

Approximate solution of a PEPA model of a key distribution centre

Yishi Zhao and Nigel Thomas

School of Computing Science, Newcastle University



- Motivation
- Key Exchange Protocol
- PEPA
- Model and Simplification
- Numerical Results
- Extensions
- Conclusion and Future Work

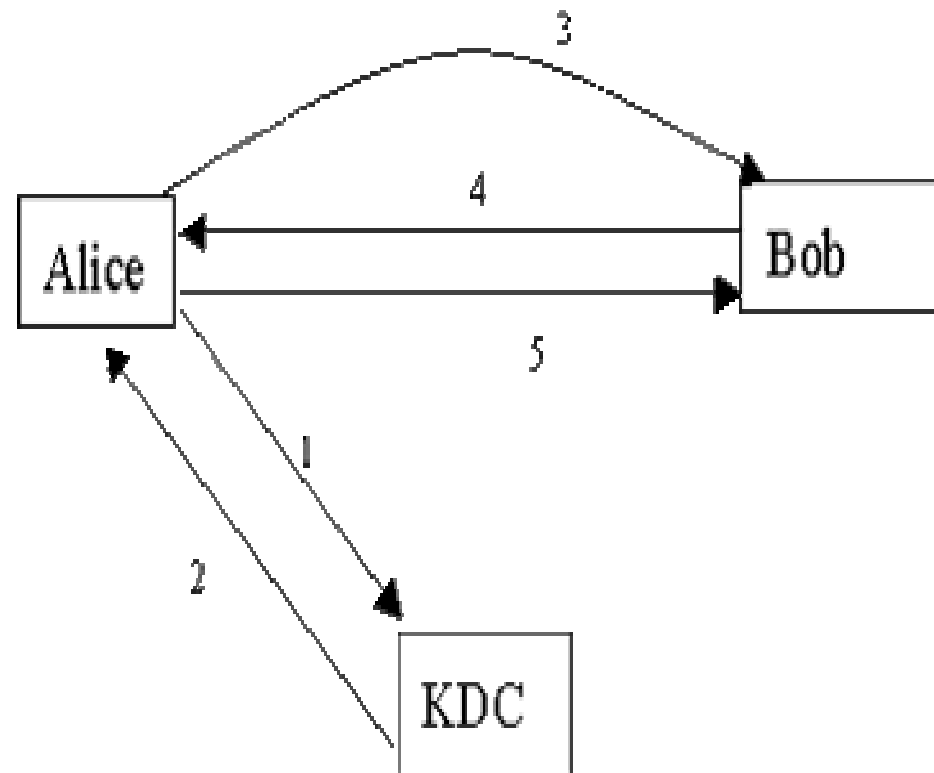


Motivation

- Making a system secure may add an overhead that degrades temporal performance.
- Making such security mechanisms temporally efficient, as well as secure, is practically important.
- Choosing a cryptography protocol is inspired by investigation of timing attack of wide mouth frog modelled by PEPA. (Buchholz, et al)
- Original PEPA model suffered from commonly encountered state space explosion problem (over 60K states for 6 clients in steady state)

Key Distribution Centre: Needham Schroeder Symmetric Key

- This key distribution protocol was originally invented by Roger Needham and Michael Schroeder in 1978.
 - Alice and KDC share a key K_A
Bob and KDC share a key K_B
1. Alice sends request to KDC with nonce N_1
 2. $E\{K_A\}[KS \mid request \mid N_1 \mid E\{K_B\}[KS \mid IDA]]$
 - KS is a session key for Alice and Bob to use.
 - Alice can't decrypt the part encode with Bob's key, she can only send it on:
 3. $E\{K_B\}[KS \mid IDA]$
 4. $E\{KS\}[N_2]$
 5. $E\{KS\}[f(N_2)]$





- PEPA is a Markovian process algebra.
- Systems are specified in PEPA in terms of activities and components.
- Each component may be atomic or composed of other components.
- Each activity $a = (\alpha, r)$ has a type α and a rate r .
- Each activity is negative exponentially distributed with rate r or passive with distinguished rate T .
- A model in PEPA specifies a continuous time Markov chain.



PEPA syntax

$P ::= (\alpha, r).P \mid P+Q \mid P/L \mid P\langle L \rangle Q \mid A$

- **Prefix: $(\alpha, r).P$** the component carries out activity (α, r) and subsequently behaves as component P .
- **Choice: $P+Q$** the component represents a system which may behave wither as P or as Q . (determined by race policy)
- **Co-operation: $P\langle L \rangle Q$** P and Q synchronise behaviour over shared activities in L
- **Hiding: P/L** the component behave as P except that any activities of types with in the set L are hidden
- **Constant: $P = A$** associate the constant P with the behaviour of the component A



Original Model

$$\text{KDC} = (\text{request}_1, T). \text{KDC}_1 + (\text{request}_2, T). \text{KDC}_2 \\ + \dots + (\text{request}_N, T). \text{KDC}_N$$

$$\text{KDC}_1 = (\text{response}_1, r_p). \text{KDC} + (\text{request}_2, T). \text{KDC}_{N+1} \\ + \dots + (\text{request}_N, T). \text{KDC}_{2N-1}$$

...

$$\text{KDC}_{2N} = (\text{response}_1, r_p/N). \text{KDC}_{2N-N} \\ + (\text{response}_2, r_p/N). \text{KDC}_{2N-N+1} + \dots + (\text{response}_N, r_p/N). \text{KDC}_{2N-1}$$

$$\text{Alice}_i = (\text{request}_i, r_q). (\text{response}_i, T). (\text{sendB}_i, r_B). (\text{sendA}_i, T). \\ (\text{confirm}_i, r_c). (\text{usekey}_i, r_u). \text{Alice}_i, \quad 1 \leq i \leq N$$

$$\text{Bob}_i = (\text{sendB}_i, T). (\text{sendA}_i, r_A). (\text{confirm}_i, T). \\ (\text{usekey}_i, T). \text{Bob}_i, \quad 1 \leq i \leq N$$

$$\text{System} = \text{KDC} \langle k \rangle ((\text{Alice}_1 \langle L_1 \rangle \text{Bob}_1) || \dots || (\text{Alice}_N \langle L_N \rangle \text{Bob}_N))$$

Where $k = \{\text{request}_1, \text{response}_1, \dots, \text{request}_N, \text{response}_N\}$ and $L_i = \{\text{sendB}_i, \text{sendA}_i, \text{confirm}_i, \text{usekey}_i\}$

Model Simplification(1)

$KDC = (\text{request}, T).KDC + (\text{response}, r_p).KDC$

$Alice = (\text{request}, r_q).Alice1$

$Alice1 = (\text{response}, T).Alice2$

$Alice2 = (\text{sendBob}, r_B).Alice3$

$Alice3 = (\text{sendAlice}, T).Alice4$

$Alice4 = (\text{confirm}, r_c).Alice5$

$Alice5 = (\text{usekey}, r_u).Alice$

$Bob = (\text{sendBob}, T).Bob1$

$Bob1 = (\text{sendAlice}, r_A).Bob2$

$Bob2 = (\text{confirm}, T).Bob3$

$Bob3 = (\text{usekey}, T).Bob$

$System = KDC \langle L \rangle (Alice \langle k \rangle Bob \parallel \dots \parallel Alice \langle k \rangle Bob)$

Where $k = \{\text{request}, \text{response}\}$ and $L = \{\text{sendBob}, \text{sendAlice}, \text{confirm}, \text{usekey}\}$

Model Simplification(2)

$KDC = (\text{response}, r_p).KDC$

$Alice = (\text{request}, r_q).Alice1$

$Alice1 = (\text{response}, T).Alice2$

$Alice2 = (\text{sendBob}, r_B).Alice3$

$Alice3 = (\text{sendAlice}, r_A).Alice4$

$Alice4 = (\text{confirm}, r_C).Alice5$

$Alice5 = (\text{usekey}, r_u).Alice$

$\text{System} = KDC \langle \text{response} \rangle (Alice || \dots || Alice)$

Model Simplification(3)

$KDC = (\text{response}, r_p).KDC$

$Alice = (\text{response}, T).(\tau, r_x).Alice$

$\text{System} = KDC \langle \text{response} \rangle (Alice || \dots || Alice)$

Where $r_x = (1/r_q + 1/r_B + 1/r_A + 1/r_c + 1/r_u)^{-1}$

M/M/1./N Closed Queueing Network

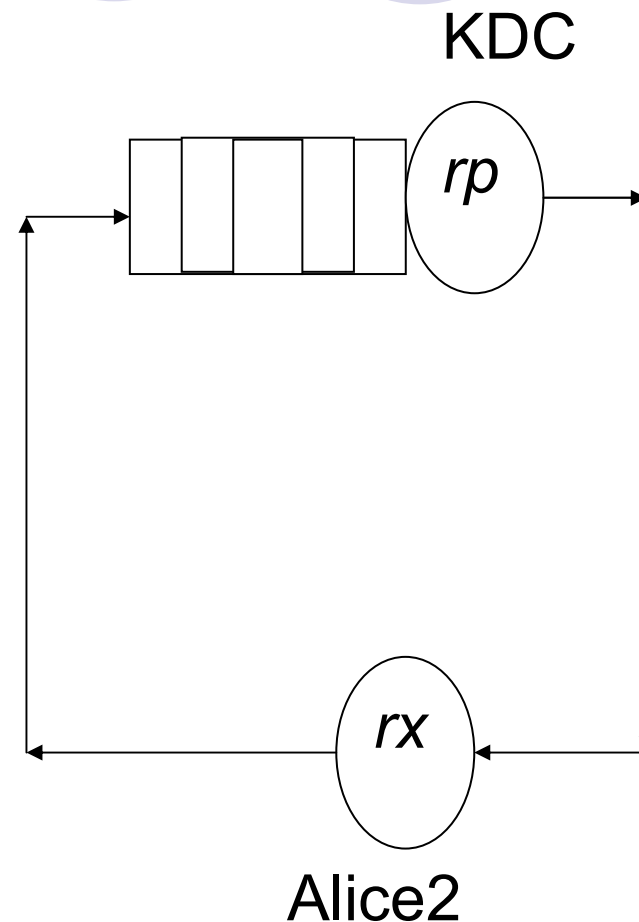
$$\Pi_0 = \left[N! \sum_{i=0}^N \frac{\rho^i}{(N-i)!} \right]^{-1}$$

$$\rho = \frac{rx}{rp}$$

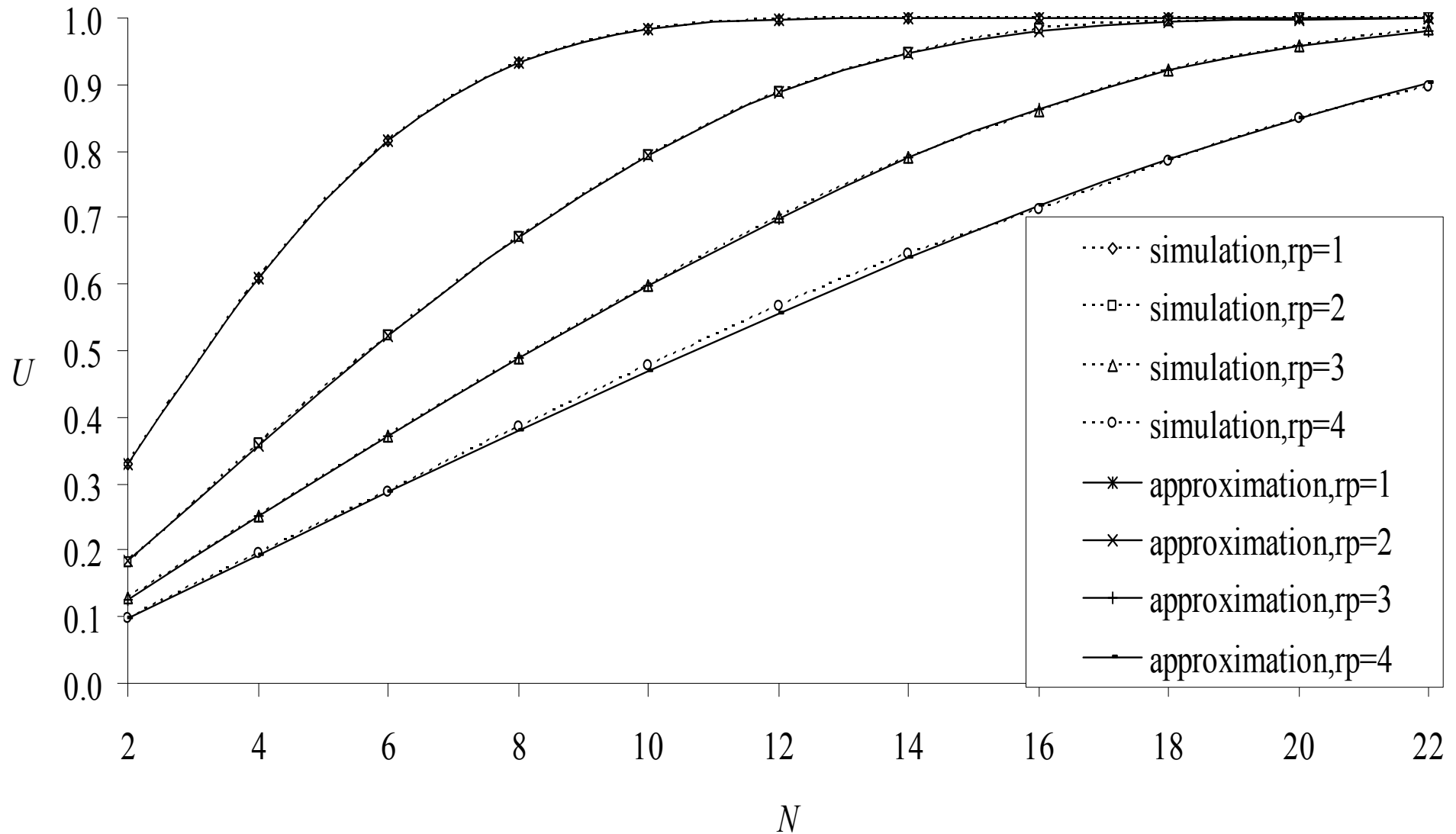
$$L = N! \Pi_0 \sum_{i=0}^N \frac{i \rho^i}{(N-i)!}$$

$$T = (N - L)rx$$

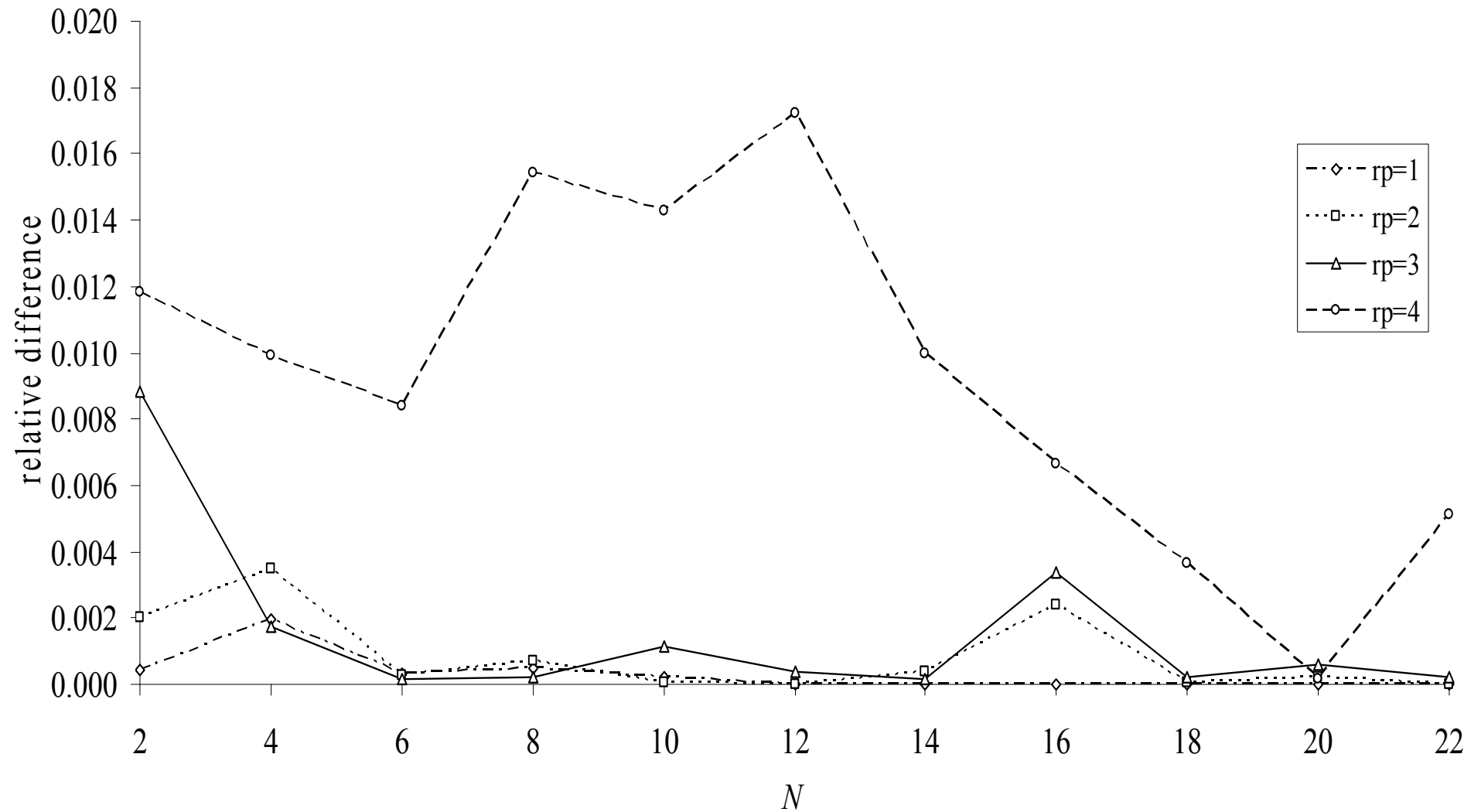
$$W = \frac{N}{T} - \frac{1}{rx}$$



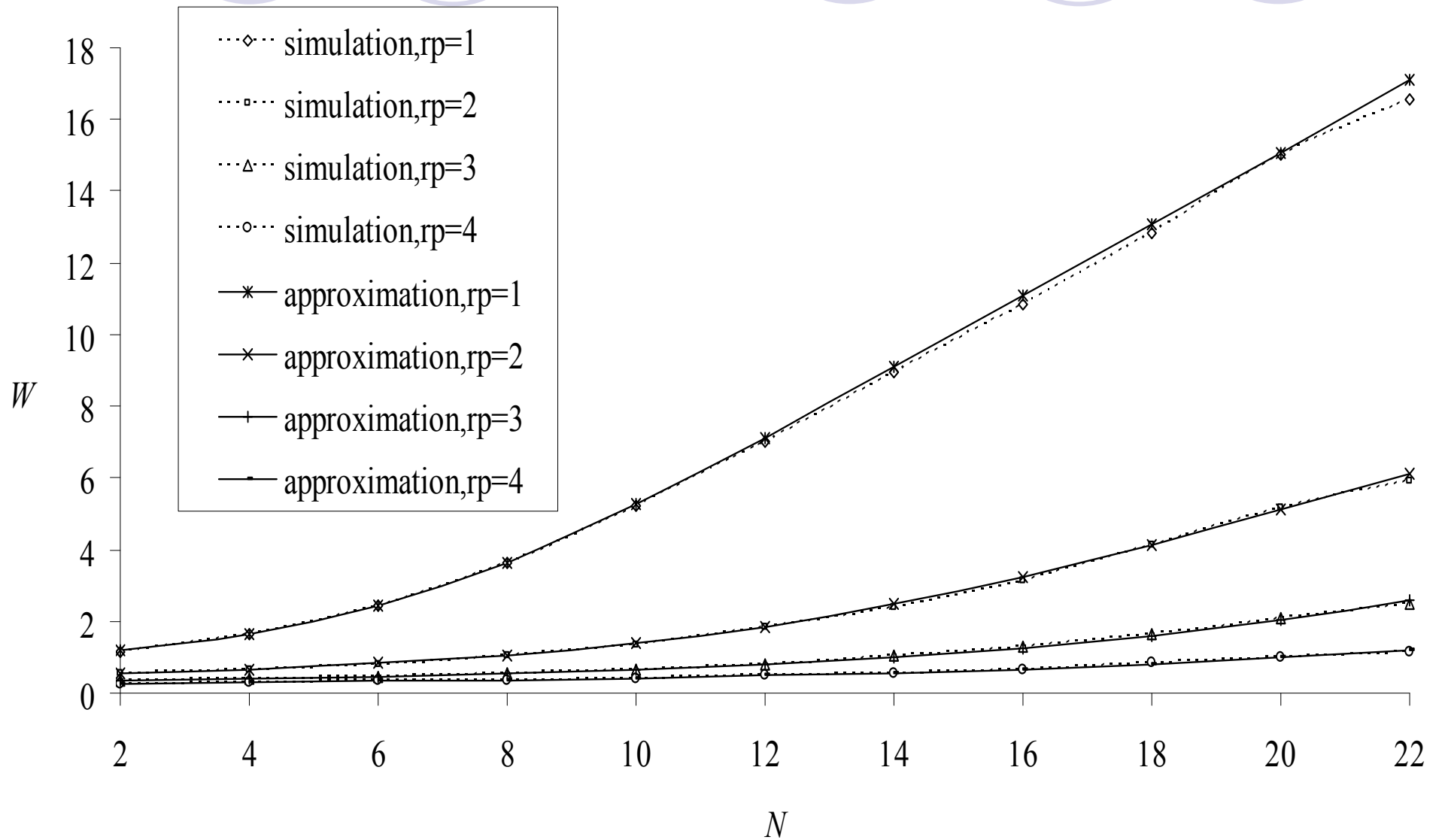
Numerical results: $r_q=r_A=r_B=r_C=1$, $r_U=1.1$



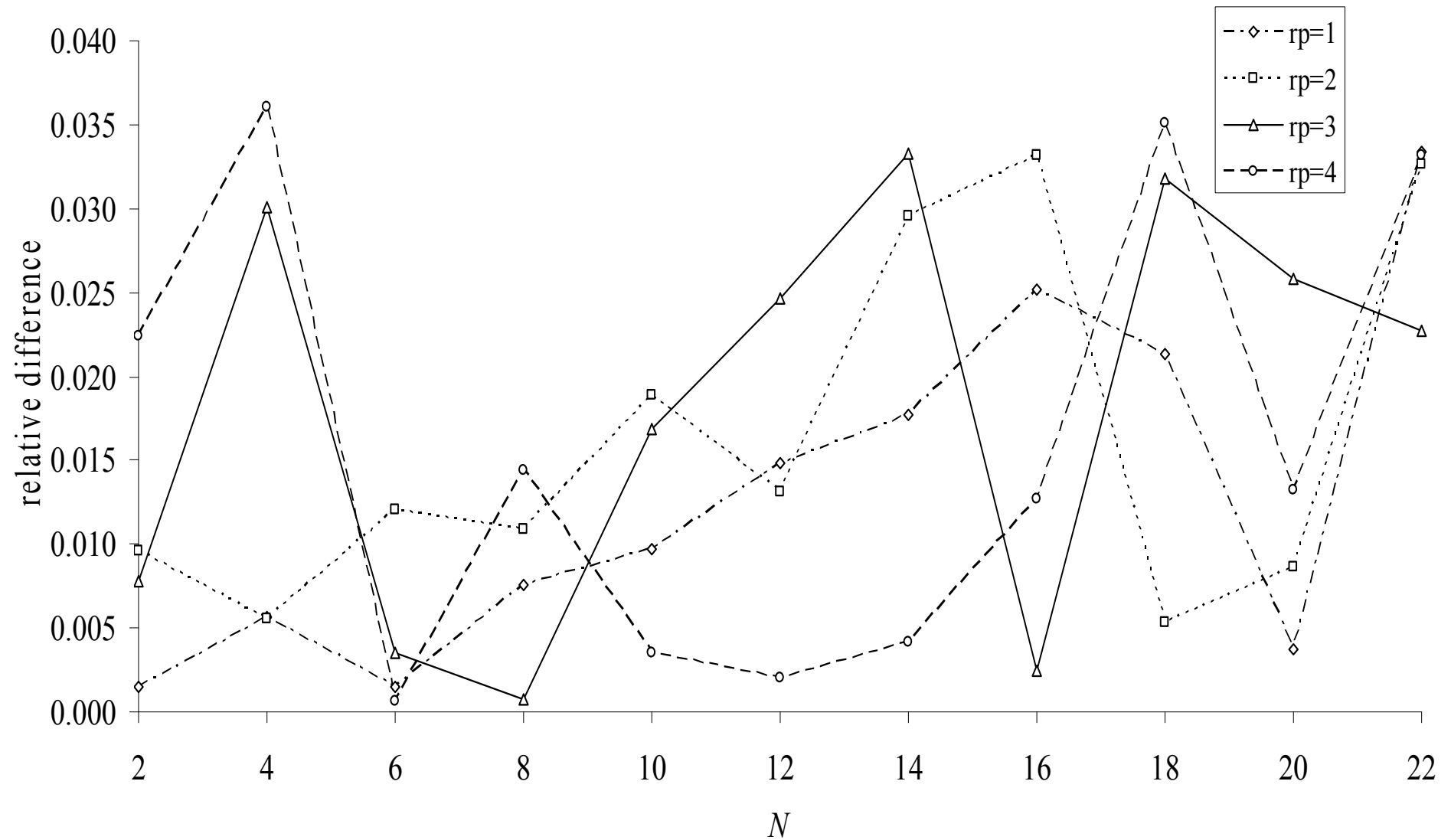
Numerical results: $r_q=r_A=r_B=r_C=1$, $r_u=1.1$



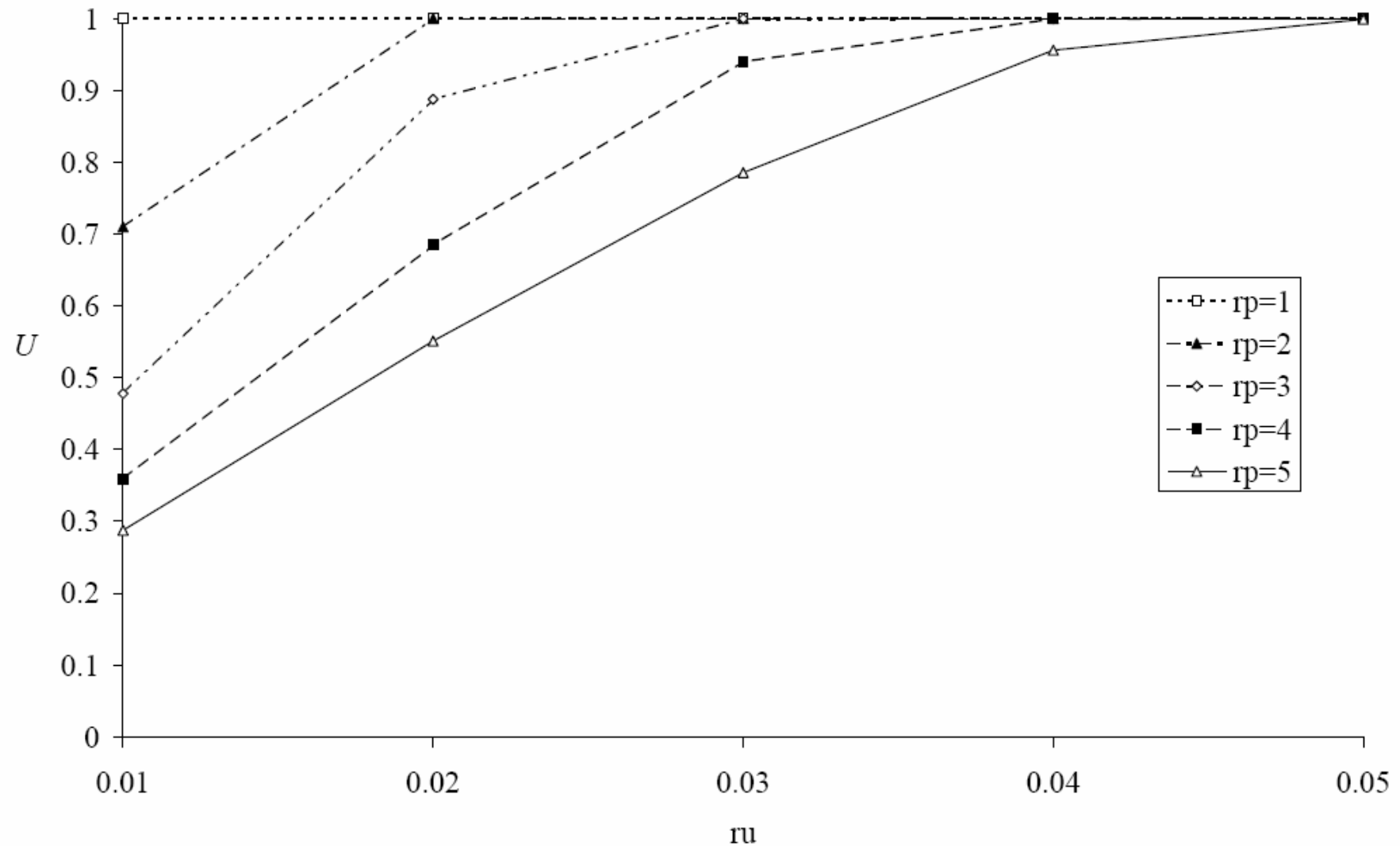
Numerical results: $r_q=r_A=r_B=r_C=1$, $r_U=1.1$



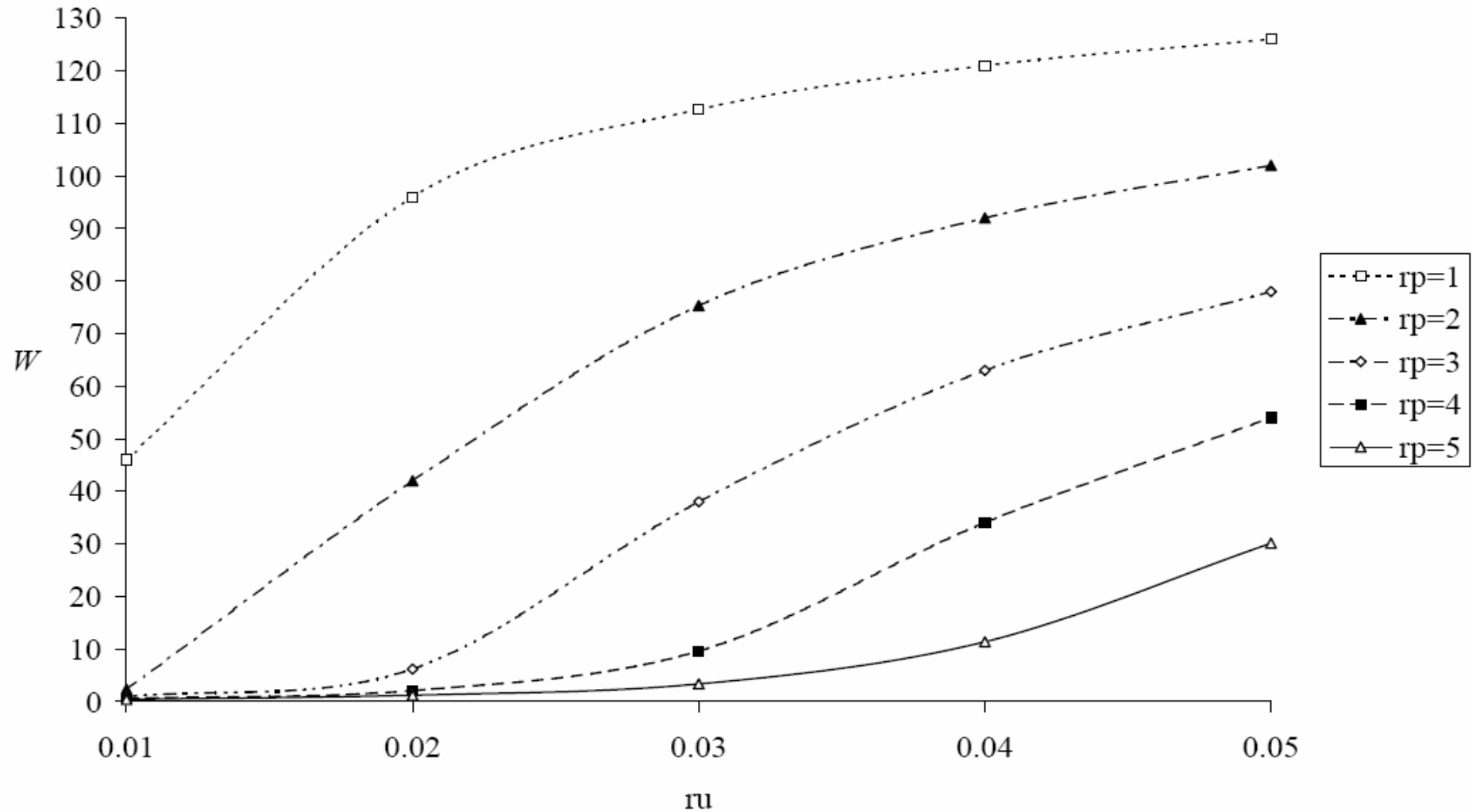
Numerical results: $r_q=r_A=r_B=r_C=1$, $r_u=1.1$



Numerical results: $r_q=r_A=r_B=r_C=1$, $N=150$



Numerical results: $r_q=r_A=r_B=r_C=1$, $N=150$





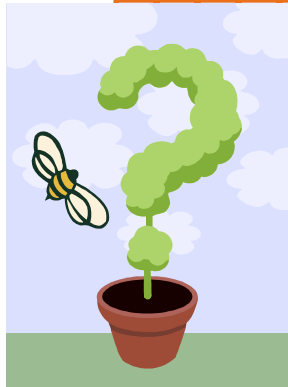
Extensions

- Multiple KDC servers
- Asymptotic bounds to QN model
- Stochastic simulation and ODE solution to PEPA model (UKPEW 2008)
- Cost model of waiting and resource provision (to be submitted to TrustCom 2008)

Conclusion and Future Work

- We've shown that our model of the KDC can be approximated as an M/M/1/.N queue.
- Approximated model showed coincidence in terms of utilisation of KDC and average response time results with discrete event simulation.
- Increased duration of session key being used to capture the practical scenario.
- Apply these techniques to a class of non-repudiation protocols.

Any questions?



?

Three stylized figures with large question marks inside their heads, arranged horizontally.

It's QUESTION TIME!!

