Análise de Desempenho de um Esquema de Acordo de Chaves de Conferência para IoT

Mateus Coutinho Marim, Kristtopher K. Coelho, Alex B. Vieira, José Augusto M. Nacif,
Michele Nogueira, Edelberto Franco Silva

***Abstract*—Wireless networks and their recent applications in the Internet of Things (IoT) have the evident necessity of mechanisms that increase its exchanged data reliability and integrity. Therefore, key agreement schemes are strong candidates to meet these requirements. Considering the resource constraints in IoT networks, verifying these limitations is vital. In this work, an analysis of computational feasibility and a proposal for using a one-way key agreement method based on second-degree equations for an IoT environment are performed. For the analysis, we simulated a network of up to 50 devices. It considered memory consumption, the time for session key generation, the size of the generated key, and the overhead in time for message exchange. The results show that the method applies to IoT networks, presenting a linear growth in the key agreement time and constant processing even with increasing the key size.**

***Index Terms*—Acordo de Chaves, IoT**

I. Introdução

A Internet das Coisas (IoT) compreende a interconexão de elementos em redes altamente heterogêneas. Atualmente, IoT está presente nos mais diferentes setores, desde casas inteligentes à Indústria 4.0, portanto espera-se que a quantidade de dispositivos conectados alcance 75 bilhões até 2025 [1]. O ambiente IoT é extremamente conectado e rico em troca de informações, indicando um cenário promissor para soluções baseadas em grupos. A comunicação de grupos ou transmissão múltipla (*multicast*) ocorre quando uma mensagem é transmitida para um conjunto de nós. Entretanto existe a necessidade de mecanismos de segurança que garantam os princípios da privacidade, confidencialidade e integridade dos dados. Porém, a maioria dos dispositivos IoT possuem recursos computacionais limitados, como memória, poder de processamento e consumo de energia [2]. Portanto, mesmo que esquemas de acordo de chaves sejam potenciais candidatos a atender os requisitos de segurança, faz-se necessário, além de propor e avaliar os mecanismos de segurança, verificar sua aderência com relação às limitações de *hardware*.

Para que uma mensagem trafegue entre dispositivos IoT de forma segura é possível adotar a criptografia simétrica ou assimétrica para geração de chaves. Além disso, é possível estabelecer uma chave criptográfica compartilhada entre três ou mais participantes de uma comunicação. Método conhecido como acordo de chaves de conferência [3]. Nesse esquema, todos os participantes influenciam a chave a ser gerada. Neste artigo, nós avaliamos o potencial de um método de geração de chaves compartilhadas a partir de chaves de conferência para $N > 2$ participantes e com complexidade de $\mathcal{O}(n)$ aplicado ao ambiente de IoT. Sabendo que o problema de chave de conferência é NP-Completo e que não existe método seguro o suficiente [4], este trabalho aplica o método proposto por Kowada e Machado [3] como forma de avaliação da escalabilidade de métodos de acordo de chaves para uma rede com $N \leq 50$ dispositivos. Além disso, este trabalho propõe uma arquitetura de aplicação para IoT que permite reduzir as vulnerabilidades intrínsecas do método de Kowada e Machado, e outros tantos dessa classe de métodos.

Para validação da proposta foi desenvolvido um ambiente simulado de dispositivos IoT sobre uma arquitetura real de troca de mensagens através de um intermediador (*broker*) *Message Queuing Telemetry Transport* (MQTT) [5]. Neste cenário, foi possível verificar a escalabilidade do mecanismo de acordo de chaves de conferência em uma rede de até 50 dispositivos. As métricas de avaliação de desempenho consideradas foram o consumo de memória, o tempo para a geração da chave compartilhada e o tamanho da chave gerada e o *overhead* no tempo para a troca de mensagens. Os resultados mostraram-se promissores para aplicação em redes IoT com dispositivos de recursos limitados. Em relação ao estado da arte, este trabalho se posiciona no ramo da avaliação do desempenho de métodos de geração de chaves compartilhadas com acordo de uma via aplicado ao ambiente de IoT.

II. Trabalhos Relacionados

Um dos métodos precursores na criptografia para geração de chaves compartilhadas por um canal inseguro é o Diffie–Hellman [6], [7]. O método permite que duas partes sem conhecimento prévio estabeleçam em conjunto uma chave secreta compartilhada. De modo análogo, o protocolo de acordo de chave de grupo (*Group Key Agreement* - GKA) permite que um grupo de usuários/nós negocie uma chave de sessão única para proteger a comunicação em uma rede não confiável. Burmester e Desmedt [8] propuseram o método base para conferência de chaves em uma via (troca de chave não interativa) e rodadas constantes. Posteriormente, outros autores

Este trabalho foi apoiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq/Brasil), pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES/Brasil), e pela Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG).
Mateus Coutinho Marim, Edelberto Franco Silva e Alex B. Vieira são do Departamento de Ciência da Computação da Universidade Federal de Juiz de Fora, MG – Brasil. E-mail: {mateus.marim, edelberto}@ice.ufjf.br e alex.borges@ufjf.edu.br. Michele Nogueira é do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais, MG – Brasil. E-mail: michele@dcc.ufmg.br. Kristtopher K. Coelho e José Augusto M. Nacif é do Instituto de Ciências Exatas e Tecnológicas da Universidade Federal de Viçosa *Campus* Florestal, MG – Brasil. E-mail: {kristtopher.coelho, jnacif}@ufv.br.

implementaram variações de modo a aumentar a resiliência a ataques [9].

Para ambiente específico IoT, Tedeschi *et al.* [10] propõem o protocolo leve de acordo de chaves de grupo sem certificado LiKe. O LiKe é caracterizado por materiais de criptografia efêmeros, suporte para conectividade intermitente com um terceiro confiável (*Trusted Third Party* – TTP), operações leves de re-chaveamento e robustez contra ataques de personificação. Garg *et al.* [11] propõe um protocolo de segurança com acordo de chaves em IoT para casas inteligentes (*smart home*) chamado *Multi-device Key Agreement* (MKA). O protocolo é baseado nas propriedades de funções *hash* e criptografia de curva elíptica. Kowada e Machado [3] propuseram um esquema de acordo de chaves baseado em equações diofantinas de segundo grau com duas variáveis de uma via com complexidade de $\mathcal{O}(n)$ para estabelecimento da chave compartilhada. O método possui bom desempenho em relação às características de economia de recursos computacionais dos dispositivos IoT.

Motivados pelo desempenho em relação a economia de recursos computacionais, este trabalho avalia a escalabilidade de um método de criptografia de chaves de conferência para $N > 2$ participantes. O método proposto possui característica de uma via (*one way*) e tem complexidade $\mathcal{O}(n)$ [3]. A metodologia aqui aplicada permite ainda que, métodos com características semelhantes e respectivas variantes, como [8], também sejam avaliados quanto à escalabilidade.

III. Proposta

A. Método

O esquema proposto por [3] consiste na construção de uma chave comum entre os participantes do grupo a partir da troca de mensagens que contém o resultado de uma função quadrática. Para ser gerado o valor da função quadrática, são usados parâmetros de sessão gerados por um dos dispositivos participantes do grupo e também valores aleatórios gerados por cada participante. O padrão geral para escolha dos valores de α, β e δ dependem da escolha de duas sequências de primos com tamanho m e n. O nível de segurança e o tamanho da chave serão impactados pelos valores de m e n. À seguir descreve-se o passo a passo do algoritmo em questão:

- Um representante do grupo:
  1) Escolhe um α e β
  2) Calcula $\alpha = \varphi(\delta)$
  3) Escolhe y coprimo com δ
  4) Publica y, α, β, γ e δ no *broker*
- Cada usuário i do grupo após receber a sequência:
  1) Escolhe um par (x_{a_i}, x_{b_i}), tal que $\text{mdc}(x_{b_i}, \alpha) = 1$
  2) Calcula $\gamma_i = \alpha x_{a_i}^2 + \beta x_{b_i}$
  3) Publica γ_i no *broker*

Seja $\{e_1, e_2, \ldots, e_r\} \in \{1, \ldots, s\}$ o subgrupo de r partes (de um total de s) que desejam se comunicar. Para e_1, por exemplo, saber a chave desse sub-grupo, basta calcular $k = y^z \mod \delta$, onde $z \equiv x_{b_1} \prod_{t=2}^{r} \gamma_{e_t} \mod \alpha$. Neste caso, tem-se a Equação 1.

$$k = y^{\beta^{r-1}} \prod_{t=1}^{r} x_{b_{e_t}} \mod \delta. \quad (1)$$

O ambiente de simulação IoT foi criado com um *broker* sobre o protocolo de comunicação MQTT. A Figura 1 representa a estrutura utilizada para os experimentos, o servidor nomeado de Trevor gera os parâmetros compartilhados entre os membros e os envia para os nós IoT conectados e autenticados na rede. Todos os novos membros do grupo devem computar o valor da função diofantina γ_i que é compartilhada para cada um dos outros participantes. Assim, depois que todos os membros recebem os valores de γ_i, a chave compartilhada é computada por cada um deles, que no fim chegam aos mesmos resultados (chave de conferência). Para que esse esquema possa ser usado em uma rede IoT real, os parâmetros "públicos" só são compartilhados pelos nós que se autenticarem no *broker* MQTT, evitando que qualquer nó malicioso possa ter acesso a eles e realizar uma criptoanálise.

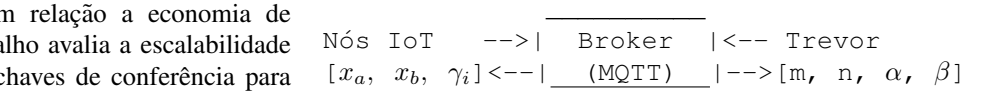

Figura 1. Arquitetura de rede escolhida para a implementação do esquema de acordo de chaves.

B. Metodologia

Para verificar a viabilidade de um esquema de geração de chaves compartilhadas baseado em chave de conferência para um ambiente IoT, foram realizados experimentos simulando uma rede de até 50 dispositivos conectados em um servidor confiável responsável pela geração dos parâmetros iniciais da sessão. A comunicação entre os dispositivos e o servidor é feita por um elemento intermédio/*broker*.

O ambiente de simulação foi desenvolvido com a `IDE Qt Creator` com as bibliotecas `QtCore`, que contém as funcionalidades padrões do `Qt`, `QtMQTT` para permitir a comunicação com o *broker* e com a `Boost` *GNU Multi-Precision* (GMP), para a manipulação de inteiros grandes. O ambiente computacional foi composto por um processador `Intel Core i5-7200U @ 2.5GHZ 64-bit` com `8GB` RAM no sistema operacional `Arch Linux 64-bit`. Os experimentos foram executados 10 vezes, variando o número de dispositivos entre 2 e 50 de forma a gerar uma margem de confiança nos resultados (intervalo de confiança de 95%).

As métricas consideradas na avaliação de desempenho, são referentes ao consumo de recursos computacionais, entre elas, o tempo de execução para geração das chaves de sessão, o *overhead* no tempo para a troca de mensagens e também o tamanho das chaves que podem ser geradas em um tempo factível, já que as mesmas poderiam ser quebradas com força bruta caso fossem muito curtas.

IV. Resultados

O primeiro experimento verifica o crescimento da curva de tempo de execução do esquema variando a quantidade de dispositivos. Portanto, a Figura 2, ilustra o crescimento do tempo

de execução de cada sessão individualmente considerando o maior tempo entre todos os dispositivos em uma sessão. Já a Figura 3 apresenta o tempo acumulado de cada sessão. As medidas de tempo do primeiro resultado representam a execução de uma sessão com um número fixo de dispositivos, enquanto no segundo, o comportamento simula a entrada de novos dispositivos na sessão ao longo do tempo.

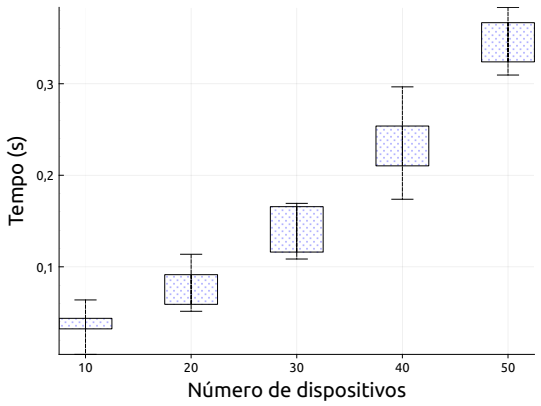

Figura 2. Diagrama de caixas do tempo individual contra o número de dispositivos.

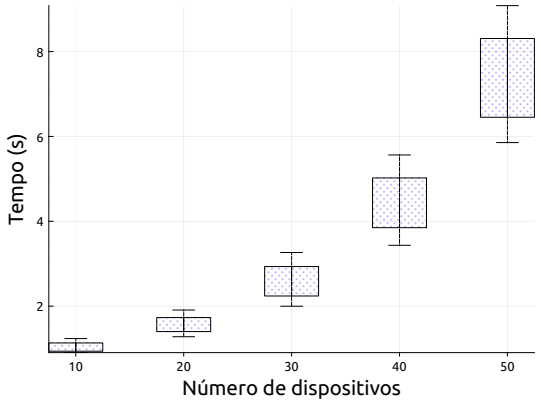

Figura 3. Diagrama de caixas do tempo cumulativo contra o número de dispositivos.

As operações realizadas pelos participantes de cada sessão tem certa influência no comportamento geral das curvas. Verificamos que esse comportamento é linear ao número de dispositivos conectados na rede. Outro fator que tem grande relevância no acordo das chaves é a quantidade de mensagens trocadas pelos dispositivos, o qual aumenta conforme o número de participantes na rede cresce. Como anteriormente enfatizado, a abordagem GKA escolhida [3], tem complexidade linear para as mensagens em relação ao número de dispositivos, o que foi verificado experimentalmente. Com a conexão sucessiva de dispositivos na rede, o número de mensagens trocadas obedece a uma progressão aritmética, cuja soma resulta em uma curva quadrática, conforme ilustrado na Figura 3. Ainda é possível notar nestes gráficos, o crescimento relativo à complexidade $\mathcal{O}(n)$, onde, conforme mais dispositivos entram na rede, maior é o tempo de processamento necessário para a geração das chaves. Destaca-se os valores de variação para 20 e 40 dispositivos, onde o crescimento apresentado foi de $\approx$ 2X em relação ao tempo total necessário.

A Figura 4 relaciona a variação do tempo, do tamanho das chaves e o número de dispositivos através da execução do esquema com diferentes combinações dos parâmetros m e n. Por questão de simplicidade os parâmetros foram testados com valores iguais. É possível observar, a partir das superfícies geradas, que o tamanho da chave não tem uma alta variabilidade conforme a quantidade de dispositivos na rede aumenta. Essa característica é fundamental para garantir a escalabilidade. Consequentemente, torna previsível a quantidade de dispositivos com um determinado *hardware* que a rede irá suportar. Outra informação relevante extraída da Figura 4 é que, mesmo com o tamanho da chave crescendo, o tempo de execução do esquema para o acordo das chaves não se altera proporcionalmente, assim o tempo de execução não se torna uma preocupação ao se definir os valores de m e n.

O comportamento geral do consumo de memória reservada pelo simulador durante a execução dos experimentos é ilustrado na Figura 5. Portanto, é possível observar que a curva de crescimento do consumo de memória segue um comportamento linear com a entrada de novos dispositivos na rede. Isso acontece porque os participantes da sessão precisam apenas receber o γ computado pelo novo dispositivo. Consequentemente, o *overhead* gerado pelo consumo de memória não é um problema ao se considerar a escalabilidade do esquema de acordo de chaves, já que é proporcional ao número de dispositivos conectados. Essa característica se torna relevante quando é levado em conta os recursos computacionais disponíveis pelos dispositivos, dessa forma é um limitador para o número de participantes da rede com um determinado *hardware*.

A análise de desempenho da geração de chave compartilhada a partir de chaves de conferência verificou que, de forma geral, um método qualquer que tenha como características, a geração de chave compartilhada em uma via com rodadas constantes e $N > 2$ participantes, têm crescimento linear, respeitando sua ordem de complexidade $\mathcal{O}(n)$. Além disso, conclui-se que, o consumo de recursos de *hardware* é baixo, possibilitando a implementação em ambientes de IoT. Entretanto, os resultados apontam que existe a necessidade de atenção ao tempo para sincronismo entre os participantes da rede. A abordagem avaliada considera que os nós participantes são confiáveis, e somente a partir de uma etapa de pré-autenticação é que os membros de um grupo podem realizar a geração e sincronismo da chave compartilhada.

V. Conclusões e Trabalhos Futuros

Este trabalho avalia um esquema para acordo de chaves de conferência para IoT [3] através da simulação de uma rede de dispositivos com um *broker* seguro. Os resultados obtidos acerca do tempo de execução, o impacto do tamanho das chaves e a memória utilizada em relação ao número de

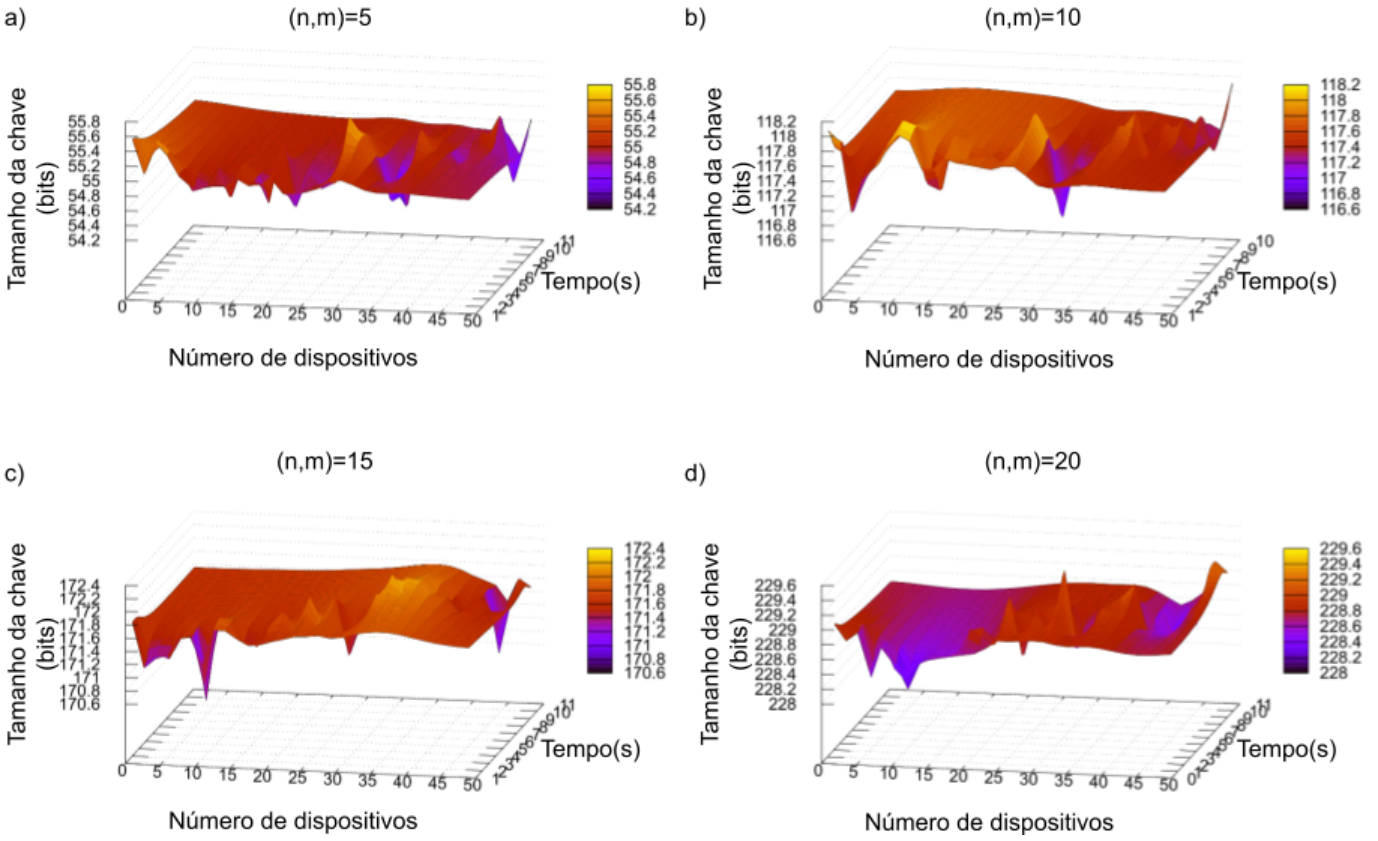

Figura 4. Superfície relacionando o tempo de execução, tamanho das chaves e o número de dispositivos.

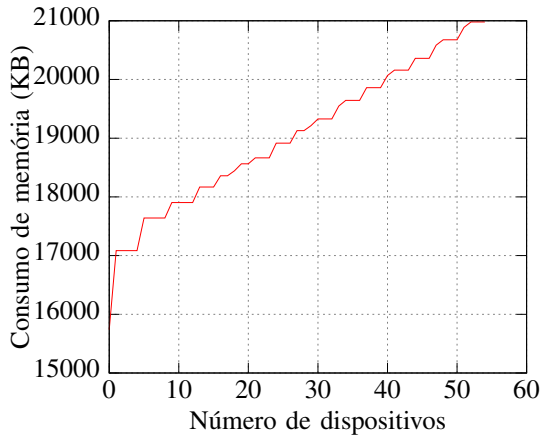

Figura 5. Gráfico de linha do consumo de memória reservada pelo sistema durante a execução dos experimentos

participantes do grupo permite observar que esquemas com as características de geração de chave compartilhada em uma via com rodadas constantes e $N > 2$ participantes, são viáveis em aplicações IoT. Em trabalhos futuros espera-se realizar a comparação entre outros métodos de acordo de chaves existentes. Além disso, espera-se avaliar a adição de múltiplos fatores à autenticação de dispositivos em ambiente IoT.

Referências

[1] K. K. Coelho, M. Nogueira, M. C. Marim, E. F. Silva, A. B. Vieira, and J. A. M. Nacif, "Lorena: Low memory symmetric-key generation method for based on group cryptography protocol applied to the internet of healthcare things," *IEEE Access*, vol. 10, pp. 12 564–12 579, 2022.

[2] K. Coelho, D. Damião, G. Noubir, A. Borges, M. Nogueira, and J. Nacif, "Cryptographic algorithms in wearable communications: An empirical analysis," *IEEE Communications Letters*, vol. 23, pp. 1931–1934, 2019.

[3] L. A. B. Kowada and R. C. Machado, "Esquema de acordo de chaves de conferência baseado em um problema de funçoes quadraticas de duas variáveis," in *Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. SBC, 2017, pp. 126–139.

[4] B. Vaidya, D. Makrakis, and H. Mouftah, "Two-factor mutual authentication with key agreement in wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 2, pp. 171–183, 2016.

[5] K. B. Andrew Banks, Ed Briggs and R. Gupta, "MQTT version 5.0. OASIS standard," 2019. [Online]. Available: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.pdf

[6] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[7] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proceedings of the 3rd ACM conference on Computer and communications security*, 1996.

[8] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1994, pp. 275–286.

[9] H. Xiong, Y. Wu, and Z. Lu, "A survey of group key agreement protocols with constant rounds," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–32, 2019.

[10] P. Tedeschi, S. Sciancalepore, A. Eliyan, and R. Di Pietro, "Like: Lightweight certificateless key agreement for secure iot communications," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 621–638, 2019.

[11] A. Garg and T. Lee, "Secure key agreement for multi-device home iot environment," *Internet of Things*, p. 100249, 2020.