Criptografia Baseada em Identidade: Uma Análise Comparativa sob a Perspectiva da Internet das Coisas

Antonio L. Maia Neto[1], Michele Nogueira[2], Harsh Kupwade Patil[3], Ítalo Cunha[1], Antonio A. F. Loureiro[1], Leonardo B. Oliveira[1]

[1]UFMG [2]UFPR [3]LG Mobile Research
{lemosmaia,cunha,loureiro,leonardo.barbosa}@dcc.ufmg.br
michele@inf.ufpr.br harsh.patil@lge.com

Abstract. *Identity-Based Cryptography (IBC) employs user's identity as public key, eliminating digital certificates. IBC is promising in constrained environments as Internet of Things (IoT) due to its benefits, such as facilitating public key management. However, different aspects on IBC (e.g. the need for bilinear pairing) require attention when applied to IoT in order to meet basic security requirements on these environments. This paper presents a comparative analysis of identity-based cryptosystems considering their application in IoT. The main characteristics of IoT serve as reference for the analysis. Hence, this paper contributes giving an overview about the benefits and drawbacks of the main identity-based cryptosystems on IoT.*

1. Introdução

Internet das Coisas (*Internet of Things – IoT*, do inglês) é uma rede de dispositivos fortemente conectados, dando suporte a aplicações ubíquas em diversas áreas (ex. saúde, segurança física, automação industrial e transportes) além de facilitar as atividades cotidianas [Sicari et al. 2015]. A IoT inclui diferentes tipos de dispositivos, como sensores, atuadores, etiquetas RFID, *smartphones* e servidores, com capacidades computacionais, funcionalidades e tamanhos diferentes. A segurança é um requisito fundamental para muitas dessas aplicações, sendo necessária a proposição de mecanismos de segurança apropriados para tratar com as características desse novo ambiente, expectativas e necessidades de segurança computacional dos usuários [Sicari et al. 2015].

Técnicas criptográficas vêm sendo aplicadas por vários anos para proteger os dados digitais de falsificação ilegal e roubo. O conceito de criptografia baseada em identidade (IBC – *Identity-Based Cryptography*) [Shamir 1984] tem se destacado, uma vez que as chaves públicas são derivadas de informações públicas univocamente identificando um usuário (*e.g.* CPF para indivíduos ou IP para máquinas) e dispensam mecanismos de autenticação. A IBC possui várias vantagens contribuindo positivamente para a proteção dos dados digitais no ambiente complexo da IoT [Sicari et al. 2015]. Ela simplifica o gerenciamento de chaves públicas, por eliminar o uso de certificados digitais, além de reduzir a sobrecarga de comunicação com trocas de mensagens de verificação de certificados e o tempo de resposta das aplicações. Há um ganho considerável em eficiência, pois para uma comunicação segura e autentica, não há necessidade de troca de chaves, além de uma redução da complexidade e do custo para estabelecer e manter a infraestrutura de chaves públicas. Tais características fazem a IBC convergir com as necessidades da IoT.

Objetivo: A IBC apresenta desvantagens, por exemplo a necessidade por uma entidade incondicionalmente confiável (*Public Key Generator* – PKG), responsável por

gerar e manter a custódia das chaves privadas do sistema. A PKG é capaz de personificar qualquer usuário. Outra exigência da IBC é que chaves devem ser entregues aos usuários através de canais confidenciais e autenticados. No entanto, como o mecanismo de criptografia em geral precisa ser usado para engendrar (*bootstrap*) o esquema de segurança, tais canais ainda não existem. Desta forma, este artigo procura contribuir com a literatura através de uma análise comparativa entre criptossistemas baseados em identidade e suas adequações quando aplicados ao contexto de IoT. As análises comparativas consideram as características de cada criptossistema analisado assim como as características e requisitos de segurança dos usuários no ambiente ubíquo. Este artigo aponta os pontos fortes e fracos de cada criptossistema para o ambiente da IoT, contribuindo assim para uma visão mais clara sobre suas vantagens e desvantagens.

2. Análise Comparativa

Identificados da literatura, cinco criptossistemas baseados em identidade formam a base para a análise comparativa apresentada nesta seção. Dentre os criptossistemas estão: *Identity Based Encryption (IBE)*, *Cocks*, *Boneh-Gentry-Hamburg (BGH)*, *Secure Key Issuing (SKI)* e *ID-based Authenticated Key Agreement (ID-AKA)*. Eles representam dois grupos principais classificados pela sua forma de implementação: $i)$ suportados por emparelhamentos e $ii)$ suportados por estratégias alternativas ao emparelhamento, como por exemplo, resíduos quadráticos e o problema de Diffie-Hellman, *i.e.* uso de operações matemáticas fáceis de computar, porém difíceis de reverter. Esses dois grupos são diferenciados pelos seus custos computacionais. O cálculo de emparelhamentos, por exemplo, gera um alto custo computacional tornando as propostas de IBC suportadas por essa solução inadequadas para os dispositivos em IoT.

Dentre os aspectos observados na análise comparativa, além do suporte por emparelhamento ou outra estratégia, estão a custódia de chaves, o tamanho dos criptogramas, necessidade de algoritmos aleatórios e necessidade de acordo de chaves. A seguir, as principais características das cinco abordagens analisadas são brevemente descritas a fim de contextualizar os aspectos principais de cada abordagem sumarizados na Tabela 1.

IBE [Boneh and Franklin 2001]: uma das primeiras implementações de IBC, tem como base os emparelhamentos bilineares. Além disso, se apoia em uma PKG incondicionalmente confiável, introduzindo o problema da custódia de chaves;

Cocks [Cocks 2001]: estratégia que surgiu paralelamente à proposta IBE, é suportada por resíduos quadráticos, que são computacionalmente mais baratos que emparelhamentos. Este esquema possui a mesma estrutura de entidade confiável adotada em IBE, portanto, não trata o problema da custódia de chaves. Uma característica importante é que o algoritmo de cifração inclui dois elementos internos a cada bit da mensagem original, produzindo mensagens cifradas muito grandes;

BGH [Boneh et al. 2007]: suportado por resíduos quadráticos, o BGH tem a mesma estrutura de geração de chaves que o IBE e o Cocks, mantendo o problema da custódia de chaves. Com o intuito de diminuir o problema do tamanho das mensagens cifradas de Cocks, o BGH sugere um novo algoritmo de cifração onde elementos aleatórios são reutilizados. Entretanto, esse algoritmo tem complexidade polinomial de ordem quatro, o que diminui consideravelmente a eficiência do método;

SKI [Lee et al. 2004]: baseado no emparelhamento bilinear, o diferencial do SKI é a

adoção de uma estrutura hierárquica de autoridades confiáveis, composto por um centro de geração de chaves (*Key Generation Center* – KGC), que produz as chaves privadas, além de múltiplas autoridades de manutenção da privacidade das chaves (*Key Privacy Authorities – KPAs*). Essa estrutura resolve parcialmente o problema da custódia de chaves, pois permite que as KPAs cooperem mutuamente para reaver o conteúdo de mensagens cifradas neste sistema. Esta cooperação é conhecida como conluio por mensagem. Um aspecto negativo da adição das KPAs é o aumento do custo de implantação e manutenção do criptossistema, pois há mais elementos envolvidos;

ID-AKA [Cao et al. 2010]: tem como base o problema Diffie-Hellman, sendo mais eficiente que o uso de emparelhamentos bilineares. A confiança em um PKG é mantida, não resolvendo o problema da custódia de chaves. A principal diferença do ID-AKA é completar o acordo de chaves com a troca de apenas duas mensagens, reduzindo significativamente a sobrecarga de comunicação em relação às outras propostas.

	IBE	**Cocks**	**BGH**	**SKI**	**ID-AKA**
Base	emparelhamento bilinear	resíduos quadráticos	resíduos quadráticos	emparelhamento bilinear	problema Diffie-Hellman
Prós	criptogramas com tamanho equivalente à mensagem original	mais eficiente que BGH	criptogramas com tamanho equivalente à mensagem original	criptogramas com tamanho equivalente à mensagem original previne custódia de chaves	criptogramas com tamanho equivalente à mensagem original algoritmos aleatórios acordo de chaves com duas mensagens
Contras	custódia de chaves	custódia de chaves criptogramas muito grandes	custódia de chaves menos eficiente que Cocks	conluio por mensagens + autoridades intermediárias	custódia de chaves

Tabela 1. Comparação entre criptossistemas baseados em identidade.

A Tabela 1 explicita as características dos sistemas IBC comparados neste trabalho. O primeiro aspecto que deve ser considerado em um ambiente IoT são os custos computacionais. Nesse sentido, as estratégias IBE e SKI são as mais caras, pois são baseadas em emparelhamentos bilineares. A adoção de resíduos quadráticos no trabalho de Cocks de fato alcança eficiência temporal. Entretanto, o algoritmo de cifração acaba por produzir mensagens cifradas muito grandes, que exigem maior espaço para armazenamento e geram sobrecarga de comunicação devido a sua transmissão. Essa característica pode não ser adequada se o ambiente IoT considerado envolver dispositivos com baixa capacidade de armazenamento ou comunicação. Já na proposta de BGH, a ideia é resolver o problema dos grandes criptogramas de Cocks. Esse objetivo é atingido, mas o algoritmo de cifração que diminui o tamanho das mensagens cifradas é de complexidade polinomial de ordem quatro, tornando o sistema ineficiente em termos computacionais. Assim, o sistema que se mostra mais adequado a um cenário IoT onde o principal fator é eficiência, consiste na estratégia ID-AKA, que adota como base o problema de Diffie-Hellman para resolver essa questão. ID-AKA também se mostra adequada quando se considera a comunicação dos dispositivos IoT, uma vez que permite a troca de chaves com apenas duas mensagens.

O segundo aspecto considerado é a custódia de chaves, que pode inviabilizar a implantação de um ambiente IoT se os dispositivos não puderem confiar incondicionalmente em uma única autoridade central. O único criptossistema comparado nesse trabalho que aborda esse problema é o SKI, que adota uma estrutura hierárquica de autoridades confiáveis, adicionando múltiplas autoridades de manutenção da privacidade das chaves. Contudo, o problema não é tratado de forma definitiva, pois existe a possibilidade de conluio por mensagem, que pode ocorrer quando as autoridades intermediárias cooperam mutuamente para reaver o conteúdo de mensagens cifradas neste sistema. Um aspecto negativo da adição das KPAs é o aumento do custo de implantação e manutenção do criptossistema, o que pode dificultar sua adoção em ambientes IoT. Além disso, a inclusão de KPAs também aumentará tempos de respostas das aplicações.

3. Conclusão

Comunicação sem fio, escalabilidade, hetereogeneidade, restrições de recursos computacionais e requisitos como baixa latência e alta vazão de algumas aplicações são características que devem ser consideradas na definição dos sistemas de segurança adotados em um ambiente de IoT. Nesse contexto, a criptografia baseada em identidade possui várias vantagens que contribuem positivamente para a proteção dos dados digitais, a principal delas é a simplificação do gerenciamento de chaves públicas. Entretanto, a IBC apresenta algumas desvantagens, como, por exemplo, o problema da custódia das chaves privadas do sistema. Este trabalho contribui com a literatura apresentando uma análise comparativa dos criptossistemas baseados em identidade e suas adequações quando aplicados ao contexto de IoT. Como conclusão, observa-se que não há solução ideal, onde todos os requisitos da IoT, de suas aplicações e dos usuários são tratados conjuntamente. Nem mesmo requisitos básicos são tratados conjuntamente por um único esquema, sendo portanto uma questão em aberta de pesquisa desenvolver esquemas mais próximos aos requisitos dos dispositivos, aplicações e usuários de uma IoT.

Referências

Boneh, D. and Franklin, M. K. (2001). Identity-based encryption from the weil pairing. In *CRYPTO '01*, pages 213–229. Springer-Verlag.

Boneh, D., Gentry, C., and Hamburg, M. (2007). Space-efficient identity based encryption without pairings. In *FOCS'07*, pages 647–657.

Cao, X., Kou, W., and Du, X. (2010). A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. *Information Sciences*, 180(15):2895–2903.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In *8th IMA Int'l Conference on Cryptography and Coding*, pages 360–363. Springer-Verlag.

Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J., and Yoo, S. (2004). Secure key issuing in id-based cryptography. In *Workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation*, pages 69–74.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *CRYPTO'84*, pages 47–53. Springer-Verlag.

Sicari, S., Rizzardi, A., Grieco, L., and Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. *Comp. Networks*, 76:146 – 164.

