II-B. It is also an energy efficient protocol due to the fact that a SIC receiver resolves collisions, and thus minimizes retransmission. The slotted Aloha-NOMA protocol can be suitable for various scenarios where many IoT devices are transmitting simultaneously on the same frequency with different power levels to an IoT gateway and then the received signals can be separated via use of a SIC receiver. A sample illustration of this scenario is depicted in Fig. 1 as a smart home with an IoT network. In this model, IoT devices send their data to the IoT gateway at the beginning of the slot using the slotted Aloha-NOMA protocol and the IoT gateway distinguish the signals with a SIC receiver.

The slotted Aloha-NOMA scheme increases the throughput significantly beyond that of conventional slotted Aloha due to the use of multiple power levels, which are considered additional channels in the power domain (and matched to the SIC receiver levels).

The slotted Aloha-NOMA protocol flowchart is depicted in Fig. 2. First, the IoT gateway transmits a beacon signal to announce its readiness to receive packets. Next, the IoT devices with packets ready to transmit send a training sequence to aid the gateway in detecting the number of active IoT devices in the medium. The IoT gateway detects the number of devices requesting transmission via a form of multiple hypotheses testing, as further explained in Section II-B, and adjusts the degree of SIC receiver for the optimum power levels. In practice, the SIC receiver has a fixed range of optimum power levels (e.g. m = 2, 3). If the IoT devices are registered with the gateway instead of using multi-hypothesis testing, implementation would be simpler, however, this will significantly increase the length of the control phase and thus decrease the payload or throughput considering the potentially large number of IoT devices. Third, if the detected number of active IoT devices is not in the range of the SIC capability, the IoT gateway aborts the transmission and starts the frame again by sending a new beacon signal and implying that the active transmitters use a random backoff. If the detected number of devices is in range, the IoT gateway broadcast the degree of SIC to the transmitters and then each active IoT device randomly picks one of the optimum power levels. If the choices are distinct the SIC receiver can decode the self-identifying signals (device ID + payload) and then the gateway sends an ACK. However, if the active IoT devices did not select distinct power levels, the reselection process is repeated and after a few attempts k if there is no successful transmission, the users receive a NACK and enter a random back-off mode. This will improve fairness among the users and will allow for the possibility of fewer active users in the next session (which will improve the probability of successful transmission). It should be clear, that the proposed protocol will be most efficient when there are a small number of active devices, so that the probability of using the optimum power levels, after one or two random tries, is high.

B. Multiple Hypothesis Testing

The detection of active devices starts after the IoT devices send their transmission request to IoT gateway as illustrated in Fig. 2. After receiving the beacon, all the IoT devices send at the same power level a training sequence of length L using the slotted Aloha protocol. The superimposed received signal

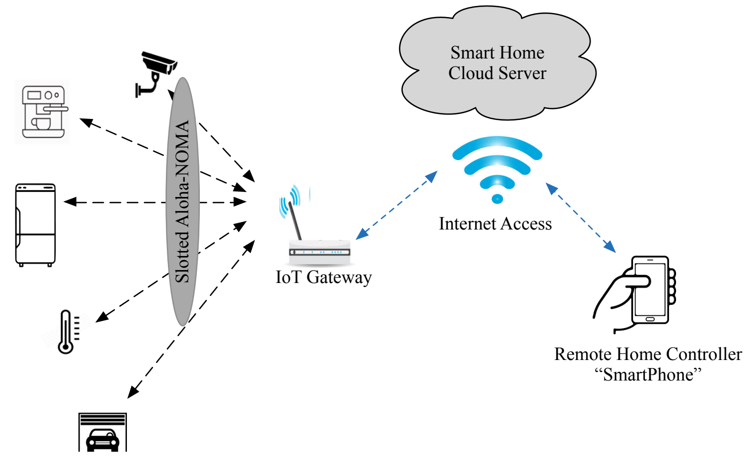

Fig. 1. A use case of Slotted Aloha-NOMA in the smart home with IoT

at the IoT gateway from N active transmitting IoT devices is given by

$$\mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{w}, \tag{1}$$

where $\mathbf{H} = [h_1, , h_2, ..., h_N] \in \mathbb{R}^{1\times N}$, h_n is the channel gain between the n^{th} IoT device and the IoT gateway, $\mathbf{s} \in \mathbb{R}^{N\times L}$ is the transmit sequence (e.g. BPSK) from N IoT active devices and $\mathbf{w} \in \mathbb{R}^{1\times L}$ is the additive white Gaussian noise with zero mean and variance σ^2. The multiple hypothesis test is used to detect the number of N active IoT devices from the total M IoT devices. The following hypotheses testing procedure is used to sequentially detect the number of active devices.

$$\begin{aligned}
\mathcal{H}_0 &: \text{Received signal contains only noise} \\
&\quad \mathbf{y} = \mathbf{w}, \\
\mathcal{H}_1 &: \text{Received signal contains} \\
&\quad \text{data from at least one IoT device} \\
&\quad \mathbf{y} = h_1 s_1 + \mathbf{w}, \\
\mathcal{H}_N &: \text{Received signal contains} \\
&\quad \text{data from at most } N \text{ IoT device} \\
&\quad \mathbf{y} = \mathbf{H}\mathbf{s} + \mathbf{w}
\end{aligned} \tag{2}$$

We assume $h_n = 1$, $\forall n \in \{1, 2, ..., N\}$. Following the Neyman-Pearson (NP) test, we can write the Likelihood Ratio (LR) testing [11] $\mathcal{H}_N$ Vs. $\mathcal{H}_{(N-1)}$ as in (3), where $\mathbf{s}_n \in \mathbb{R}^{1\times L}$ is the transmitted sequence from n^{th} IoT device. By taking the logarithm, (3) is simplified to (4).

The NP detector or the test statistics in (4) compares the sample mean of the received signal to the threshold $\gamma\prime$ to decide on a hypothesis $\mathcal{H}_N$ or $\mathcal{H}_{N-1}$. The NP test terminates if the number of detecting devices exceeds the SIC receiver optimum power levels, which are 3 levels in this paper. To compute the threshold $\gamma\prime$ in (4) for a desired probability of false alarm P_{FA}, which occurs when deciding $\mathcal{H}_N$ if the test in (4) is greater than the threshold $\gamma\prime$, so that P_{FA} can be written as

$$P_{PF} = p(T(\mathbf{y}) > \gamma\prime). \tag{5}$$

$$\frac{p(\mathbf{y};\sum_{n=1}^{N}\mathbf{s}_n,\mathcal{H}_N)}{p(\mathbf{y};\sum_{n=1}^{N-1}\mathbf{s}_n,\mathcal{H}_{N-1})}=\frac{exp[-\frac{1}{\sigma^2}(\mathbf{y}-\sum_{n=1}^{N}h_n\mathbf{s}_n)^T(\mathbf{y}-\sum_{n=1}^{N}h_n\mathbf{s}_n)]}{exp[-\frac{1}{\sigma^2}(\mathbf{y}-\sum_{n=1}^{N-1}h_n\mathbf{s}_n)^T(\mathbf{y}-\sum_{n=1}^{N-1}h_n\mathbf{s}_n)]}\lessgtr_{\mathcal{H}_{N-1}}^{\mathcal{H}_N}\gamma, N=1,...M. \tag{3}$$

$$T(\mathbf{y})=\frac{1}{L}\sum_{l=0}^{L-1}\mathbf{y}\lessgtr_{\mathcal{H}_N}^{\mathcal{H}_{N-1}}\frac{2\sigma^2\ln\gamma-((\sum_{n=1}^{N-1}h_n\mathbf{s}_n)^T(\sum_{n=1}^{N-1}h_n\mathbf{s}_n)+(\sum_{n=1}^{N}h_n\mathbf{s}_n)^T(\sum_{n=1}^{N}h_n\mathbf{s}_n))}{-2(\sum_{n=1}^{N-1}h_n\mathbf{s}_n+\sum_{n=1}^{N-1}h_n\mathbf{s}_n)}=\gamma\prime. \tag{4}$$

Since the test in (4) under both hypothesis is a Gaussian distribution, that $T(\mathbf{y})\sim\mathcal{N}(\sum_{l=0}^{L-1}\sum_{n=1}^{N-1}\mathbf{s}_n,\frac{\sigma^2}{L})$ under $\mathcal{H}_{N-1}$ and $T(\mathbf{y})\sim\mathcal{N}(\sum_{l=0}^{L-1}\sum_{n=1}^{N}\mathbf{s}_n,\frac{\sigma^2}{L})$ under $\mathcal{H}_N$, we rewrite (5) as

$$P_{FA}=Q\left(\frac{\gamma\prime-\sum_{l=0}^{L-1}\sum_{n=1}^{N}\mathbf{s}_n}{\sqrt{\frac{\sigma^2}{L}}}\right) \tag{6}$$

Thus the threshold $\gamma\prime$ is given by

$$\gamma\prime=Q^{-1}(P_{FA})\sqrt{\frac{\sigma^2}{L}}+\sum_{l=0}^{L-1}\sum_{n=1}^{N-1}\mathbf{s}_n \tag{7}$$

Following the same steps, the probability of detecting the number of active devices is

$$P_D=Q\left(\frac{\gamma\prime-\sum_{l=0}^{L-1}\sum_{n=1}^{N-1}\mathbf{s}_n}{\sqrt{\frac{\sigma^2}{L}}}\right) \tag{8}$$

From (7) and (8) the probability of detection P_D can be written as a function of signal to noise ratio SNR

$$P_D=Q\left(Q^{-1}(P_{FA})+\frac{\sum_{l=0}^{L-1}\sum_{n=1}^{N}\mathbf{s}_n-\sum_{l=0}^{L-1}\sum_{n=1}^{N-1}\mathbf{s}_n}{\sqrt{\frac{\sigma^2}{L}}}\right) \tag{9}$$

The receiver operating characteristic (ROC) curve of the energy detector is shown in Fig.3. Observe that the detection performance increases monotonically and smoothly with increasing SNR.

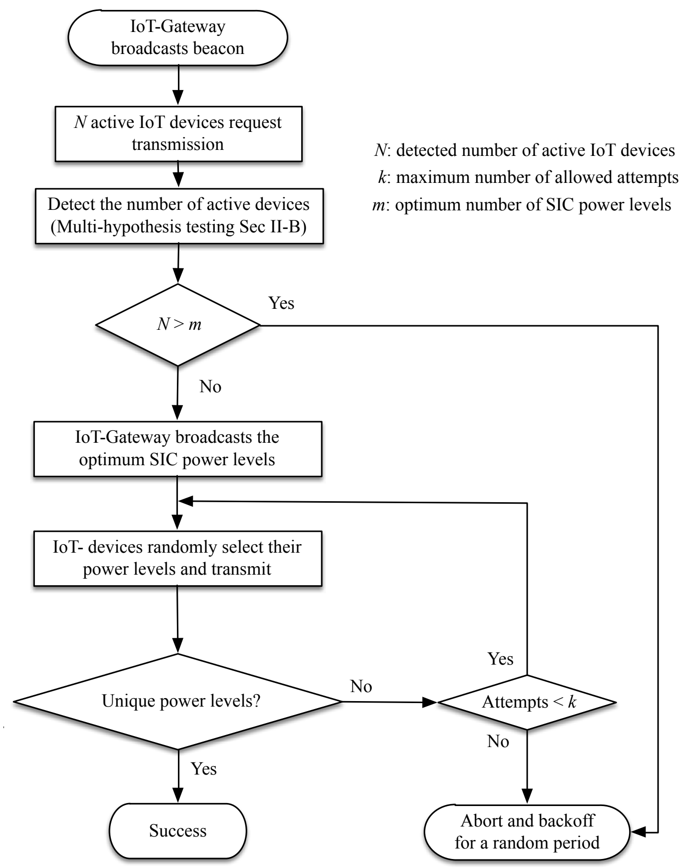

Fig. 2. Slotted Aloha-NOMA protocol.

III. An overview of CSMA/CA

The IEEE 802.15.4 standard specifies the MAC and physical (PHY) layers for low-rate wireless personal area networks (LR-WPANs). The CSMA/CA mechanism is used to reduce collision probability due to simultaneous node transmissions. In the standard, two channel access modes are defined. A beacon-enabled, where periodic beacons are used in the personal area network (PAN) for synchronization. In this case, the MAC sublayer employs the slotted version of the CSMA/CA algorithm and exponential backoff for transmissions in the contention access period (CAP) of the superframe [12], while in the unslotted version the CSMA/CA algorithm is used in non-beacon-enabled mode. In this paper the slotted Aloha-NOMA is compared to the slotted CSMA/CA version.

In slotted CSMA/CA algorithm of the IEEE 802.15.4, each devices MAC sub-layer initiate three variables for each transmission attempt. The number of times (NB) the CSMA-CA algorithm was required to back off while attempting the current transmission, the contention window (CW) length, which defining the number of backoff periods that need to be clear of channel activity before the transmission can start and the bakeoff exponent (BE), which is related to the number of bakeoff periods an IoT device waits before attempting to assess the channel. Fig. 4 depicts the flowchart of IEEE 802.15.4 slotted CSMA/CA scheme.

Consider an IoT device trying to transmit a ready packet. In IEEE 802.15.4 slotted CSMA/CA, the number of backoffs and the contention window are initialized (NB = 0 and CW = 2). Depending on the value of the Battery Life Extension MAC attribute, the backoff exponent is initialized to BE = 2 or BE = min (2, macMinBE), where macMinBE is a constant defined in the standard [12]. Then, the algorithm starts counting down a random number of backoff periods (BPs) uniformly generated within $[0,2^{BE}-1]$ at the boundary of a BP. When the timer expires, the algorithm then performs

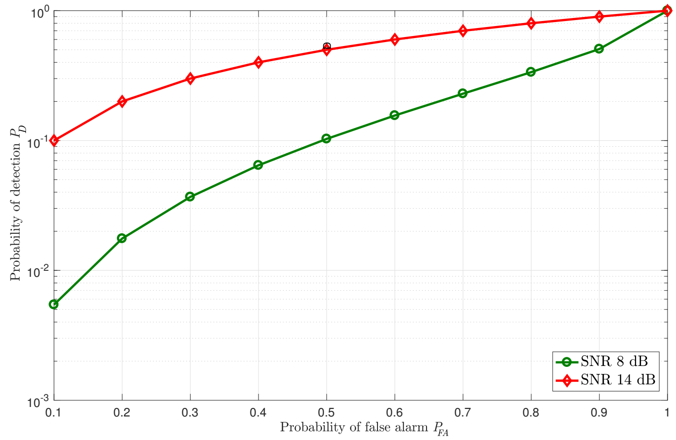

Fig. 3. ROC of the energy detector

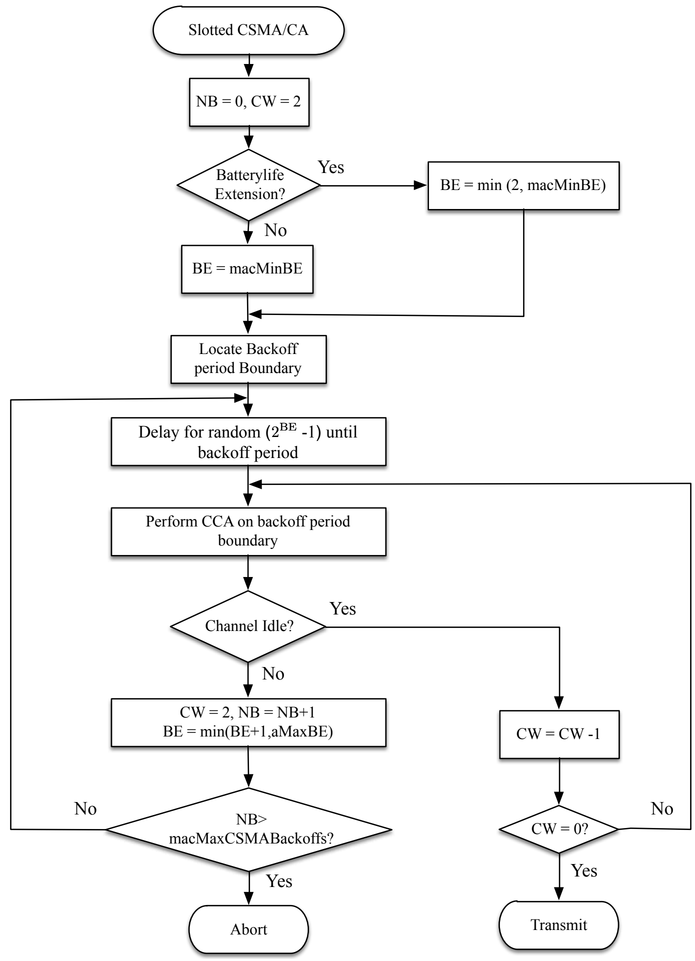

Fig. 4. IEEE 802.15.4 slotted CSMA/CA protocol flowchart [12].

one clear channel assessment (CCA) operation at the BP boundary to assess channel activity. If the channel is busy, CW is reset to 2, NB and BE are incremented, where BE must not exceed aMaxBE (default value equal to 5) [12]. Observe that Incrementing BE increases the probability of greater backoff delays. Once the maximum number of backoffs (NB = macMaxCSMABackoffs = 5) is reached, a failure is reported to the higher layer, otherwise, the IoT device performs another backoff operation. If the channel is sensed as idle, CW is decremented. The CCA is repeated if CW 0 to avoid collisions with acknowledgement frames. If the channel is again sensed as idle, the IoT device attempts to transmit, if the remaining BPs in the current CAP are sufficient to transmit the frame and the subsequent acknowledgement. If not, the CCAs and the frame transmission are both postponed to the next superframe.

IV. Simulation Results

In this section, the simulation results are presented to evaluate the performance of slotted Aloha-NOMA and CSMA/CA protocol based on throughput and average delay. Throughout the simulation, we assume there is one IoT gateway with a single antenna and a total of M IoT devices. A binomial distribution is considered to model the random number of active IoT devices N, each with probability of transmission p_T.

$$P_T(N; p_T, M) = \binom{M}{N} p_T^N (1 - p_T)^{M-N} \tag{10}$$

Fig. 5 shows the throughput of slotted Aloha-NOMA for different values of p_T, M=50 and k=3 attempts for the random selection of distinct optimum power levels (so, the probability of success should be 0.4). The throughput is the average number of successful transmissions for each probability of transmission over time. As expected, we observe that the throughput decreases with increasing probability of transmission in both protocols. More importantly, we can see that the throughput of the slotted Aloha-NOMA protocol is weighted by the average payload of successful transmissions and always higher than that of the slotted Aloha protocol. When the probability of transmission is 0.03, the throughput of slotted Aloha-NOMA with 3 power levels performs better than the CSMA/CA and has 5 times higher throughput than that of (conventional) slotted Aloha. This demonstrates that NOMA with a SIC receiver can help improve the throughput of slotted Aloha. However, the throughput of slotted Aloha-NOMA becomes lower than CSMA/CA for a probability of transmission greater than 0.06 (i.e. increase of offered load from the IoT devices), which is not surprising since for M = 50 the average number of active devices exceeds the number of acceptable power levels (SIC capability). The improved performance of CSMA/CA in a higher probability of transmission regime is due to the collision avoidance mechanism. It can be noted from Fig. 5. that adding more power levels (6 power levels) to slotted Aloha-NOMA increase the throughput at the expense of the average delay, which is discussed next.

The second performance metric is the average delay as shown in Fig. 6. In the simulation, the average delay is composed of propagation delay, data processing delay, random backoff delay, sensing delay (in CSMA/CA) and selecting unique power levels attempts (in slotted Aloha-NOMA). Ob-

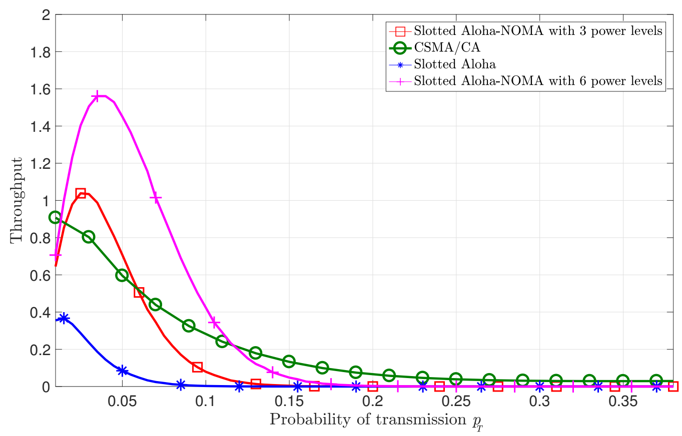

Fig. 5. Throughput of slotted Aloha-NOMA vs. slotted Aloha and CSMA/CA (BE =2, CW = 2, macMaxCSMABackofs = 2) for different values of probability of transmission M=50.

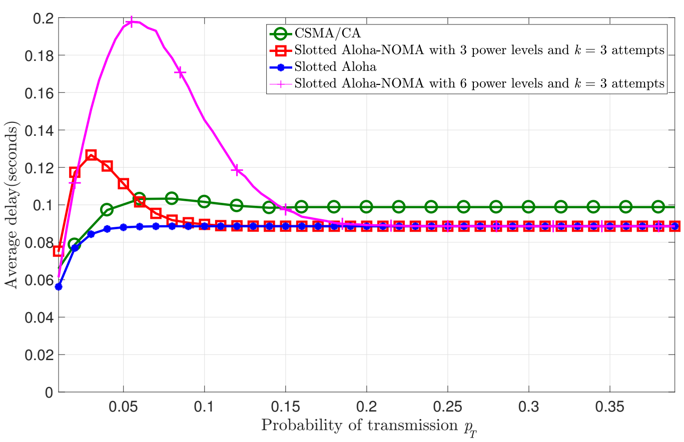

Fig. 6. Average delay of slotted Aloha-NOMA and CSMA/CA.

serve that the average delay of slotted Aloha-NOMA is larger than the CSMA/CA in the low probability of transmission due to the unique power levels selection process, which enables the higher throughput as mentioned above. The more attempts allowed for picking the distinct optimum power levels, the higher the throughput that can be achieved at the cost of increased delay. Since the backlogged IoT devices (i.e., failed to transmit in the previous try) have not been considered to rejoin the transmission queue, the average delay reported at a higher probability of transmission is the propagation delay and the random backoff delay.

V. Conclusion

This paper compares the slotted Aloha-NOMA and CSMA/CA protocols for M2M communications in IoT networks. The synergistic combination of slotted Aloha with NOMA and SIC receivers was demonstrated to significantly improve the throughput performance with respect to the CSMA/CA protocol at a low probability of transmission. This paper demonstrates through simulation results that the slotted Aloha-NOMA protocol can outperform CSMA/CA at a higher probability of transmission by increasing the number of received signals (that is, the power levels) at the cost of average delay. Future research directions are to investigate the fairness of both MAC protocols and study the effect of the backlogged IoTs that rejoin the transmission queue.

References

[1] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, “Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions,” *IEEE Communications Magazine*, vol. 52, no. 5, pp. 86–92, May 2014.

[2] 3GPP, “Study on RAN improvements for machine-type communications,” TS 37.868 V11.0, October 2011.

[3] 3GPP, “Evolved universal terrestrial radio access (E-UTRA); medium access control (MAC) protocol specification,” TS 36.321 V13.2.0, October 2016.

[4] E. Toscano and L. L. Bello, “Comparative assessments of ieee 802.15.4/zigbee and 6lowpan for low-power industrial wsns in realistic scenarios,” in *2012 9th IEEE International Workshop on Factory Communication Systems*, May 2012, pp. 115–124.

[5] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, “Non-orthogonal multiple access (NOMA) for cellular future radio access,” in *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, June 2013, pp. 1–5.

[6] X. Wang and H. V. Poor, “Iterative (Turbo) soft interference cancellation and decoding for coded CDMA,” *IEEE Transactions on Communications*, vol. 47, no. 7, pp. 1046–1061, Jul 1999.

[7] F. Al Rabee, K. Davaslioglu, and R. Gitlin, “The optimum received power levels of uplink non-orthogonal multiple access (NOMA) signals,” in *2017 IEEE 18th Wireless and Microwave Technology Conference (WAMICON)*, April 2017, pp. 1–4.

[8] E. Balevi, F. Al Rabee, and R. D. Gitlin, “ALOHA-NOMA for massive machine-to-machine IoT communication,” in *2018 IEEE International Conference on Communications (ICC)*, 2018. [Online]. Available: http://arxiv.org/abs/1803.09323

[9] J. Choi, “NOMA-based random access with multichannel ALOHA,” *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 12, pp. 2736–2743, Dec 2017.

[10] D. Shen and V. O. K. Li, “Performance analysis for a stabilized multichannel slotted ALOHA algorithm,” in *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.*, vol. 1, Sept 2003, pp. 249–253 Vol.1.

[11] S. M. Kay, *Fundamentals of Statistical Signal Processing: Practical Algorithm Development*. Prentice Hall, 2013.

[12] “IEEE Standard for Low-Rate Wireless Networks,” *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pp. 1–709, April 2016.