AN INFINITE PHASE-SIZE BMAP/M/1 QUEUE AND ITS APPLICATION TO SECURE GROUP COMMUNICATION

Hiroshi Toyoizumi
Waseda University
Nishi-waseda 1-6-1, Shinjuku, Tokyo 169-8050

Keywords: Secure group communication, rekeying, Markovian arrival process, queue, performance evaluation.

Abstract: We derive the bounds of the mean queue length of an infinite phase size $BMAP/M/1$ queue which has an $M/M/\infty$-type phase transition, and use them to evaluate the performance of secure group communication. Secure communication inside a groups on an open network is critical to enhance the internet capability. Extending the usual matrix analysis to the operator analysis, we derive a new estimation of the degradation of secure group communication model.

1 INTRODUCTION

One-to-one secure communication has been widely used on the internet such as, SSL (Security Socket Layer) (Thomas, 2000). As the internet grows all over the world, we get the freedom to communicate with anyone, anytime, anywhere. On the internet, we can easily make a community which shares common interest. Inside the community, sometimes we need a secure communication to protect our own interest. For example, we need a secure group communication for pay TV on the internet, or sharing the business confidential information on the internet.

These secure group communication might be solved by one-to-one secure communication by specifying one sender and one receiver. However, if we use one-to-one model in a group, the sender has to encrypt the information using different individual keys that was securely delivered to each receivers before hand. When the group size is large and we need real-time encryptions, the one-to-one model will not be scalable. For example, consider an internet broadcasting company which has 10,000 subscribers. The server has to encrypt the data 10,000 times with different keys. Thus, it is impossible for streaming type real-time applications like Pay TV or teleconference.

One of the solutions to this problem is to share a common symmetric group key among the group, and use it when sending information (Harney and Muckenhirn, 1997a; Harney and Muckenhirn, 1997b). This will reduce the number of encryptions dramatically. However, when a participant leaves or joins the group, the shared group key has to be renewed and send it securely. This will be the potential overhead to the server managing the keys. For example, if the population size of the group is 10,000, then the number of encryption of the new group key would be 10,000 when a member leave the group. Not only the processing time for the encryptions, but the time required to deliver the new group key would be the potential security problem, since during the delivery, the communication among the group can be eavesdropped by the participants who left the group. Thus estimating the time required to renew the group key is essential for the performance of the secure group communication.

Since the rekeying process takes place when joins and leaves occurs with as many encryptions as the size of group, the natural choice to evaluate the system is to use the Batch Markovian Arrival Process (BMAP) (Latouche and Ramaswami, 1999; Makimoto, 2001). The phase is corresponding to the size of the group. However, the ordinary BMAP queue deals with the finite phase size, while our problem has potentially the large or infinite size of phase. Tweedie and Senguputa extended the idea of matrix analysis to the operator analysis and derive the so-called operator geometric and matrix exponential distribution (Sengupta, 1989; Tweedie, 1982; Latouche and Ramaswami, 1999). The other choice to analyze the problem is to model the group size by the state depending quasi-birth-and-death process (Latouche and

Toyoizumi H. (2006).
AN INFINITE PHASE-SIZE BMAP/M/1 QUEUE AND ITS APPLICATION TO SECURE GROUP COMMUNICATION.
In *Proceedings of the International Conference on Security and Cryptography*, pages 283-288
DOI: 10.5220/0002095202830288

Ramaswami, 1999) with infinite phase space, which corresponds to the the number of encryptions to be processed. However, we have the same difficulty due to the infinite size of the phase space.

In this paper, we extend the matrix argument to operator argument in $BMAP/M/1$ queues to evaluate the number of encryptions in the secure communication model sharing a common symmetric group key.

In Wong (Wong et al., 2000) and RFC2627 (Wallner et al., 1999), the authors introduce a concept of subgroup in the secure group communication to reduce the number of encryptions. They showed that using additional subgroup keys, they can decrease the number of encryptions of the group key, dramatically. The subgroup keys are exclusively shared in its subgroup, and used to encrypt a new group key. In (Toyoizumi and Takaya, 2004), the authors discussed the marginal distribution of number of encryptions can be Poisson distribution. However, as always the correlation of the process will greatly affect the system. These alternatives may be analyzed by the similar method of ours by modeling the subgroup appropriately.

2 $BMAP/M/1$ QUEUEING MODEL

We use the word "customer" to indicate the participants of a group sharing secure communication. Let U_n be the n-th customer of the group, T_n be the join (arrival) time and S_n be the sojourn time of U_n in the group. We assume the point process of joins of customer $\{T_n\}$ is Poisson process with its rate λ. Also, assume the sojourn time S_n has independent and identical exponential distribution with its mean $E[S_n] = 1/\mu$. There is no limit of the number of customers in the group.

When a customer leaves the group, the group has to change the group key to keep the security inside the group. The new group key has to be encrypted by individual private keys and to be delivered to the customers in the group. Thus, at the leaves of customers, we need to encrypt the new key as many as the number of customers in the groups left behind. We assume the time required to encrypt the new key is independent and exponentially distributed with the mean $1/\sigma$. In the following, we use the word "job" to indicate the workload required to encrypt the new group key.

Remark 1. *We neglect the jobs required at the join of new customers for simplicity. The key renewal at the join will guarantee the confidentiality of the past information, which is not always important. Also, the number of the encryptions at the customer's join is always* 2 *since we can use the old group key to send the new one to the existing customers, so it is easy to modify our approach.*

A batch of jobs arrive at the leave of a customer, so we can model the arrival of the jobs in the form of Batch Markovian Arrival Process (BMAP)(Makimoto, 2001). Let $L(t)$ be the number of customers in the group, and $M(t)$ be the number of jobs in the system (key encryption server) at time t. By the above assumptions, it is easy to see the process $X(t) = (L(t), M(t))$ is a Markov process. Denote the joint stationary probability by $\pi_{l,m} = P[L = l, M = m]$ when the utilization of this system is less than 1. Also, we use the following infinite dimension vectors of probabilities:

$$\pi_m = (\pi_{m0}, \pi_{m1}, ...).$$
$$\pi = (\pi_0, \pi_1, ...).$$

We treat the number of customers in the group $L(t)$ as the phase of the system. These stationary probability vectors should satisfy the following stationary equation.

$$\pi \mathbf{Q} = \mathbf{0}, \tag{1}$$

where $\mathbf{Q}$ is the infinitesimal generator of the Markov Process $X(t) = (L(t), M(t))$. Since l jobs will be arrived at the server simultaneously when a customer left l customers in the group, the matrix $\mathbf{Q}$ can be represented in the matrix form as

$$\begin{pmatrix} \mathbf{D}_0 & \mathbf{D}_1 & \mathbf{D}_2 & \mathbf{D}_3 & \cdots \\ \sigma\mathbf{I} & \mathbf{D}_0 - \sigma\mathbf{I} & \mathbf{D}_1 & \mathbf{D}_2 & \cdots \\ & \sigma\mathbf{I} & \mathbf{D}_0 - \sigma\mathbf{I} & \mathbf{D}_1 & \cdots \\ & & \sigma\mathbf{I} & \mathbf{D}_0 - \sigma\mathbf{I} & \ddots \\ & & & \ddots & \ddots \\ & & & & \end{pmatrix}.$$

The matrix $\mathbf{D}_l$ is representing the transition of the process by the l-job arrival, and having the form as

$$\mathbf{D}_l = \begin{matrix} \\ l+1 \end{matrix} \overset{l}{\begin{pmatrix} & \vdots \\ \cdots & (l+1)\mu \\ & \end{pmatrix}}, \tag{2}$$

for $l \geq 1$, and

$$\mathbf{D}_0 = \begin{pmatrix} -\lambda & \lambda & & & \\ \mu & \lambda - \mu & \lambda & & \\ & 0 & -\lambda - 2\mu & \lambda & \\ & & \ddots & \ddots & \ddots \end{pmatrix}, \tag{3}$$

where those components which are not indicated are all zero.

Remark 2. *It is easy to see that the matrix* $\mathbf{D} = \sum_{l=0}^{\infty} \mathbf{D}_l$*, which is the generator of the phase transitions, is the infinitesimal generator of an* $M/M/\infty$ *queue, and its stationary probability vector is Poisson distribution with its mean* λ/μ*.*

These matrices are of the infinite size, so the ordinary matrix analytic methods cannot be readily applied. However, the parallel argument can be applied. Let $\mathbf{\Pi}(z) = (\Pi_0(z), \Pi_1(z), ...)$ be the vector of z-transform of $\pi_{l,m}$ defined by

$$\mathbf{\Pi}(z) = \sum_{m=0}^{\infty} z^m \pi_m. \tag{4}$$

Then, by (1), we have the stationary equation;

$$\sigma\left(1-\frac{1}{z}\right)\pi_0 + \mathbf{\Pi}(z)\left\{\mathbf{D}(z) - \left(1-\frac{1}{z}\right)\sigma I\right\} = \mathbf{0}, \tag{5}$$

where $\mathbf{D}(z) = \sum_{m=0}^{\infty} z^m \mathbf{D}_m$. By using (2), we have the explicit form of $D(z)$ as

$$\mathbf{D}(z) = \begin{pmatrix} -\lambda & \lambda & & & \\ \mu & \lambda-\mu & \lambda & & \\ & 2z\mu & -\lambda-2\mu & \lambda & \\ & & \ddots & \ddots & \ddots \end{pmatrix}. \tag{6}$$

Further, let $\pi(z, y)$ be the double z-transform of $\pi_{l,m}$, i.e.,

$$\pi(z,y) = \sum_{l=0}^{\infty} y^l \Pi_l(z) = \sum_{l,m} z^m y^l \pi_{l,m} = E[z^M y^L]. \tag{7}$$

Before studying the equation to be satisfied with $\pi(z, y)$, we need to introduce the concept of the linear operator corresponding to the transition matrix and derive some basic caluculus.

Definition 1. *Let* f *be a function and* $f(y) = \sum_{j=0}^{\infty} f_j y^j$ *be its formal power series. We can define the linear operator* U *corresponding to a matrix* $\mathbf{U}$ *by*

$$[Uf](y) = \sum_{i,j} f_i [\mathbf{U}]_{ij} y^j.$$

Lemma 1. *The operator* $D(z)$ *corresponding to the transition matrix* $\mathbf{D}(z)$ *in (6) can also be written by*

$$[D(z)f](y) = \mu f_y(zy) + \lambda y f(y) - \lambda f(y) - \mu y f_y(y). \tag{8}$$

Especially, when $z = 1$*, we have*

$$[D(1)f](y) = \mu(1-y) f_y(y) - \lambda(1-y) f(y). \tag{9}$$

Proof. Using (6), we have

$$\begin{aligned}[D(z)f](y) &= \sum_{l=0}^{\infty} f_{l+1}(l+1)\mu (zy)^l \\ &\quad + \sum_{l=0}^{\infty} f_l(-\lambda - l\mu) y^l + \sum_{l=0}^{\infty} f_l \lambda y^{l+1} \\ &= \mu f_y(zy) + \lambda y f(y) - \lambda f(y) - \mu y f_y(y).\end{aligned}$$

□

Remark 3. *Intuitively, the first term of (8) represents the batch of jobs arriving at the customer leave, and the second term represents customer joins to the group. The rests represent the counter balance of the system.*

Then after some calculation, we have the following theorem.

Theorem 1. *The double* z*-transform of the stationary probability* $\pi(z, y)$ *satisfies the following equation:*

$$\sigma\left(1-\frac{1}{z}\right)\{\pi(0,y) - \pi(z,y)\} + [D(z)\pi(z)](y) = 0, \tag{10}$$

where

$$\begin{aligned}[D(z)\pi(z)](y) &= \mu\pi_y(z, zy) + \lambda y \pi(z,y) \\ &\quad -\lambda\pi(z,y) - \mu y \pi_y(z,y).\end{aligned} \tag{11}$$

Proof. Apply z-transform on (5) and use Lemma 1, then we have (10) and (11). □

Corollary 1. *The "marginal"* z*-transform of* L *is given by*

$$\pi(1,y) = E[y^L] = e^{\frac{\lambda}{\mu}(y-1)}. \tag{12}$$

Thus, the number of customers in the group $L(t)$ *is Poisson distribution with its mean* λ/μ*. In addition,* $\pi(1, y)$ *is the solution of the equation* $[D(1)f](y) = 0$*.*

By differentiating (10), it is easy to get the utilization of the server as we can see in the following corollary.

Corollary 2. *Let the utilization of server be* $\rho = P[M > 0]$*, then we have*

$$\rho = \frac{\lambda^2}{\sigma\mu} = \frac{1}{\sigma}\lambda E[L]. \tag{13}$$

3 MEAN QUEUE LENGTH OF JOBS

First, we define a linear operator A and its inverse A^{-1}, which are useful to calculate the mean queue length $E[M(t)]$.

Theorem 2. *Define a linear operator A by*

$$Af = [D(1)f](y) + f(1)\pi(1,y), \qquad (14)$$

for an arbitrary bounded smooth function f. Then, we have the inverse operator of A and

$$A^{-1}g = \pi(1,y)\left\{g(1) - \int_y^1 \frac{g(u)e^{-\frac{\lambda}{\mu}(u-1)} - g(1)}{\mu(1-u)}du\right\}, \qquad (15)$$

if the integral exits.

Remark 4. *Since the integrant of the (15) satisfies*

$$\lim_{u\to 1}\frac{g(u)e^{-\frac{\lambda}{\mu}(u-1)} - g(1)}{\mu(1-u)} = \frac{g'(1) - \frac{\lambda}{\mu}g(1)}{-\mu}, \qquad (16)$$

the operator A^{-1} is well defined when $g'(1)$ and $g(1)$ are bounded.

Proof. Set $f = A^{-1}g$. Assume f can be expressed in the form as

$$f(y) = c(y)\pi(1,y) = c(y)e^{\frac{\lambda}{\mu}(y-1)}, \qquad (17)$$

where $c(y)$ is an unknown function of y and to be determined. Using Lemma 1, we have

$$[Af](y) = \mu(1-y)f_y(y) - \lambda(1-y)f(y) + f(1)\pi(1,y).$$

Substituting (17), we obtain

$$g(y) = [Af](y) = e^{\frac{\lambda}{\mu}(y-1)}\left\{\mu(1-y)c'(y) + c(1)\right\}. \qquad (18)$$

Rearrange the above equation to have the differential equation of $c(y)$ as

$$c'(y) = \frac{1}{\mu(1-y)}\left\{e^{-\frac{\lambda}{\mu}(y-1)}g(y) - c(1)\right\}.$$

Integrating this equation over $[0,y]$, we obtain

$$c(y) = \int_0^y \frac{g(u)e^{-\frac{\lambda}{\mu}(u-1)} - g(1)}{\mu(1-u)}du + C,$$

where C is the integral constant. Note we used the fact $c(1) = g(1)$, which can be obtain by setting $y = 1$ in (18). Set $y = 1$, then we can find the integral constant should be

$$C = g(1) - \int_0^1 \frac{g(u)e^{-\frac{\lambda}{\mu}(u-1)} - g(1)}{\mu(1-u)}du.$$

Thus,

$$c(y) = g(1) - \int_y^1 \frac{g(u)e^{-\frac{\lambda}{\mu}(u-1)} - g(1)}{\mu(1-u)}du.$$

□

Lemma 2. *$\pi(1,y) = e^{\frac{\lambda}{\mu}(y-1)}$ is the fixed point of the operator A.*

Proof. From Corollary 1, $[D(1)\pi(1)](y) = 0$. Thus, it is easy to see that $[A\pi(1)](y) = \pi(1,y)$. □

Using the operator A and its inverse, we can find the mean queue length $E[M]$.

Theorem 3. *The mean queue length of encryption jobs $E[M]$ can be obatined by*

$$E[M] = \frac{\rho}{1-\rho} + \frac{1}{\sigma(1-\rho)}\Big\{\sigma\rho^2 + \frac{1}{2}[D''(1)\pi(1)](1) - \sigma[D'(1)A^{-1}\pi(0)](1) - [D'(1)A^{-1}D'(1)\pi(1)](1)\Big\}. \qquad (19)$$

Remark 5. *If we find $\pi(0,y)$ which is the z-transform of the boundary distribution π_{0l}, then we can obtain the mean queue length by Theorem 3. Generally, in matrix analysis, those boundary distributions can be obtained by estimating fundamental period matrix **G** where $\pi(o,y)$ is its invariant distribution. However, in the case of the infinite phase size case, the iteration process to find **G** can not be easy to perform. So, instead, using Theorem 3 we are going to get the bounds of the mean queue length in the following section.*

4 BOUNDS OF THE MEAN QUEUE LENGTH

Now we are going to evaluate each terms in $E[M]$ in Theorem 3 to obtain its bounds. Using some elementary calculations, we can obtain the following lemmas.

Lemma 3.

$$[D''(1)\pi(1)](1) = \lambda\left(\frac{\lambda}{\mu}\right)^2. \qquad (20)$$

Lemma 4.

$$[D'(1)A^{-1}\pi(0)](1) = \sigma\rho(1-\rho) + \frac{1}{2}\left\{3\left(\frac{\lambda}{\mu}\right)^2 - 2\left(\frac{\lambda}{\mu}\right)\pi_y(0,1) - \pi_{y^{(2)}}(0,1)\right\}. \qquad (21)$$

Lemma 5.

$$[D'(1)A^{-1}D'(1)\pi(1)](1) = \lambda(\lambda-1)\left(\frac{\lambda}{\mu}\right)^2. \qquad (22)$$

Theorem 4. *We have the upper and lower bounds of mean queue length of jobs $E[M]$ as*

$$E[M] \le \frac{\rho}{1-\rho} + \frac{3\rho(\lambda/\mu)(1-\lambda/\mu)}{2(1-\rho)}, \qquad (23)$$

and

$$E[M] \geq \left[\frac{\rho}{1-\rho} + \frac{3(\lambda/\mu)\{\rho-(1-\rho)(\lambda/\mu)\}}{2(1-\rho)}\right]^+, \tag{24}$$

where $x^+ = max(x, 0)$.

Proof. Applying Lemma 3, 4 and 5 in Theorem 3, we have the exact estimate of $E[M]$ as

$$\begin{aligned} E[M] &= \frac{\rho}{1-\rho} \\ &+ \frac{1}{2(1-\rho)}\Big\{3\Big(\frac{\lambda}{\mu}\Big)\rho - 3(1-\rho)\Big(\frac{\lambda}{\mu}\Big)^2 \\ &+ 2\Big(\frac{\lambda}{\mu}\Big)\pi_y(0,1) + \pi_{y^{(2)}}(0,1)\Big\} \end{aligned} \tag{25}$$

Since L and $L(L-1)$ are both non-negative, we have $0 \leq \pi_y(0,1) = E[L1_{(M=0)}] \leq E[L] = \lambda/\mu$, and $0 \leq \pi_{y^{(2)}}(0,1) = E[L(L-1)1_{(M=0)}] \leq E[L(L-1)] = (\lambda/\mu)^2$. Thus, we can obtain both the upper and lower bound as in (23) and (24). □

Remark 6. *We may obtain a reasonable approximation (and possibly better upper bound) of* $E[M]$ *by replacing the estimates in the proof of Theorem 4 with* $E[L1_{(M=0)}] \sim (1-\rho)E[L]$ *and* $E[L(L-1)1_{(M=0)}] \sim (1-\rho)E[L(L-1)]$. *However, in practical situation, as we can see in the following, the above bounds may be sufficient.*

If the service rate σ is large, most of the time the system is empty and $E[L1_{(M=0)}]$ can be well approximated by $E[L]$. Thus we may expect our bounds derived from the assumptions is tight for a large σ. We will check this conjecture.

Lemma 6. *We have the following estimates of the difference for the large service rate of jobs* σ*:*

$$E[L] - E[L1_{\{M=0\}}] \to 0, \tag{26}$$

$$E[L(L-1)] - E[L(L-1)1_{\{M=0\}}] \to 0 \text{ as } \sigma \to \infty. \tag{27}$$

5 NUMERICAL ANALYSIS OF THE BOUNDS

In this section, we briefly see the bounds of the mean waiting time for encryption including its service time (encryption time). As pointed out before, the waiting time for processing encryptions in the group security model corresponds the time duration when the security level degrades, since we need to use the older key to communicate inside the group.

Let W be the time required to finish all the encryptions when a customer leaves the group. By Little's Formula (Wolff, 1989; Kleinrock, 1975), we have $E[W] = E[M]/\lambda$. Thus, using Theorem 4, the bounds for $E[W]$ can be easily obtained. In the following, we fixed the service rate of the encryptions to be $\sigma = 10,000$. In Figure 1 - 3, the mean waiting time $E[W]$ is depicted as the function of λ for various μ. Note that $\rho = \lambda^2/\sigma\mu$ is the utilization of our $BMAP/M/1$ queue and $E[L] = \lambda/\mu$ is its population of the secure group. For the reference, not only the bounds, but we also show the waiting time of both the $M/M/1$ queue with the same utilization and the batch-arrival $M/M/1$ queue where their batch size is independent and identically to Poisson distribution with its mean λ/μ. Comparing these graphs, although we can see only bounds, $E[W]$ of the $BMAP/M/1$ queue is significantly larger than the ones of other queues. Thus, we need to take into account the correlation between the batches, or we underestimate the time length of security degradation. Also, we can see the bounds get tighter as the sojourn time of the customer $1/\mu$ gets shorter.

REFERENCES

Harney, H. and Muckenhirn, C. (1997a). Group key management protocol (gkmp) architecture. *RFC 2094*.

Harney, H. and Muckenhirn, C. (1997b). Group key management protocol (gkmp) sepcification. *RFC 2093*.

Kleinrock, L. (1975). *Queueing Systems Vol. 1*. John Wiley and Sons.

Latouche, G. and Ramaswami, V. (1999). *Introduction to Matrix Analytic Methods in Stochastic Modeling*. SIAM.

Makimoto, N. (2001). *Machigyouretsu Algorithm (Algorithm of Queueing System)*. Asakura.

Sengupta, B. (1989). Markov processes whose steady state distribution is matrix-exponential with an application to the gi1 queue. *Adv. Appl. Prob.*, (21):159–180.

Thomas, S. A. (2000). *SSL and TLS Essentials: Securing the Web*. John Wiley and Sons.

Toyoizumi, H. and Takaya, M. (2004). Performance evaluation of secure group communication. *Journal of the Operations Research Society of Japan*, 47(1):38–50.

Tweedie, R. (1982). Operator-geometric stationary distribution for markov chains, with applications to queueing models. *Adv. Appl. Prob.*, (14):368–391.

Wallner, D., Harder, E., and Agee, R. (1999). Key management for multicast: Issues and architectures. *Request for Comments: 2627*.

Wolff, R. (1989). *Stochastic modeling and the theory of queues*. Princeton-Hall.

Wong, C., Gouda, M., and Lam, S. (2000). Secure group communications using key graphs. *IEEE/ACM Trans. on Networking*, 8(1):16–30.

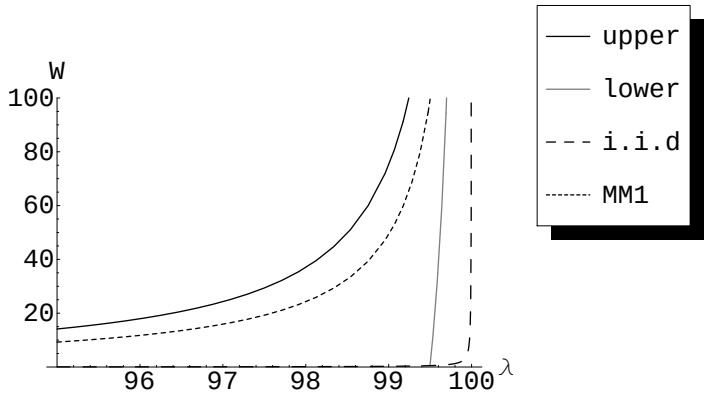

Figure 1: Upper bound and lower bound of $E[W]$ when $\mu = 1$. The lines "upper " and "lower" are the upper and lower bounds of mean waiting time respectively. The line "i.i.d" corresponds to the batch arrival $M/M/1$ queue where the batch size is independent and identically to Poisson distribution with its mean λ/μ.

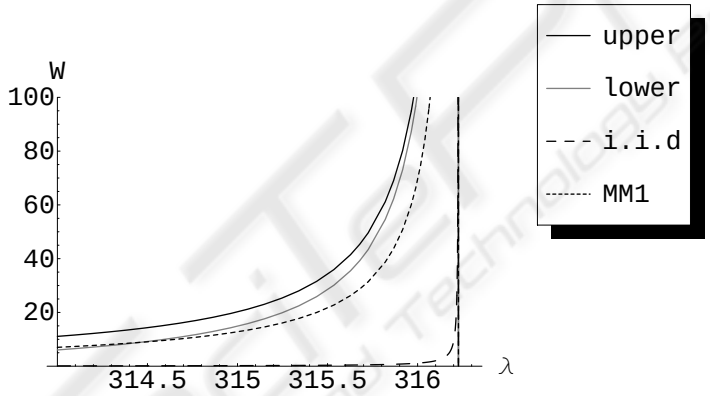

Figure 2: Upper bound and lower bound of $E[W]$ when $\mu = 10$.

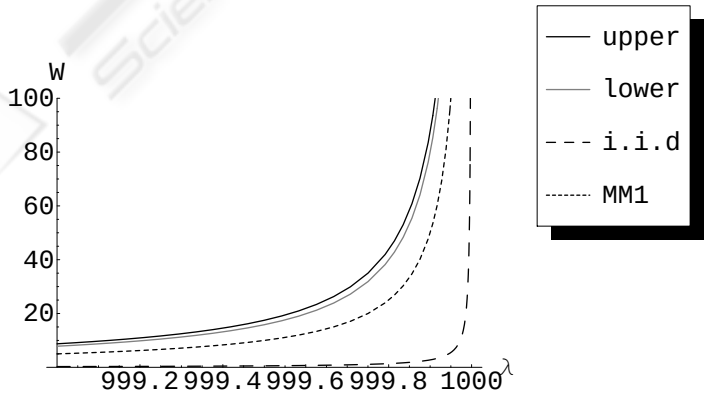

Figure 3: Upper bound and lower bound of $E[W]$ when $\mu = 100$.