Avaliação de um Sistema de Reputação e Incentivo*

Nuno Cruz[1,2] and Hugo Miranda[2]

[1] Instituto Politécnico de Lisboa
Instituto Superior de Engenharia de Lisboa
ADEETC
[2] Universidade de Lisboa - Faculdade de Ciências
LaSIGE - Large-Scale Informatics Systems Laboratory

Resumo Num ambiente de computação móvel em nuvem colaborativa, os dispositivos móveis utilizam os recursos livres dos pares para melhorar o desempenho das suas aplicações. Para prevenir comportamentos desviantes (egoísmo, falsificação de resultados, etc.), estes ambientes devem ser munidos de ferramentas que penalizem os utilizadores. Contudo, a ausência de uma entidade confiável e centralizada que aplique de imediato as penalizações põe em risco todo o ambiente, uma vez que pode levar os utilizadores bem comportados a assumirem também eles comportamentos desviantes ou a abandonar o sistema. Adicionalmente, o sistema é vulnerável a interpretações incorretas de comportamentos, que resultam quer das incertezas que caracterizam o meio de execução, quer de atuações maliciosas de alguns utilizadores.
Para avaliar o impacto que estas condicionantes poderão ter no correto funcionamento de um ambiente de computação móvel em nuvem colaborativa foi desenvolvido um simulador que permite variar não só os tipos de comportamento dos utilizadores mas também as características do ambiente de execução, assumindo a existência de um protocolo viável de incentivo e confiança. Este artigo apresenta os resultados das simulações, analisando as limitações que o ambiente coloca a um sistema com estas características.

1 Introdução

Recentemente assistimos a uma expansão do poder computacional e da capacidade de memória nos dispositivos móveis (*smart-phones, tablets*, portáteis, etc.). O padrão de utilização destes dispositivos sugere que o seu CPU está inativo grande parte do tempo. Um padrão semelhante, identificado em computadores de secretária, contribuiu para o surgimento de alguns projetos que utilizam este tempo de inatividade para acelerar tarefas de computação complexas (vide por exemplo o Boinc [2]). Apesar de a participação ser voluntária, estes projetos têm

* O trabalho descrito neste artigo foi parcialmente suportado pela Fundação para a Ciência e Tecnologia (FCT) através do projeto PTDC/EIAEIA/103751/2008 - PATI

sido capazes de agregar um número significativo de utilizadores. Nestes projetos, a cooperação é facilitada pela omnipresença da Internet, que simplifica a transferência de código e resultados entre os computadores e os servidores.

As vendas substanciais de dispositivos móveis sugerem que, em locais onde ocorrem concentrações significativas de indivíduos (centros comerciais, aeroportos, eventos desportivos), é possível encontrar uma quantidade não negligenciável de ciclos de CPU desperdiçados, resultantes do padrão intermitente de utilização dos dispositivos. À semelhança do Boinc, estes ciclos poderiam ser utilizados pelos dispositivos que em cada instante se encontram ativos para paralelizar a realização de tarefas requeridas por aplicações complexas. A delegação das tarefas pode ser completamente distribuída, utilizando uma interface de rede de curto alcance (ex.: WiFi) e dispensando a participação de um mediador, o que contribuiria para o alívio do consumo de largura de banda nas redes dos operadores móveis. Neste artigo utilizamos o termo computação em nuvem colaborativa (CNC) para nos referir a este modelo de computação distribuído e colaborativo. Uma descrição da arquitetura de uma CNC, bem como os seus casos de uso podem ser encontrados em [4].

Numa CNC os utilizadores consideram os seus ciclos de CPU um recurso valioso, cuja utilização tem um impacto negativo na autonomia do dispositivo. Um mercado de ciclos de CPU permite que os utilizadores cedam os seus ciclos quando não estão interessados na utilização dos seus dispositivos, recolhendo-os quando se encontram numa situação em que poderiam tirar benefício de poder computacional adicional. Para ser útil, o mercado deve ter uma memória de longo prazo, que permita aos utilizadores serem recompensados pelos ciclos disponibilizados dias ou semanas mais tarde. Para atrair o maior número possível de participantes, é importante demonstrar que o mercado é funcional, justo e benéfico. Isto obriga à concretização de mecanismos que permitam adiar a recompensa dos utilizadores, penalizem comportamentos incorretos e assegurem o anonimato dos participantes. No entanto, a natureza descentralizada da CNC levanta questões quanto à eficácia destes mecanismos. Estas questões podem ser observadas noutros contextos, como é o caso dos serviços de leilões (por exemplo o EBay [15]) mas que aqui são agravados pela indisponibilidade de um servidor de reputação confiável no momento em que as transações são realizadas e pela utilização de uma moeda virtual.

Para compreender o impacto que o mau comportamento dos utilizadores pode ter num sistema em que a sua penalização é diferida, foi concretizado um simulador que permite modelar as transações e o ambiente computacional e de rede esperados numa CNC. O simulador permite emular comportamentos de utilizadores distintos (maliciosos e corretos), bem como comportamentos transitórios em que os utilizadores tentam camuflar o seu comportamento desonesto. Este artigo apresenta os resultados das simulações, onde se pode verificar os tipos de comportamentos a que o sistema é mais vulnerável e a evolução da capacidade deste em detetar e penalizar os comportamentos maliciosos.

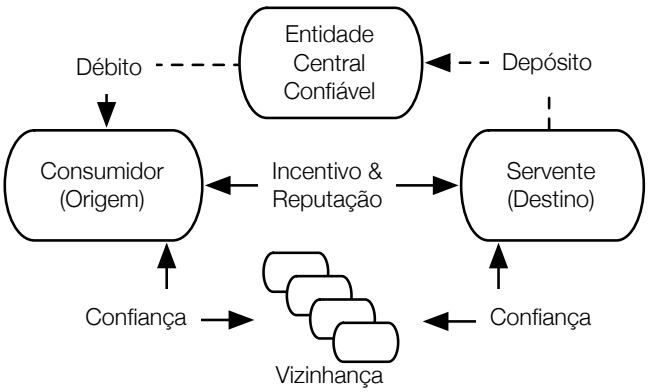


Figura 1. Relações entre as diferentes entidades durante uma transação na CNC

2 Caracterização do Sistema Híbrido de Incentivo

Numa CNC, assume-se que a prestação de serviços é recompensada utilizando uma moeda virtual, denominada TwinCoin. As quatro classes de participantes numa transação são apresentadas na Fig. 1. A entidade central confiável (*ECC*) emite e valida TwinCoins, mantém uma conta para cada utilizador e gere a sua reputação. O *consumidor* é o utilizador que inicia uma transação expressando o seu interesse em utilizar os serviços disponibilizados por outro dispositivo. O *servente* é o utilizador que aceita executar uma determinada tarefa recebendo em troca uma quantia. *Vizinhos* são dispositivos em proximidade física do consumidor e servente. A presença ou participação de vizinhos numa transação não é obrigatória.

As interações com a ECC são assíncronas relativamente às transações e podem ocorrer de acordo com a conveniência do utilizador (por exemplo, quando a bateria do dispositivo está em carga e existe ligação à Internet de baixo custo). Durante estes contactos são realizadas duas operações. As operações de depósito consistem no crédito de TwinCoins obtidos pela prestação de serviços a outros utilizadores. As operações de débito consistem no levantamento de TwinCoins, por forma a recompensar os serventes de operações que venha a realizar no futuro. Devido às características do algoritmo utilizado para a moeda virtual, não é possível utilizar TwinCoins obtidas como servente sem antes as creditar na ECC. A ECC serve ainda de guardião da reputação, disseminando informações sobre a reputação de alguns utilizadores em cada interação.

As transações decorrem em três passos. No passo de *seleção*, o consumidor anuncia aos vizinhos o interesse em delegar uma determinada tarefa e seleciona o servente, em função dos custos propostos e da sua reputação. No passo de *delegação*, o consumidor entrega os dados da operação a realizar e sinaliza o pagamento. Finalmente, no passo de *retorno*, o servente entrega os resultados ao consumidor e conclui o pagamento. O pagamento é sinalizado entregando

uma parte das TwinCoins que é univocamente associável ao consumidor mas que, por si só, não permite ao servente reclamar o valor à ECC. O servente terá que apresentar igualmente a segunda parte, entregue pelo consumidor no passo *retorno*.

A identidade real e imutável dos utilizadores é apenas conhecida da ECC. Em todas as interações com outros dispositivos, os utilizadores apresentam-se com um pseudónimo, criado em conjunto por cada utilizador e pela ECC. Para aumentar a privacidade, espera-se que os utilizadores mudem frequentemente de pseudónimo. Os certificados de reputação são emitidos para os pseudónimos, sendo responsabilidade da ECC a transferência da reputação entre pseudónimos.

2.1 Informação de Confiança e Reputação

O sistema monetário da CNC não é suficiente para prevenir fraudes. O objetivo da informação de reputação é transmitir informações tão precisas quanto possível sobre o comportamento típico de cada utilizador, para que possam decidir, de forma informada, sobre aqueles com que aceitam participar em transações. São utilizados dois tipos de reputação. A *reputação global* é gerida pela entidade central confiável (ECC). A *reputação local* é construida diretamente pelos dispositivos, de acordo com a sua experiência em transações anteriores.

A reputação de cada utilizador é atualizada pela ECC para cada registo de transação recebido. A reputação de um utilizador u é um valor, $GR_u \in [-1.00, +1.00]$ inicializado a 0 aquando da sua entrada no sistema, atualizada por uma fórmula de alisamento exponencial simples descrita na Eq. 1 onde, o coeficiente α, pondera a reputação anterior e o custo da transação reportado é dado por C_t.

$$GR_u = \alpha \times GR_u + (1 - \alpha) \times S_t \times (1 - \frac{1}{C_t + 1}) \tag{1}$$

S_t é um fator de sucesso que será respetivamente $+1$ ou -1 se a transação tiver sido concluída com sucesso ou não pelo que transações com sucesso aumentarão a reputação do utilizador e transações sem sucesso diminuirão o valor. Como forma de fomentar a cooperação, o sistema é assimétrico na medida em que apenas beneficia serventes nas transações realizadas com sucesso, mas penaliza ambos os participantes nas transações falhadas.

Os *certificados de reputação* são estruturas de dados assinadas digitalmente pela ECC. Cada certificado contém a identidade de um utilizador (u), a sua reputação (GR_u) e a data de emissão. Em cada interação com os dispositivos, a ECC entrega um novo certificado do utilizador que a contactou e uma lista aleatória de certificados de reputação dos utilizadores. Esta lista é influenciada de forma a incluir com uma maior probabilidade os utilizadores com uma reputação mais baixa. Este mecanismo de disseminação probabilista cria uma base de dados distribuída de reputação para fazer face a utilizadores maliciosos que escondam os seus certificados recentes por não lhe serem favoráveis. Os dispositivos que necessitem desta informação podem obtê-la contactando os seus vizinhos.

A informação de reputação local é exclusiva a cada dispositivo e é construida pelas interações com os seus vizinhos. Contudo, esta informação é partilhada na vizinhança da mesma forma que a disseminação dos certificados de reputação.

3 Simulação

Para avaliar a resistência da CNC a comportamentos incorretos dos utilizadores, foi concretizado um simulador que emula diferentes comportamentos dos utilizadores e as diferentes operações que estes podem realizar. O meio de transmissão modelado simula um típico ambiente de rede sem fios, com difusão a 1-salto. A ordem pela qual os nós recebem as mensagens de difusão é aleatória, permitindo uma distribuição uniforme das mensagens. Os dispositivos móveis podem assumir o papel de nós com comportamentos adequados, ou assumir perfis desonestos. Um nó com comportamento adequado é definido como partilhando os seus recursos e enviando tarefas para os restantes. Um nó desonesto é modelado de acordo com os diferentes ataques possíveis, abordados na Sec. 3.2. O perfil de um nó desonesto é dado por uma probabilidade de assumir um determinado comportamento. Para simular os períodos de operação desligada da Internet dos dispositivos, a ECC é modelada para a cada ciclo ter uma determinada probabilidade de estar *online* ou *offline* para um determinado grupo de nós. Nos contactos com a ECC, cada nó atualiza o seu certificado de reputação e recebe certificados de 10 outros dispositivos.

A simulação progride em ciclos. A cada ciclo um nó pode executar uma das cinco ações disponíveis, selecionada com uma probabilidade uniforme: *i*) débito; *ii*) depósito; *iii*) solicitar tarefa; *iv*) alterar pseudónimo; *v*) permanecer inativo. Todos os nós estão permanentemente disponíveis para realizar tarefas. De salientar que as operações *i*), *ii*) e *iv*), que implicam contactos com a ECC são ainda condicionadas pela disponibilidade da ECC e permanecerão inativos caso a ECC se encontre indisponível.

No inicio da simulação todos os nós têm conectividade com a ECC, o que permite aos nós executar uma operação de débito por forma a ficarem com TwinCoins.

Ao executar a ação de depositar notas, o dispositivo irá depositar na ECC todas as notas que recebeu. Ao mesmo tempo irá apresentar as queixas sobre eventuais transações falhadas.

Os parâmetros base de configuração do simulador estão resumidos na Tabela 1. Esta configuração representa um grupo de nós relativamente reduzido de forma a simular um grupo de participantes na CNC em proximidade. No decorrer da simulação são recolhidos, como parâmetros para a avaliação, a reputação dos dispositivo, o seu saldo na ECC, as TwinCoins que tem atualmente em carteira, bem como o número de tarefas enviadas e recebidas,

3.1 Simulação base de referência

A simulação de referência assume a inexistência de dispositivos maliciosos, mudanças de pseudónimo ou indisponibilidade da ECC. A Fig. 2(a) apresenta a

Rede	Nº de dispositivos corretos	10
	Nº de dispositivos maliciosos	2
	Custo das tarefas	10
ECC	Valor inicial de TwinCoins na conta de cada dispositivo	500
	Número de nós enviados aos nós como reputação global	10
	Probabilidade da ECC estar Online a cada iteração do nó	0,5
Dispositivos	α de GR_u	0,7
	Total de notas pedidas em operações de débito	100
	Valor de TwinCoins atribuído inicialmente a cada dispositivo	100
	Limiar da reputação pré-conhecida aceitável para o nó	-0,25
	Limiar de reputação a partir do qual aceita a reputação vinda dos vizinhos sobre um dispositivo	0,5
	Limiar de reputação para aceitar reputação enviada diretamente pelo outro dispositivo	-0,5
	Validade dos certificados de reputação	10 iterações
Simulação	Iterações	1000
	Período de recolha de estatísticas	10

Tabela 1. Parâmetros da Simulação

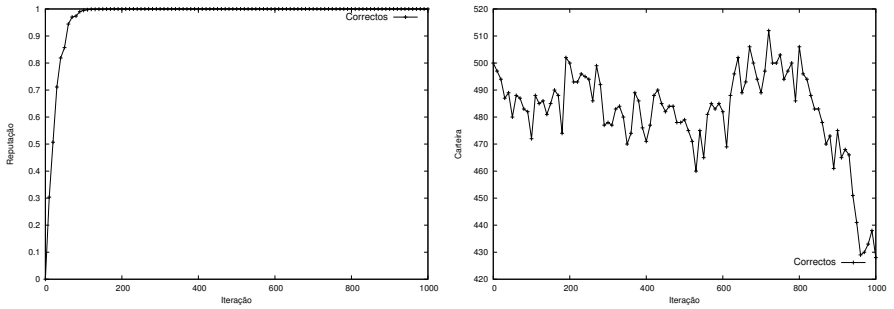
evolução da reputação média dos nós, verificando-se a tendência dos nós atingirem o limiar máximo da reputação com um número reduzido de operações. As oscilações da média de dinheiro virtual na carteira local de cada dispositivo (Fig. 2(b)) são atribuídas às diferentes iterações entre os dispositivos e com a ECC.

3.2 Modelação de ataques

A modelação de dispositivos maliciosos passa pela criação de diferentes perfis, que retratam um conjunto de ataques possíveis a um sistema desta natureza. As simulações assumem que todos os ataques são detetados, permitindo assim focar no objetivo deste trabalho que é perceber os efeitos dos ataques nas propriedades da CNC para os dispositivos corretos.

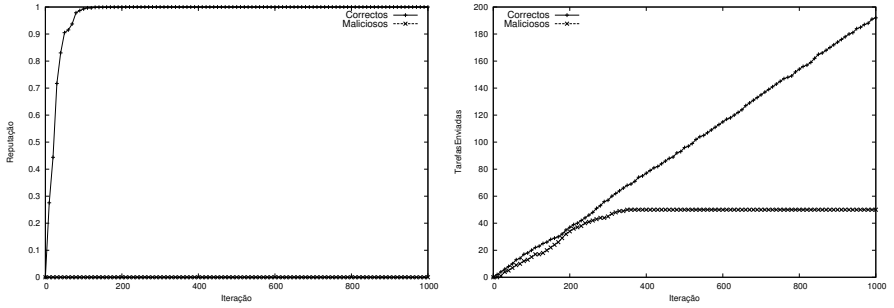
Modelo de Ameaça 1: Dispositivo Egoísta. Neste modelo o dispositivo comporta-se de forma egoísta, não aceitando tarefas de outros dispositivos. Este modelo permite validar o capacidade de incentivar os dispositivos a partilhar os seus recursos. A Fig. 3 apresenta a evolução dos diferentes parâmetros nas simulações com dispositivos egoístas. A Fig. 3(a) mostra que os nós egoístas não recolhem reputação positiva, devido à característica do algoritmo de só premiar a reputação dos nós serventes. Ao fim de algumas iterações, o dinheiro virtual atribuído inicialmente ao dispositivo esgota-se e os dispositivos egoístas deixam de poder enviar tarefas, como se comprova na Fig. 3(b).

Modelo de Ameaça 2: Ataque ao protocolo de dinheiro virtual. Neste modelo os dispositivos maliciosos começam por executar um pedido de tarefa corretamente. No entanto, após receber os resultados do dispositivo servente, estes dispositivos não entregam a segunda parte do dinheiro virtual. Este



(a) Reputação média dos nós (b) Média do dinheiro virtual nos dispositivos

Figura 2. Simulação base, sem dispositivos maliciosos, ECC *online*

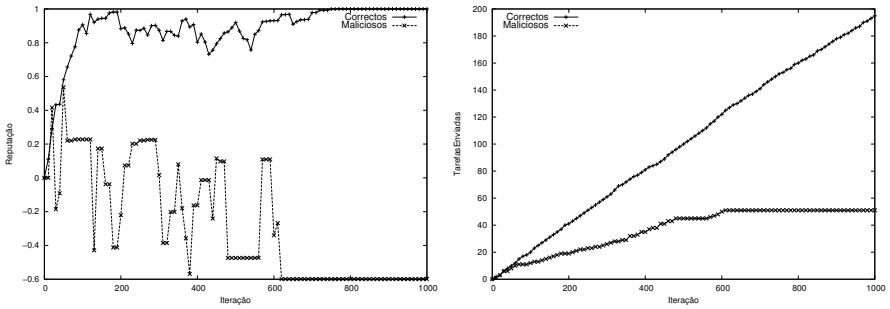


(a) Reputação (b) Tarefas enviadas

Figura 3. Simulação para o modelo de ameaça 1

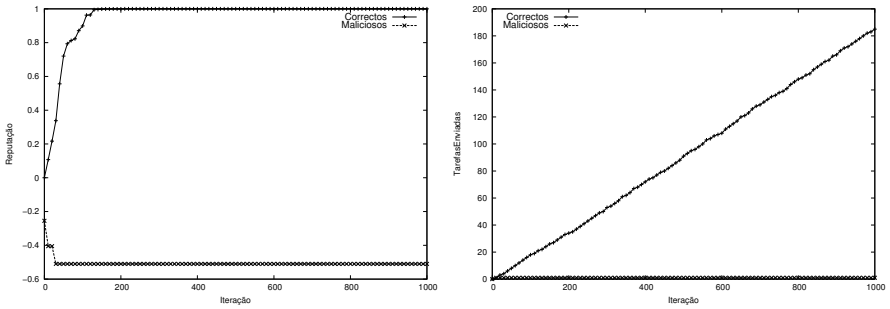
comportamento impede o dispositivo servente de receber o dinheiro correspondente à transação. Neste caso, os serventes apresentam queixa sobre o dispositivo malicioso, no seu próximo contacto com a ECC. A Fig. 4, mostra que os dispositivos maliciosos são corretamente detetados pelos restantes. Ao fim de algumas iterações, a propagação de reputação faz com que os restantes dispositivos deixem de aceitar as propostas dos dispositivos maliciosos para executar tarefas. Desta forma o dinheiro que os dispositivos maliciosos têm em carteira deixa de lhes servir para executar tarefas e mesmo a mudança de pseudónimo não lhes permite execuções de tarefas, devido à impossibilidade de apresentar um certificado de reputação recente. Durante esta experiência observámos também que que o dinheiro virtual dos dispositivos maliciosos é superior ao dos restantes. No entanto isto apenas significa que estes dispositivos estão a conseguir executar operações de débito. A Fig. 4(b) confirma que não o conseguem utilizar na execução de novas tarefas.

Um efeito colateral deste ataque é a redução do total de TwinCoins no sistema, descartadas pela ECC a cada reclamação. Assim neste modelo de ameaça,



(a) Reputação (b) Tarefas enviadas

Figura 4. Simulação para o modelo de ameaça 2

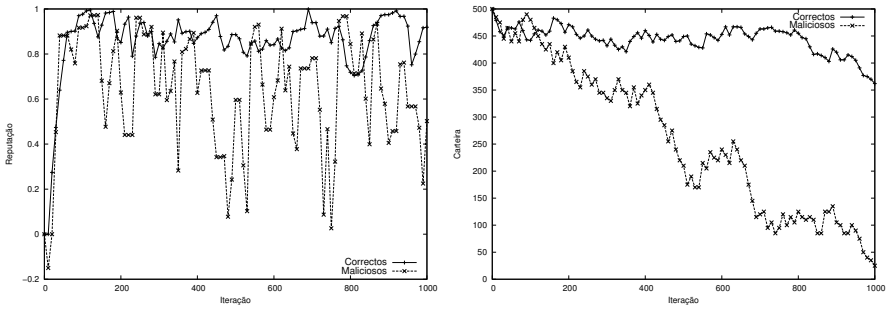


(a) Reputação (b) Tarefas enviadas

Figura 5. Simulação para o modelo de ameaça 3

ao fim das 1000 iterações da simulação, perdeu-se cerca de 21% do dinheiro virtual existente no mercado. Este resultado sugere a necessidade de re-injeção de TwinCoins nas contas dos dispositivos utilizando um modelo que não beneficie os infratores.

Modelo de Ameaça 3: Ataque à CNC. A modelação deste ataque simula dispositivos que em vez de executar a tarefa, e consumir assim os seus recursos, respondem imediatamente com resultados forjados. A resposta do sistema a este ataque representada na Fig. 5, é semelhante à do modelo de ameaça 2. Contudo, nota-se uma convergência mais rápida para os valores finais que se devem ao facto de ser apenas a execução correta de uma tarefa que aumenta a reputação de um dispositivo. Assim, basta os dispositivos maliciosos devolverem resultados errados para nunca verem a sua reputação melhorada, conseguindo assim a desconfiança de todos os restantes dispositivos. Devida à deteção mais rápida dos dispositivos egoístas, o dinheiro virtual existente no mercado apenas decresce em sensivelmente 1% até ao final da simulação.



(a) Reputação (b) Dinheiro virtual nos dispositivos

Figura 6. Simulação para o modelo de ameaça 4

Modelo de Ameaça 4: Malicioso cuidadoso. Neste perfil, um dispositivo realiza apenas uma ação maliciosa, optando com probabilidades iguais por injetar resultados errados ou por não cumprir o protocolo de dinheiro virtual. Após o ataque, o dispositivo comporta-se corretamente até ter hipótese de trocar de pseudónimo. Após a mudança de pseudónimo volta a comportar-se de forma incorreta. Neste modelo de ameaça podemos dizer que os dispositivos maliciosos são em parte bem sucedidos, o que resulta do seu comportamento entre acessos à ECC. No entanto, assim que assumem comportamentos maliciosos, os dispositivos são penalizados. Na Fig. 6(b) é visível que o dinheiro virtual em carteira dos dispositivos maliciosos decresce mais rapidamente, em contraste com os dispositivos corretos. A reputação dos dispositivos maliciosos (Fig. 6(a)), é inferior à dos restantes, apesar de ser suficiente para o dispositivo ser selecionado para executar algumas tarefas. Assim, um dispositivo malicioso pode explorar o limiar de reputação, de forma a não descer abaixo dele. De acordo com as definições na Tab. 1, este limiar para os dispositivos corretos é de -0,25.

3.3 Avaliação Global

Os resultados anteriores confirmam a robustez de um sistema híbrido de incentivo e confiança a ataques de um pequeno número de participantes. Contudo, importa também avaliar o seu comportamento na presença de um número elevado de dispositivos maliciosos. Sendo o modelo de ameaça 4 aquele que maior interferência mostrou provocar no sistema, foram realizadas simulações com 10%, 20%, 50%, 80% e 90% de dispositivos exibindo este comportamento. Para cada percentagem, foram realizadas 5 simulações. A Fig. 7 apresenta a distribuição média das classificações atribuídas pelo sistema aos nós, em função da reputação que apresentavam no final das simulações. O gráfico considera como falso negativo um dispositivo malicioso, detetado como correto ($GR_u > 0$) e um falso positivo um dispositivo correto, detetado como malicioso ($GR_u <= 0$).

Os resultados demonstram que a possibilidade de um nó malicioso conseguir escapar sem ser detetado é muito baixa, mesmo utilizando o modelo de ameaça

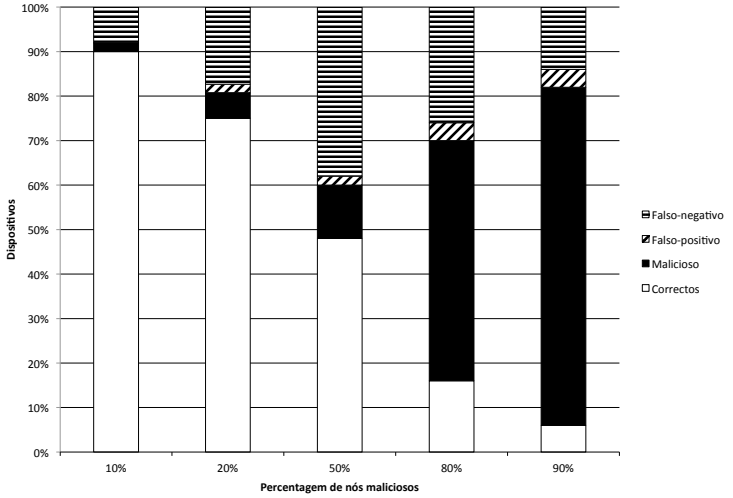


Figura 7. Robustez a dispositivos maliciosos

menos favorável. A maior funcionalidade do sistema proposto resulta de que, quanto maior é a percentagem de nós maliciosos no sistema, melhor este os vai detetar. Isto acontece porque os dispositivos maliciosos acabam por se prejudicar mutuamente, nunca retirando os benefícios esperados com as suas ações.

4 Trabalho Relacionado

A teoria dos jogos sugere que os participantes num dado sistema se comportam de forma racional, ou seja, de todas as ações possíveis os participantes irão escolher aquela que maior benefício lhes traz face ao custo dessa mesma ação [12]. Num ambiente de Computação em Nuvem Colaborativa (CNC), esta decisão centra-se no facto de um utilizador partilhar ou não os recursos do seu dispositivo móvel. A existência de um número considerável de utilizadores que optam por partilhar foi já observada noutras formas semelhantes a uma CNC, nomeadamente em projetos de computação colaborativa.

Por detrás desta decisão podem estar os incentivos oferecidos pelo sistema, como a retribuição em forma de créditos, ou a criação de confiança [13]. Nos sistemas baseados em confiança não existe remuneração pela execução de uma tarefa. O nível de confiança entre dispositivos passa pela classificação numérica da confiança, que é incrementada sempre que uma tarefa é executada com sucesso. Num modelo baseado em retribuição/troca, executar uma tarefa implica uma remuneração, tipicamente na forma de dinheiro virtual [11, 16]. O dinheiro virtual é usado para estabelecer um modelo económico entre dispositivos.

Os sistemas de reputação têm sido alvo de interesse considerável no âmbito das redes de partilha de ficheiros entre-pares (P2P). As concretizações variam entre a necessidade de uma entidade confiável e central ou, em alternativa, vistas

locais a cada participante [1, 6, 7]. Contudo, nenhum destes sistemas assume a possibilidade do sistema funcionar com ligações transientes à Internet.

Na camada de rede podemos encontrar sistemas de reputação para a identificação de nós egoístas [5,9]. A maioria destes sistemas assume a indisponibilidade de uma entidade confiável e central partindo do pressuposto de que quando um nó egoísta é detetado, a sua identificação é disseminada na vizinhança. Contudo, os sistemas falham na identificação duradoura do comportamento dos nós, em particular em ambientes onde a vizinhança é transitória.

Alternativamente, os utilizadores podem descartar a sua (má) reputação apresentando-se ao sistema com múltiplas identidades não relacionadas. Para resolver este problema, pode ser utilizado um identificador imutável, emitido por uma entidade confiável [14]. Contudo, um identificador imutável levanta problemas de privacidade, já que reduz as expectativas de anonimato dos utilizadores. Uma plataforma que combina a preservação do anonimato sem descartar a reputação foi apresentado em [10]. Contudo esta solução é bastante dispendiosa computacionalmente e por isso vocacionada para cenários onde os dispositivos não tenham limitações energéticas, como as redes veiculares.

Os Nuglets [3] são um sistema baseado em trocas para redes móveis *Ad-hoc* que define uma moeda de forma a fornecer incentivo para cooperação no encaminhamento de pacotes. O sistema assume que as moedas (Nuglets) de cada dispositivo são armazenadas num componente de hardware inviolável que previne simultaneamente alguns dos comportamentos assumidos. Contudo este componente não está disponível em todas as plataformas.

A aplicação de mecanismos de criptografia assimétrica no suporte a um protocolo seguro é abordada em [8]. Os autores reconhecem a complexidade computacional do mecanismo, aliviando a complexidade após os primeiros passos do estabelecimento da relação de confiança.

5 Conclusões

Os ambientes de computação móvel em nuvem colaborativa necessitam de mecanismos para lidar com a transitividade dos grupos e com a inerente falta de confiança entre membros. Os desafios são amplificados pelas limitações de recursos dos dispositivos utilizados, o que obriga à criação de incentivos à cooperação. Infelizmente, a maioria dos sistemas de reputação que têm vindo a ser propostos assume que a cooperação de todos os dispositivos é obrigatória e que deve ser independente da vontade do utilizador em participar.

Este artigo valida a introdução de um sistema híbrido de confiança e incentivo que combina um sistema de reputação com dinheiro virtual. O sistema permite que os utilizadores beneficiem do sistema de forma proporcional ao seu contributo, enquanto penaliza utilizadores que tentem usar o sistema apenas em seu proveito. Os resultados das simulações sugerem que o sistema é capaz de tolerar um número elevado de utilizadores maliciosos, classificando-os corretamente. A classificação correta dos utilizadores maliciosos é algo esperado de um sistema destes, mas de todas as funcionalidades apresentadas, a não classificação

incorreta dos utilizadores honestos revela-se necessária para justificar a adoção de um sistema destes numa CNC.

O trabalho irá seguir de maneira a introduzir mais modelos de ameaça, bem como discutir alguns dos pontos ainda em aberto no ambiente da computação em nuvem colaborativa. Posteriormente, o sistema será integrado numa CNC.

Referências

1. Anagnostakis, K.G., Greenwald, M.B.: Exchange-based incentive mechanisms for peer-to-peer file sharing. In: Procs. of the 24th Int'l Conf. on Distributed Computing Systems (ICDCS 2004). pp. 524–533 (2004)
2. Anderson, D.P.: BOINC: a system for public-resource computing and storage. In: Procs. of the 5th IEEE/ACM Int'l Works. on Grid Computing (GRID 2004). pp. 4–10 (2004)
3. Buttyan, L., Hubaux, J.: Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks. Technical Report DSC/2001/001, Swiss Federal Institute of Technology (2001)
4. Cruz, N., Miranda, H.: Arquitectura para uma computação em nuvem colaborativa entre dispositivos móveis. In: Atas do INFORUM 2011 - Terceiro Simpósio de Informática. pp. 450–455 (Sep 2011)
5. Hu, J., Burmester, M.: Cooperation in mobile ad hoc networks. Guide to Wireless Ad Hoc Networks pp. 1–15 (2009)
6. Jun, S., Ahamad, M.: Incentives in BitTorrent induce free riding. In: Procs. of the 3rd ACM SIGCOMM Works. on Economics of Peer-to-Peer Systems (P2PECON 2005). pp. 116–121 (2005)
7. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In: Proceedings of the 12th Int'l Conf. on World Wide Web. pp. 640–651. WWW '03, ACM (2003)
8. Mahmoud, M.E., Shen, X.: ESIP: secure incentive protocol with limited use of public-key cryptography for multi-hop wireless networks. IEEE Transactions on Mobile Computing (2010)
9. Mahmoud, M.E., Shen, X.: Stimulating cooperation in multi-hop wireless networks using cheating detection system. In: Procs. of the 29th IEEE Int'l Conf. on Computer Communications (INFOCOM 2010). pp. 1–9 (2010)
10. Miranda, H., Rodrigues, L.: Reputation in anonymous vehicular networks. Journal of Autonomous and Adaptive Communications Systems 3(2), 178–197 (2010)
11. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2009), http://fastbull.dl.sourceforge.net/project/bitcoin/Design%20Paper/bitcoin.pdf/bitcoin.pdf
12. Neumann, J.V., Morgenstern, O.: Theory of Games and Economic Behavior. Princeton University Press (1944), http://jmvidal.cse.sc.edu/library/neumann44a.pdf
13. Obreiter, P., Nimis, J.: A taxonomy of incentive patterns. In: Moro, G., Sartori, C., Singh, M. (eds.) Agents and Peer-to-Peer Computing, Lecture Notes in Computer Science, vol. 2872, pp. 89–100. Springer Berlin / Heidelberg (2005)
14. Resnick, P., Kuwabara, K., Zeckhauser, R., Friedman, E.: Reputation systems. Communications of the ACM 43(12), 45–48 (2000)
15. Resnick, P., Zeckhauser, R.: Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system. Advances in Applied Microeconomics: A Research Annual 11, 127–157 (2002)
16. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., 2nd edn. (1995)