AN EXACT ANALYTICAL MODEL FOR AN IOT NETWORK WITH MMPP ARRIVALS

Osama Salameh

Department of Computer Engineering, Arab American University, Palestine

ABSTRACT

Analytical modeling of the Internet of Things (IoT) networks is challenging. This is due to the presence of a large number of devices in these networks and the complexity of the priorities between different types of traffic. Taking these aspects into account, the objective of this paper is to analyze the performance of an IoT network where the IoT devices work independently of one another. To this end, we developed a novel multi-dimensional Continuous-Time Markov Chain (CTMC) model with threshold-based preemption. In this model, each IoT device is modeled as a Markov Modulated Poisson Process (MMPP) that can transmit regular and alarm packets. Alarm packets have higher priority over regular packets. To measure access to the channel between alarm and regular packets, we introduced a threshold parameter where the threshold is the number of packets in the alarm queue that indicates when preemption starts. The performance measures include blocking probability, the average delay of regular packets and alarm packets, discard rate , and success probability of regular packets. Comprehensive numerical analysis was conducted. Our results indicate that impact of the threshold on performance measures is higher on the boundary values of the threshold. The model was proven to be efficient in analyzing the performance of IoT networks on a wide range of parameter values. These results may be used in the future to develop and assess a protocol that utilizes a scheduling algorithm with a dynamic preemption threshold to optimize the performance of the IoT network.

KEYWORDS

Continuous-Time Markov Chain, IoT, MMPP.

1. INTRODUCTION

Internet of Things is a major advancement that enables a device to device communication. IoT is facilitated by the proliferation of new telecommunication technologies including 5G, where hundreds of thousands of devices can be deployed in one square kilometer. According to [1], the number of used IoT devices is expected to exceed 3.5 billion in 2023. The enormous number of devices in IoT networks causes substantial traffic that is different from traffic generated in ordinary telecommunication networks. This traffic is mainly uplink and consists of short messages [2].

Two types of models exist to represent the traffic in IoT networks: source traffic models and aggregated traffic models [3]. Source traffic models allow the capture of details of the operation of each device and thus are more accurate. Aggregated traffic models treat the traffic of all devices as a single stream. We used a source traffic model to represent devices in IoT networks of this study due to its higher level of accuracy.

Depending on the nature of the application, IoT devices can work in correlation with each other as well as without correlation. Devices can work in a correlated manner in response to a mass event such as a fire. If a fire spreads in a building, many fire sensors will send alarm messages

(packets) over the communication network. On the other hand, many health care sensors work in an uncorrelated manner, where a heart attack alarm packet, for example, indicates the status of a unique patient.

The IoT gateway is a key element in IoT architecture [4]. It can store incoming packets from IoT devices and transmit them over a communication network to IoT applications according to a designated scheduling discipline.

The rest of the paper is organized as follows: In section 2, we discuss related work. The objectives and system model are presented in section 3. In section 4, the Markov chain model is described in detail. The performance measures are given in section 5. In section 6, results are illustrated and in section 7, the paper is concluded.

2. RELATED WORK

In this section, we discuss some related analytical models. Uncoordinated IoT traffic has been considered in [8] where a channel is shared between IoT devices using a Fixed-Access Grant Time Interval scheduling scheme(AGTI). Performance analysis of this system is reduced to investigating one IoT device represented as a Markov Modulated Poisson Process (MMPP/D/1/K) queuing system. This work does not consider priority between regular and alarm traffic. Performance Analysis of a state-dependent MMPP/M/1 queue is analyzed in [9] and an analysis of a non-preemptive MMPP/M/1 queue is presented in [10]. In [11] and [12], the authors consider N IoT devices that share a channel according to a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme. In [11], each IoT device is modeled as an on-off process with its queue, but packet priorities are not considered. A combination of 2 Discrete-Time Markov Chain (DTMC) models is proposed in [12]. This work considers two classes of packets (high and low priority packets) in the context of IoT networks with one channel. Our study assumes is that packets of each class arrive according to separate Poisson processes.

A priority M/G/1 system is proposed to model IoT networks in [13] and [14]. In [13], a non-preemptive M/G/1 queuing model is proposed to model an aggregator. The queuing system has two separate queues: one for periodic traffic and another for alarm traffic, where each traffic class is modeled as a Poisson process. A preemptive M/G/1 system representing priority channel access is proposed in [14]. In this work, it is assumed that the IoT devices can be in one state only; either event-driven or normal data. Arriving packets of each class may be placed in separate queues before accessing the channel. Performance analysis of IoT is conducted using a Geo/G/1 queuing system in [4]. In this work, the devices are classified into massive and critical, where the packets generated by critical IoT devices have higher priority over packets generated by massive IoT devices.

3. OBJECTIVES AND SYSTEM MODEL

It is important to note that in all the models discussed above that considered priority in the model, the authors either reduce the analysis of the network to the analysis of one device or assume an aggregate traffic model where two separate Poisson processes are assumed to represent low and high priority traffics. In both these cases, the analysis is oversimplified and does not capture the fact that at any given moment, the offered traffic (low and high priority) rates depend on how many devices are in regular and alarm states.

Unlike the papers mentioned above, our proposed analytical model represents a network with the following features combined:

- Each IoT device is modeled as an MMPP with two states (regular and alarm).
- The model captures the dynamics where some devices may be in a regular state (generating regular packets) and others may be in an alarm state (generating alarm packets).
- Priority queuing is considered where alarm packets have priority over regular packets.
- Threshold-based priority is applied, allowing for a representation of preemptive and non-preemptive scheduling.

Performance analysis under these settings has been rarely been seen in the literature.

The objectives of this work are:

- To develop and test a novel multi-dimensional Continuous-Time Markov Chain (CTMC) model to represent the IoT network under consideration based on the superposition of MMPPs is proposed.
- To investigate the effect of preemption based on the number of alarm packets in the buffer.
- To conduct a comprehensive performance analysis based on the proposed model.

In this study, we considered an IoT network with N identical uncorrelated IoT devices connected to a gateway. We assumed that the connection was error-free and that no collision between packets generated by different IoT devices could happen. A gateway uses one channel to transmit arriving packets from IoT devices to a sink. We assumed that each device could have two states: regular and alarm. Furthermore, we assumed that the packets generated during the alarm state had priority over packets generated during the regular state. Arriving packets can be stored in buffers if the channel is not available. We assumed that the gateway has two buffers: one for regular traffic and another for alarm traffic.

In our model, preemption based on a threshold scheme was applied, where the threshold is the number of alarm packets in the buffer. If the number of alarm packets (high priority) is below the threshold, then non-preemptive priority is applied. Otherwise, preemptive priority is used. Preemption based on this threshold allows for the integration of both cases of preemptive and non-preemptive priorities into a single model. Threshold-based preemption has been considered in the literature to control starvation of low priority traffic. In [5], three schemes are investigated where the threshold is based on either remaining service time, or on elapsed service time, or on the ratio of elapsed to total service time of low priority jobs. In [6], the threshold is based on the number of preempted low priority tasks by high priority tasks and the number of channels occupied by emergency traffic in [7].

3.1. IoT device model

Each device is modeled as an MMPP with two states: regular and alarm (See **Fig. 1**) as in [15]. We assume that during regular or alarm states, packets arrive according to a Poisson process at a rate of λr or λa, respectively. Also, the service time for the regular or alarm packets is exponentially distributed at a rate of $\mu_2$or μ_1, respectively. A device switches from the alarm state to the regular state at a rate of $\sigma_1$and from the regular to alarm state at a rate of σ_2. The switching times σ_1 and $\sigma_2$are exponentially distributed as well.

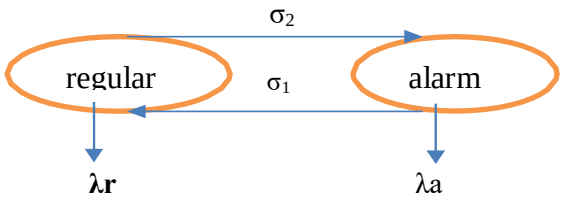

Fig. 1. IoT device MMPP model

3.2. Superposition of N MMPPs

In source traffic modeling of IoT traffic, the processes of individual MMPPs have to be superimposed. The composite process is also anMMPP and can be quite complex. This complexity is reduced if the MMPPs are identical. We integrate the superposition of N 2-state MMPPs as defined in [16] in our CTMC model. The graphical representation of the composite process for this case is shown in **Fig. 2.** As can be seen, the composite process has only N + 1 states, where the state (N-i) (0≤ I≤ N) is the number of devices in a regular state. In-state N, all the devices are in regular state, and the rate generated by all devices is**Nλr**. In state N-1, N-1 devices generate regular traffic at a rate of**(N-1) λr** and one device generates alarm traffic at a rate of **λa,** and so on until state 0, in which all devices generate alarm traffic at a rate of N**λa**

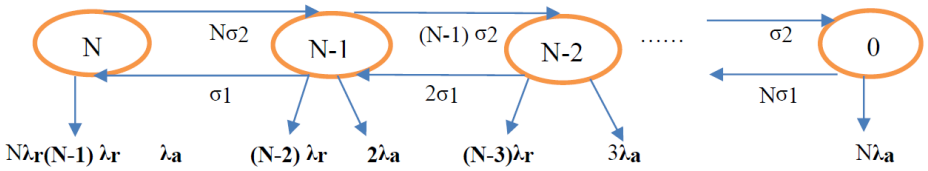

Fig. 2. Superposition of N 2-state MMPPs

3.3. Queuing Model

In this paper, we consider a queuing model (See **Fig. 3**) that consists of one server representing a channel to transmit the packets with 2 queues. One queue has a capacity of B1 to hold the arriving alarm packets (i.e. packets generated by devices in the alarm state). Likewise, the capacity of the second queue holding the regular packets is B2. If the alarm buffer is full, an arriving regular packet is lost and if the regular buffer is full, an arriving alarm packet is lost. The scheduling discipline of packets in each queue is First In First Out (FIFO).

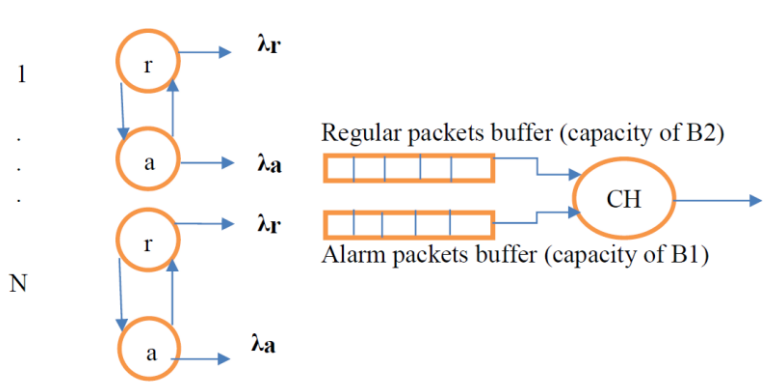

Fig. 3. Queuing Model

To control access to the channel between alarm and regular packets, we introduce a threshold parameter: Thrs. The threshold is the number of packets in the alarm queue ($0 \leq Thrs. \leq B1$) that indicate when preemption starts. If a regular packet is in transmission, the alarm queue is empty, and the Thrs. = 0.Then, an arriving alarm packet will preempt the regular packet and the alarm packet seizes the channel. If Thrs. = 1, an arriving alarm packet preempts a regular packet in transmission only if another alarm packet is already waiting in the alarm queue. Likewise, when Thrs. = 2, the regular packet in transmission gets preempted by an arriving alarm packet only if the number of packets in the alarm queue equals 2, and so on. If an arriving alarm packet does not preempt a regular packet in transmission because the threshold is not met, then the arriving alarm packet waits in the alarm buffer. It is important to note that when an alarm packet occupies the channel, all the alarm packets in the queue will be transmitted one by one until the queue is empty since alarm packets have higher priority. The preempted regular packet will rejoin the regular queue if space is available and get discarded otherwise.

The introduction of the threshold parameter allows us to model the boundary cases of preemptive and non-preemptive priorities using one CTMC model. If Thrs. = 0, a queuing system with preemptive priorities is modeled whereas when Thrs. = B1 the system becomes one with non-preemptive priorities. In the latter case, an arriving alarm packet will be blocked if the alarm buffer is full. All model parameters are presented in Table 1.

Table 1. Model parameters

λ_a	Packet arrival rate from one device in alarm state
λ_r	Packet arrival rate from one device in regular state
$\mu 1$	Transmission rate of alarm packets
$\mu 2$	Transmission rate of regular packets
N	Number of IoT devices
Thrs.	System threshold at which preemptive priority is activated
B_1	Capacity of buffer holding alarm packets
B_2	Capacity of buffer holding regular packets
$\sigma 1$	Transition rate from alarm state to regular state
$\sigma 2$	Transition rate from regular state to alarm state

4. MARKOV CHAIN MODEL

In this section, we discuss the developed multidimensional Markov Chain that captures the dynamics of operation of the IoT network as described above. Let N be the number of IoT devices in the network. We model the network using a four-dimensional CTMC. In this CTMC, a state is given by x = (i, j, k, m) where i is the number of devices in the alarm state and the number of devices in the regular state is $N - i$. The number of packets in the alarm buffer is j and the number of packets in the regular buffer is k. The status of the channel is m = 0,1,2 where 0 indicates that the channel is not occupied, 1 indicates that the channel is occupied by an alarm packet and 2 indicates that the channel is occupied by a regular packet. The capacity of the alarm buffer is B1 and the capacity of the regular buffer is B2. The number of states in this CTMC is

$$(2(B2+1)(Thrs+1)+(B2+1)(B1-Thrs)+1)(N+1) \qquad (1)$$

where the term (N+1) represent the number of states of the composite process as described in section 3.2. Next, we provide a complete specification for the infinitesimal generator matrix Q. The transition rates from a state x = (i, j, k, m) to all possible states are defined in Table 2. As can be seen, we distinguish 12 transition cases as follows:

- In the first case, a transition occurs from a state (i, j, k, m) to state (i, j + 1, k, m) at a rate of iλa. An arriving alarm packet joins the alarm buffer if the number of packets in the alarm buffer is less than the threshold and the channel is busy.
- In case (2), and arriving alarm packet joins the alarm buffer if the channel is busy transmitting another alarm packet and the alarm buffer is not full.
- In case (3), and arriving alarm packet interrupts the regular packet in transmission if the number of alarm packets equals the threshold and the threshold is less than buffer size B1. In case the threshold equals B1, the system behaves like an ordinary priority system with two classes and no preemption. The interrupted regular packet rejoins the regular buffer.
- Case (4) differs from the case (3) in that the interrupted regular packet is discarded from the system if the buffer is full. In cases (1)-(4) above, an arriving alarm packet is blocked if the buffer is full.
- In case (5), an alarm packet seizes the channel upon arrival if both buffers are empty and the channel is idle.
- In case (6), the number of devices in the regular state is (N − i). Then, an arriving regular packet joins the buffer at a rate of (N − i)λr if the buffer is not full and the channel is busy.
- In case (7), and arriving regular packet seizes the channel if both buffers are empty and the channel is idle.
- In case (8), the packet in transmission releases the channel at a rate of μm, (m = 1,2) and an alarm packet seizes the channel decreasing the buffer content by 1, if the alarm buffer is not empty.
- Case (9) differs from the case (8) in that when a packet finishes transmission, a regular packet seizes the channel if the alarm buffer is empty and the regular buffer is not empty.
- In case (10), the number of devices in the alarm state is decreased by 1 at a rate ofiσ1.
- In case (11), the number of devices in the alarm state increased by 1 at a rate of (N − i) σ2.
- In the last transition case, the system becomes empty at a rate of μm if the channel is busy transmitting a packet, and both buffers are empty. The transition rate between states other than those described above is 0.

Table 2. Transition Rate Table

	To State	Rate	Condition
1	i, j + 1, k, m	iλa	m = {1,2}, j <Thrs., Thrs. ≤ B1
2	i, j + 1, k, 1	iλa	m=1, B1 > j ≥ Thrs., Thrs.<B1
3	i, j, k + 1, 1	iλa	m = 2, j = Thrs., Thrs.< B1, k < B2
4	i, j, k, 1	iλa	m = 2, j = Thrs., Thrs.< B1, k = B2
5	i, j, k, 1	iλa	j=k=m=0
6	i, j, k + 1,m	(N − i)λr	k<B2 ,m=1,2
7	i, j, k, 2	(N − i)λr	j=k=m=0
8	i, j − 1, k, 1	μm	j > 0, m = 1, 2
9	i, j, k − 1, 2	μm	k > 0, j = 0, m = 1, 2
10	i – 1 , j, k, m	iσ1	
11	i + 1, j , k, m	(N − i)σ2	
12	i, 0, 0, 0 0	μm Otherwise	j = k = 0, m = 1, 2

To compute the performance measures defined in section 5, we first need to obtain the steady-state probability vector π. This can be done by solving the equations:

$$\pi Q = 0, \sum_{\pi_x \in S} \pi_x = 1 \tag{2}$$

Where πx is the probability of state x and S is the set of all states in the proposed CTMC.

The proposed CTMC is a quasi-birth-death (QBD) process. In QBD processes, the state space is divided into levels and each level has a many states (or phases). In our CTMC, the level is represented by the number of stations in the alarm state i. In level 0, no station is in the alarm state (all the stations are in the regular state). In level 1, one station is in the alarm state, and so on. The phase is represented by the triplet (j,k,l). The importance of QBD processes is that it has efficient computation algorithms to obtain steady-state probabilities of the CTMC. We use a computation algorithm as defined in [17].

5. PERFORMANCE MEASURES

Based on the steady-state probability vector obtained, several performance measures can be computed. We are interested in: blocking probability of both regular packets (*Bpr)* and alarm packets (*Bpa)*, discard rate (α) of regular packets, the average delay in the queue for both regular *(E*[*Dr*]) and alarm packets (*E*[*Da*]), and in success probability of regular packets (*Sp)*.

Following the definition of blocking probability for MMPP arrivals [18], the blocking probability of regular traffic is given as

$$Bp_r = \frac{\sum_{i=0}^{N-1} \sum_{j=0}^{B_1} (N-i)\lambda_r \pi_{(i,j,B_2,m)}}{\sum_{i=0}^{N-1} \sum_{j=0}^{B_1} \sum_{k=0}^{B_2} (N-i)\lambda_r \pi_{(i,j,k,m)}} \tag{3}$$

where m= 0,1,2. Likewise, the blocking probability of the alarm traffic can be computed using

$$Bp_a = \frac{\sum_{i=1}^{N} \sum_{k=0}^{B_2} i\lambda_a \pi_{(i,B1,k,m)}}{\sum_{i=1}^{N} \sum_{j=0}^{B_1} \sum_{k=0}^{B_2} i\lambda_a \pi_{(i,j,k,m)}} \tag{4}$$

The number of packets in the regular queue is given as

$$N_r = \sum_{i=0}^{N} \sum_{j=0}^{B_1} \sum_{k=1}^{B_2} k\, \pi_{(i,j,k,m)}, \quad m = 1,2 \tag{5}$$

The number of packets in the alarm queue is given as

$$N_a = \sum_{i=0}^{N} \sum_{j=1}^{B_1} \sum_{k=0}^{B_2} j\, \pi_{(i,j,k,m)}, \quad \mathrm{m} = 1,2 \tag{6}$$

For equations (5) and (6), the value of m $\neq 0$ because when the channel is idle (m = 0) there are no packets in the corresponding queue. The throughput for regular traffic is given as

$$\eta_r = \sum_{i=0}^{N} \sum_{j=0}^{B_1} \sum_{k=0}^{B_2} \pi_{(i,j,k,2)}\, \mu_2 \tag{7}$$

The discard rate is the rate at which regular packets are interrupted and discarded due to the arrival of alarm packets. Note that discarding a regular packet is different from interrupting it. A regular packet in transmission can get interrupted several times where it rejoins the buffer if space is available. It is discarded only when it is interrupted and the buffer is full. This rate is given as

$$\alpha = \sum_{i=1}^{N} i\lambda_a\, \pi_{(i,Thrs,B_2,2)} \tag{8}$$

where Thrs< B1. The success probability for regular traffic is given as

$$S_p = \frac{\eta_r}{\lambda_r^e} \tag{9}$$

where is the effective arrival rate?. is λ_r^e given as

$$\lambda_r^e = \sum_{i=0}^{N-1} \sum_{j=0}^{B_1} \sum_{k=0}^{B_2-1} (N-i)\, \lambda_r \pi_{(i,j,k,m)} \tag{10}$$

where m = 0, 1, 2. The effective arrival rate of the alarm traffic is given by

$$\lambda_a^e = \sum_{i=1}^{N} \sum_{j=0}^{B_1-1} \sum_{k=0}^{B_2} i\lambda_a^e\, \pi_{(i,j,k,m)} \tag{11}$$

where m = 0,1,2. Lastly, the average delay of regular and alarm packets can be computed using the following equations:

$$E[D_r] = N_r/\lambda_r^e, \quad E[D_a] = N_a/\lambda_a^e \tag{12}$$

6. RESULTS

We assume that the values of packet arrival rates in alarm or regular states are as follows: λa = 0.125 pkt/ms, λr = 0.0125 pkt/ms [8]. Also, we assume service rates of alarm and regular packets are μ1 = 1 pkt/ms, μ2 = 0.05 pkt/ms and the transition rate from alarm state of a device to regular state is σ1 = 0.01 (ms−1) and from regular state to alarm state of a device is σ2 = 0.001(ms−1). These values of σ1, σ2 reflect the fact that a device spends more time in the regular state than in the alarm state.

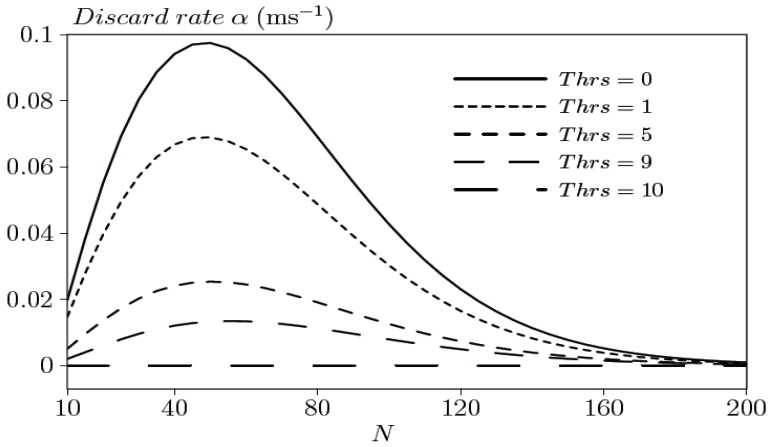

Fig. 4. Discard rate (α) of regular packets versus number of IoT devices (N) for different threshold values (Thrs.) where B1 = B2 = 10, λa = 0.125, λr =0.0125, μ1 =1, μ2 =0.05, σ2 =0.001, σ1 =0.01.

In **Fig. 4**, we show the discard rate (α) versus the number of IoT devices (N) for different threshold values (Thrs.). This curve can be divided into two parts; in the first part, for smaller values of N, increasing N increases the alarm traffic causing the increase of discarded regular packets due to a full buffer. In the second part, for higher values of N, we notice that the decrease in the discard rate is due to the inability of regular packets to seize the channel. As expected, increasing the threshold decreases the amount of discarded regular packets. Surprisingly, we notice a large difference in the discard rates at thresholds of 0 and 1. When Thrs. = 0, the system operates as an ordinary system with preemption i.e. an arriving alarm packet will interrupt a regular packet in transmission. When Thrs. = 1, an arriving alarm packet will interrupt the regular packet in transmission only when the number of packets in the alarm queue equals 1.

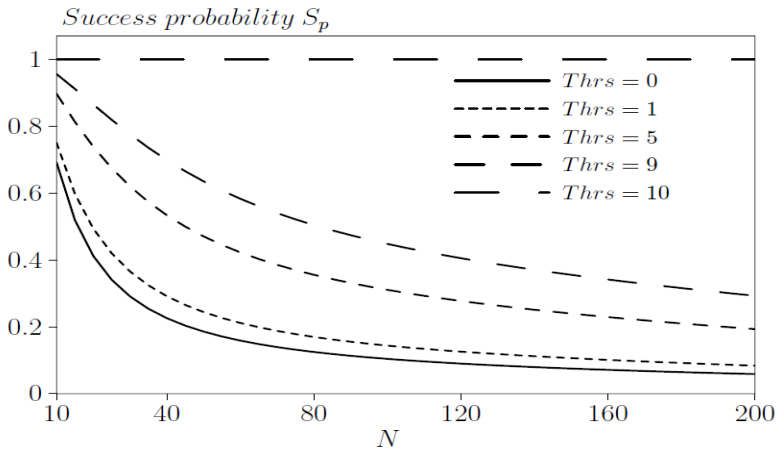

Fig. 5. Success probability (S*p*) of regular packets versus number of IoT devices (N) for different threshold values (Thrs.) where B1 = B2 = 10, λa =0.125, λr =0.0125, μ1 =1, μ2 =0.05, σ2 =0.001, σ1 =0.01.

The Success probability (S*p*) versus the number of IoT devices (N) for different threshold values is presented in**Fig. 5**. Increasing N decreases the success probability for thresholds not equal to B1. This decrease is in line with **Fig. 4,** where fewer regular packets can be in the transmission state. When the threshold equals B1, no interruptions of regular packets can happen, that is the system becomes an ordinary system with no preemptive priority and all admitted regular packets will be eventually transmitted. Also, interestingly, we notice a large difference in success probability for values of the threshold B1 and B1 − 1. At Thrs. =B1 − 1, and arriving alarm

packet interrupts a regular packet in transmission if the alarm queue has B1 − 1 packet, whereas it cannot when the threshold equals B1 and the queue is full. This illustrates that the effect of preemption is important even when the change of the threshold is only 1.

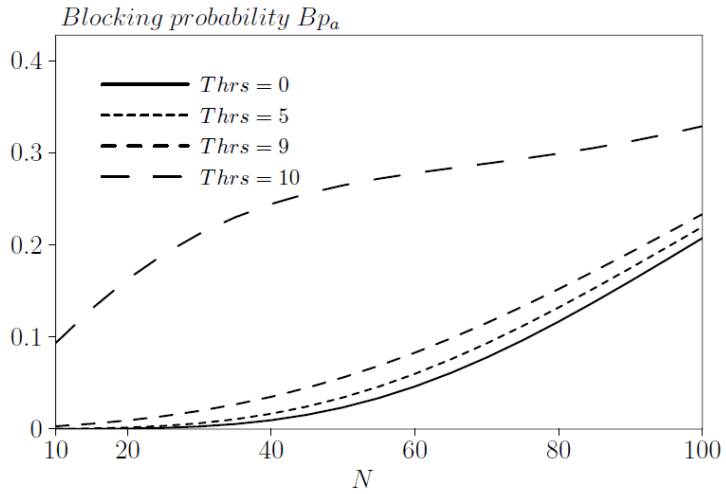

Fig. 6. Blocking probability of alarm packets (Bpa) versus number of IoT devices (N) for different threshold values (Thrs,) where B1 = B2 = 10, λa = 0.125, λr =0.0125, μ1 =1, μ2 =0.05, σ2 =0.001, σ1 =0.01.

In **Fig. 6**, we show the blocking probability of the alarm traffic Bpa versus the number of IoT devices (N)at different thresholds. As expected, the blocking probability of the alarm traffic increases with an increasing N. Moreover, we notice a large increase in blocking probability when Thrs. = B1 in comparison with Thr. = B1 − 1. Again, this is due to the fact no preemption is allowed for Thrs. = B1.

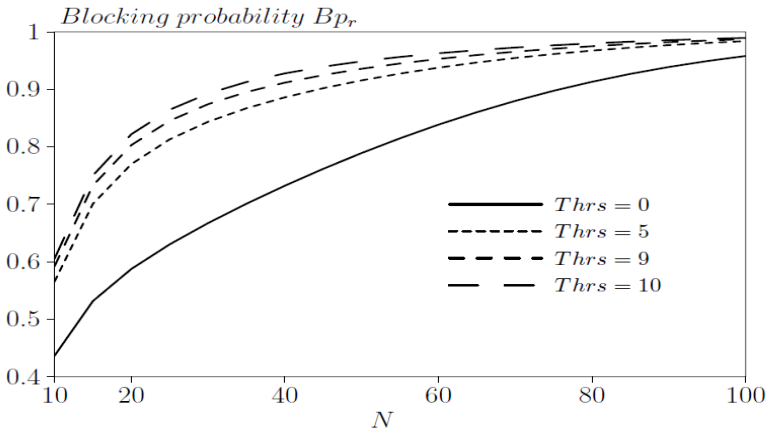

Fig. 7 Blocking probability of regular packets (Bpr) versus number of IoT devices (N) for different threshold values (Thrs.) where B1 = B2 = 10, λa = 0.125, λr =0.0125,μ1 =1,μ2 =0.05,σ2 =0.001,σ1 =0.01.

In **Fig. 7**, the blocking probability of regular packets Bpr versus the number of IoT devices (N) at different thresholds (Thrs.) is presented. Again, increasing N increases the high priority alarm traffic generated, and the blocking probability for regular packets increases. Also, we notice that increasing the threshold increases the blocking probability, which is counter- intuitive. This is because fewer packets get discarded in this case, which, in turn, increases the number of packets

in the regular queue, and the blocking probability increases. It is important to note that the generated traffic from IoT devices is independent of the values of buffer sizes and the value of the threshold.

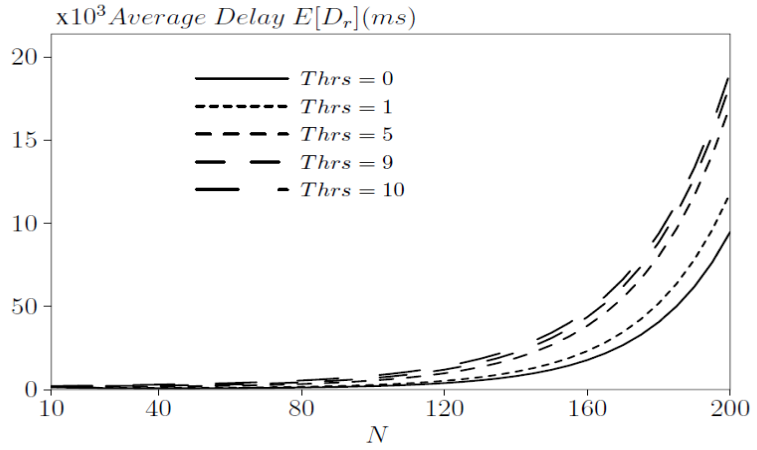

Fig. 8.Average delay of regular packets versus number of IoT devices (N) for different Threshold values (Thrs.) where B1 = B2 = 10, λa = 0.125, λr =0.0125, μ1 =1, μ2 =0.05, σ2 =0.001, σ1 =0.01.

The average delay of the regular (alarm) packets versus the number of devices (N) for different threshold values (Thrs) is shown in**Fig. 8** and **Fig. 9**. In **Fig. 8**, we notice that when N increases the delay of regular packets increases exponentially. This is since the buffer becomes almost full and the effective arrival rate decreases. Another observation is that increasing the threshold decreases the discard rate and the delay of regular packets increases. In **Fig. 9**, for smaller values of N, the effect of increasing the threshold is significant on the delay of alarm packets as it forces more alarm packets to wait. As expected, for larger values of N, this effect is no longer noticed since the channel is busy mainly transmitting alarm packets. The delay converges to a limiting value because both the number of alarm packets in the queue and the effective arrival rate of alarm packets reach their limiting values too.

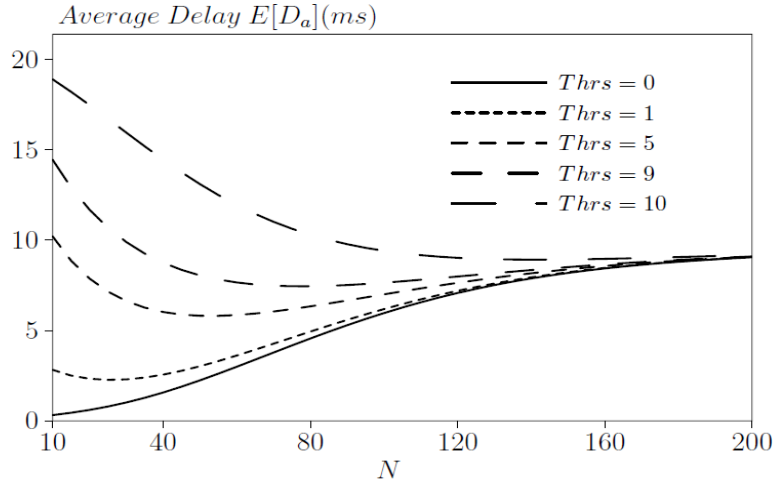

Fig. 9. Average delay of alarm packets versus number of IoT devices (N) for different threshold values (Thrs.) where B1 = B2 = 10, λa = 0.125, λr =0.0125, μ1 =1, μ2 =0.05, σ2 =0.001, σ1 =0.01.

It is important to note that if the ratio σ1/σ2 is kept fixed, the specific values of the rate to generate an alarm σ1 have little effect on performance measures.

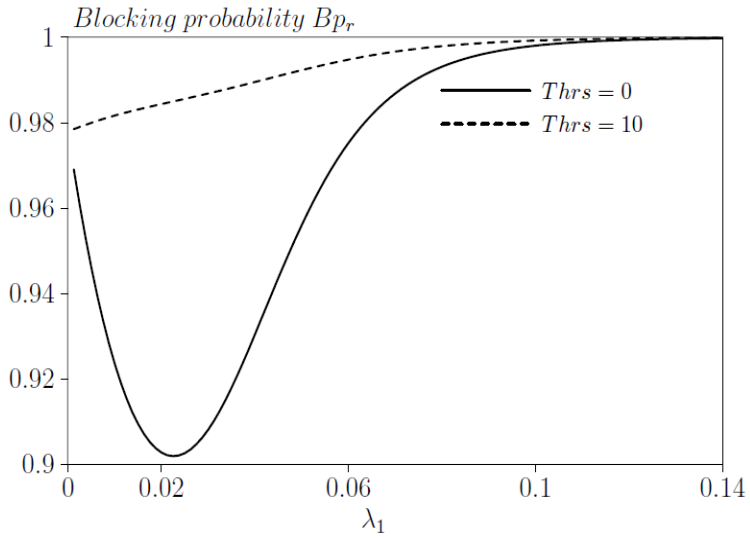

Fig. 10. Blocking probability of regular packets versus the arrival rate of alarm traffic (λa) for different threshold values (Thrs.) = 0, B1, N = 200, λr =0.0125, μ1 =1, μ2 =0.05, σ2 =0.001, σ1 =0.01.

Next, we concentrate on analyzing the system when Thrs. = 0, B1. These threshold values represent the cases of preemptive and non-preemptive priorities, respectively. In **Fig. 10**, the blocking probability of the regular traffic versus the arrival rate λa for different values of the thresholds 0 and B1 is shown. It can be seen for this parameter set that the blocking probability decreases first before it increases again when preemptive scheduling is employed (Thrs. = 0). This decrease is due to increasing discarded packets from the system (as can be seen in **Fig. 11**) that also decreases the queue length of the regular traffic (as can be seen in **Fig. 12**).

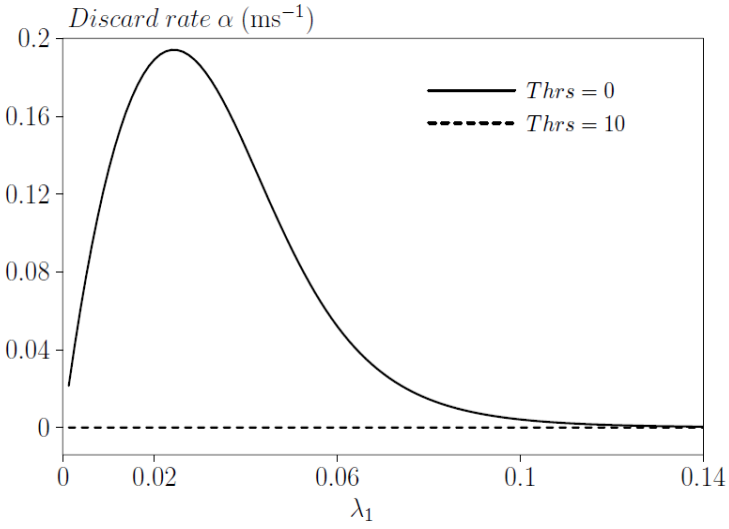

Fig. 11. Discard rate (α) of regular packets versus the arrival rate of alarm traffic (λa) for different threshold values; Thrs. = 0, B1; N = 200, λr = 0.0125, μ1 =1, μ2 =0.05, σ2 =0.001, σ1 =0.01.

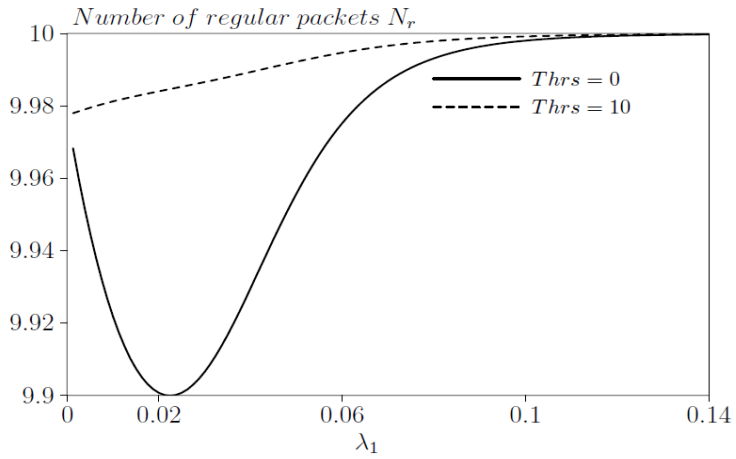

Fig. 12. Number of regular packets (N_r) versus the arrival rate of alarm traffic (λ_a) for different threshold values; Thrs = 0, B1; N = 200, λ_r =0.0125, μ_1 =1, μ_2 =0.05, σ_2 =0.001, σ_1 =0.01.

It is important to note that all the numerical results in this paper have been extensively verified by simulations using the direct method version of the stochastic simulation algorithm as described in [19]. This method is computationally efficient and exact. Using this algorithm, we first generate all the states in the state space. Next, for a given state x, the transition rates λi(i=1,…,d) to all possible states are determined and the time until the next transition is simulated by drawing from an exponential distribution with mean $1/\lambda$ where $\sum_{\{i=1\}}^{d} \lambda i$.The transition to the next state is simulated by generating a random number from a uniform distribution and choosing the transition type with probability Prob(transition = i) = $\lambda i/\lambda$.

7. CONCLUSION

In this paper, we developed a CTMC for an IoT network where N IoT devices share one channel. The model takes into account preemptive and non-preemptive priority between alarm and regular packets. The impact of model parameters on the performance of the system has been thoroughly investigated. Our results indicate that the impact of the threshold on performance measures is higher on the boundary values of the threshold. The model has proven to be efficient in analyzing the performance of IoT networks on a wide range of parameter values. One distinguishing feature of our model is that it allows making a realistic estimation of the performance measures of IoT networks for a given number of IoT devices. The numerical results show that for a specific parameter set, we can determine the maximum value of N that results in acceptable measures for alarm and regular traffics. The model can be used by practitioners who investigate these kinds of IoT networks where IoT devices are uncorrelated. In our future work, we intend to develop and assess a protocol that utilizes a scheduling algorithm with a dynamic preemption threshold to optimize the performance of the IoT network.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] S. Mattisson, “An overview of 5G requirements and future wireless networks: Accommodating scaling technology,” IEEE Solid-State Circuits Mag., vol. 10, no. 3, pp. 54–60, 2018.

[2] M.Centenaroand, L.Vangelista,"AstudyonM2Mtrafficanditsimpact on cellular networks," 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, 2015, pp. 154-159.
[3] M.Laner, P. Svoboda, N. Nikaein and M. Rupp, "Traffic Models for Machine Type Communications," ISWCS 2013; The Tenth International Symposium on Wireless Communication Systems, Ilmenau, Germany, 2013, pp. 1-5.
[4] S.Alqahtani, 'Performance evaluation of a priority-based resource allocation scheme for multiclass services in IoT", Int J Commun Syst. vol. 32, no 18, 2019.
[5] Y.Z.Cho, C.K.Un," Analysis of the M/G/1queueunderacombined preemptive/non-preemptive priority discipline," IEEE Trans. Commun., vol. 41, no. 1, pp. 132–141, 1993.
[6] S.Drekic and D. A. Stanford, "Reducing delay in preemptive repeat priority queues", Oper. Res., vol. 49, no. 1, pp. 145–156, 2001.
[7] J.Zhou , C.Beard," A Controlled Preemption Scheme for Emergency Applications in Cellular Networks", IEEE Trans on Vehicular Technology, vol. 58, no. 7, pp. 3753-3764, 2009.
[8] M.Zarrini A. Ghasemi, "Loss and delay analysis of non-Poisson M2M traffic over LTE networks", Transactions on emerging telecommunication technologies,vol.29, issue 2, 2018.
[9] R.Sakthi, V.Vidhya, K.Mahaboob H. Sherieff, "Performance Measures of State Dependent MMPP/M/1 Queue", International Journal of Engineering and Technology, vol. 7 , no. 4.10, pp. 942-945, 2018.
[10] B.Venkataramania, S. Bose, K.R. Srivathsan, "Queuing analysis of a non-preemptive MMPP/D/1 priority system", Volume 20, Issue 11, Pages 999-1018, 1997.
[11] S.B.Yaala, F.´oleyre, R.Bouallegue," Performance Modeling of IEEE 802.15.4-TSCH with Shared Access and ON-OFF traffic," 2018 14th International Wireless Communications and Mobile Computing Conference (IWCMC), Limassol, 2018, pp. 352-357.
[12] L. Guntupalli, H. Farag, A. Mahmood, M. Gidlund, "Priority- Oriented Packet Transmissions in Internet of Things: Modeling and Delay Analysis," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1-6.
[13] N.Kouzayha, M. Jaber and Z. Dawy, "Measurement-Based Signaling Management Strategies for Cellular IoT," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1434-1444, 2017.
[14] S. Bhandari, S. K. Sharma and X. Wang, "Latency Minimization in Wireless IoT Using Prioritized Channel Access and Data Aggregation," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6.
[15] H. Thomsen, C. N. Manchon and B. H. Fleury, "A traffic model for machine-type communications using spatial point processes," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-6.
[16] Fischer, W., Meier-Hellstern, K. "The Markov-modulated Poisson process (MMPP) cookbook", Performance Evaluation, vol. 18 issue 2, pp.149–171. 1993.
[17] Osama Salameh, Koen De Turck , Herwig Bruneel, Chris Blondia •, Sabine Wittevrongel , "Analysis of secondary user performance in cognitive radio networks with reactive spectrum handoff",Telecommun Syst vol. 65, pp.539–550, 2017.
[18] Cao Y, Sun H, Trivedi K, "The effect of access delay in capacity-on-demand access over a wireless link under bursty packet-switched data",Performance Evaluation vol. 57, issue 1, pp. 69-87, 2004.
[19] Banks H.T, Anna Broido, Brandi Canter, Kaitlyn Gayvert, Shuhua Hu, Michele Joyner, Kathry Link, "Simulation Algorithms for Continuous Time Markov Chain Models", International Workshop on Simulation and Modeling related to Computational Science and Robotics Technology (SiMCRT2011), pp. 3-18, Kobe university, Japan, 2011.

AUTHOR

Osama Salameh was born in Schongau, Germany. He received his M.Sc.degreeand a Ph.D.degree in Computer Engineering from Odessa State Polytechnic University, Ukraine in 1990 and 1996 respectively. During his career, he was employed by several universities in Palestine and Jordan. He is a member of the SMACS research group at Ghent University and a full-time associate professor at the Arab American University. His main research interests include queuing models and performance evaluation of computer and telecommunication networks.