Revista brasileira de iniciação científica
ISSN: 2359-232X

MECANISMO PARA DISTRIBUIÇÃO DE AUTORIZAÇÕES DE SEGURANÇA COM ALTA DISPONIBILIDADE

MECHANISM FOR DISTRIBUTION OF HIGH SECURITY AUTHORIZATIONS AVAILABILITY

MECANISMO DE DISTRIBUCIÓN DE AUTORIZACIONES DE ALTA SEGURIDAD DISPONIBILIDAD

Jean Trindade Garcia[1]
Tiago Antônio Rizzetti[2]

Resumo: Este artigo implementa um mecanismo para propagar autorizações de segurança através de uma rede baseada em *distributed hash table* (DHT). As informações de Autenticação e Autorização (AA) são distribuídas na rede DHT e de posse destas os nós executam localmente o processo de AA. É proposto um modelo de autenticação inicial na rede DHT com o acoplamento de uma infraestrutura de chave pública (ICP). Para comprovação do mecanismo foi desenvolvida uma aplicação na linguagem de programação c++ com as bibliotecas do openDHT e cryptopp. Os testes foram realizados utilizando meios computacionais simulando um ambiente virtual de rede. Foram mensurados os tempos de publicação e obtenção de estruturas de AA distribuídas na rede. Os resultados demonstraram que o mecanismo é escalável, visto que o tempo de obtenção das estruturas de AA não aumentou significativamente mesmo com a entrada de mais nós no sistema. Obtendo, portanto, um sistema seguro, escalável e tolerante a falhas.
Palavras-chave: Autenticação. Autorização. DHT.

Abstract: This article implements a mechanism to propagate security authorizations over a network based on the distributed hash table (DHT). The Authentication and Authorization (AA) information is distributed on the DHT network and in the possession of these the nodes execute the AA process locally. An initial authentication model is proposed in the DHT network with the coupling of a public key infrastructure (ICP). To prove the mechanism, an application was developed in the c ++ programming language with the openDHT and cryptopp libraries. The tests were performed using computational means simulating a virtual network environment. The times of publication and obtaining AA structures distributed in the network were measured. The results demonstrated that the mechanism is scalable, since the time of obtaining the structures of AA did not increase significantly even with the entry of more nodes in the system. Thus, a secure, scalable and fault-tolerant system is in place.
Keywords: Authentication. Authorization. DHT.

1Aluno. Universidade Federal de Santa Maria. jeangarcia@redes.ufsm.br
2Professor. Universidade Federal de Santa Maria. rizzetti@ctism.ufsm.br

Revista brasileira de iniciação científica
ISSN: 2359-232X

Resumen: Este artículo implementa un mecanismo para propagar las autorizaciones de seguridad en una red basada en la tabla hash distribuida (DHT). La información de Autenticación y Autorización (AA) se distribuye en la red de DHT y, en posesión de estos, los nodos ejecutan el proceso de AA localmente. Se propone un modelo de autenticación inicial en la red DHT con el acoplamiento de una infraestructura de clave pública (ICP). Para probar el mecanismo, se desarrolló una aplicación en el lenguaje de programación c ++ con las bibliotecas openDHT y cryptopp. Las pruebas se realizaron utilizando medios computacionales que simulan un entorno de red virtual. Se midieron los tiempos de publicación y obtención de las estructuras AA distribuidas en la red. Los resultados demostraron que el mecanismo es escalable, ya que el tiempo de obtención de las estructuras de AA no aumentó significativamente incluso con la entrada de más nodos en el sistema. Por lo tanto, existe un sistema seguro, escalable y tolerante a fallos.
Palabras-clave: Autenticación. Autorización. DHT.

Envio: 20/04/2019 **Revisão: 22/04/2019** **Aceite: 05/07/2019**

Revista brasileira de iniciação científica
ISSN: 2359-232X

Introdução

Os sistemas computacionais atuais exigem cada vez mais segurança com alta disponibilidade (NAGARAJAN; VARADHARAJAN; TARR, 2014) como sistemas de comércio eletrônico, sistemas para controle de acesso, entre outros. Nesse contexto, os sistemas distribuídos alteraram significativamente a maneira como as empresas e indivíduos armazenam e processam informações (NAGARAJAN; VARADHARAJAN; TARR, 2014). As questões de segurança como autenticação e autorização, desempenham um papel vital nesse contexto. No que se refere a autenticação, existem várias técnicas. Neste trabalho é realizada a autenticação utilizando certificados digitais para comprovação da identidade dos nós na rede. Os certificados são distribuídos e homologados pela infraestrutura de chave pública (ICP).

Dentro da ICP existe uma autoridade de certificação que utiliza a criptografia de chave pública para homologar a identidade de uma entidade com a sua chave pública gerando um certificado digital assinado (MENKE, 2003). Neste trabalho é utilizada uma estrutura de dados com informações de segurança para sumarizar autorizações de segurança, sendo esta distribuída a todos os nós da rede, permitindo que o processo de autenticação ocorra localmente.

Tendo em vista a alta disponibilidade do mecanismo, é utilizada uma rede DHT, visto que são resilientes tolerantes a falhas, descentralizadas e operam com códigos de hash para rotear mensagens na rede (AVRAMIDIS et al., 2012). Cada nó mantém uma estrutura de tabela de hash similar ao roteamento. A rede DHT possui duas funções principais obter e colocar uma informação na rede através da operação de *lookup(k)* que retorna os dados associados a chave k. Dessa forma, este trabalho tem como objetivo principal implementar um mecanismo que propague autorizações de segurança com alta disponibilidade através de uma rede DHT. Realizando autenticação inicial entre nós para garantir que apenas nós autênticos participem do sistema. Além disso, testar o desempenho do mecanismo, no que diz respeito a velocidade de propagação de estruturas de Autenticação e Autorização na rede DHT.

Revista brasileira de iniciação científica
ISSN: 2359-232X

Metodologia

Em uma rede DHT um nó para ingressar na rede deve contatar outro nó já inserido na rede, chamado de nó de bootstrap. A figura 1 ilustra a troca e validação dos certificados no processo inicial de autenticação. O processo é feito mutuamente verificando a assinatura da autoridade de certificação e ainda se o certificado não foi revogado. Todas as mensagens entre os nós, são verificadas através de um desafio aleatório (Nonce). Se ambos os certificados forem autênticos o nó ingressa na rede DHT. Para distribuir as estruturas de segurança na rede o nó responsável assina com a sua chave privada o pacote que contém as informações e publica-o na rede DHT. O nó que desejar obter a base de informações para AA da rede verificará a assinatura do pacote com a chave pública do emissor, com o intuito de garantir que é uma informação da rede autêntica.

Os testes foram realizados no emulador de redes CoreEmulator que possibilita a simulação de redes reais em um ambiente virtual. Os testes foram realizados na mesma máquina local com processador core I3 com 8 gigabytes de memória RAM e rodando um sistema operacional linux mint na versão 19 de 64 bits. Foi possível executar até 80 nós simultaneamente. Para colocar a rede DHT em funcionamento foi utilizado a biblioteca do openDHT. A biblioteca da Cryptopp foi utilizada para assinatura das mensagens e dos certificados digitais. Desse modo quando um nó publicar um pacote contendo a estrutura de dados de autenticação, os nós participantes da rede recebem esse pacote através da estrutura da rede DHT.

Com isso, é possível mensurar o tempo inicial de publicação e o tempo final de recebimento da base para AA. O tempo obtido é um número do tipo *double* que contém o total de milissegundos desde a época do sistema operacional. De posse do tempo obtido em milissegundos do relógio do sistema, os nós, então, inserem esses tempos em um banco de dados indexado construído através da biblioteca sqlite3. Após os dados estarem no banco é calculado o tempo, subtraindo o maior tempo final do tempo inicial. Foram executados quatro testes cada um contendo um conjunto de nós, vinte nós, quarenta nós, sessenta nós e oitenta nós. Em cada teste foram realizadas vinte rodadas e mensurado a média de tempo dessas rodadas. Em relação à emissão de certificados o nó ao ser executado já possui um certificado emitido por uma ICP configurada previamente. A lista de revogação de certificados foi publicada na mesma máquina local.

Revista brasileira de iniciação científica
ISSN: 2359-232X

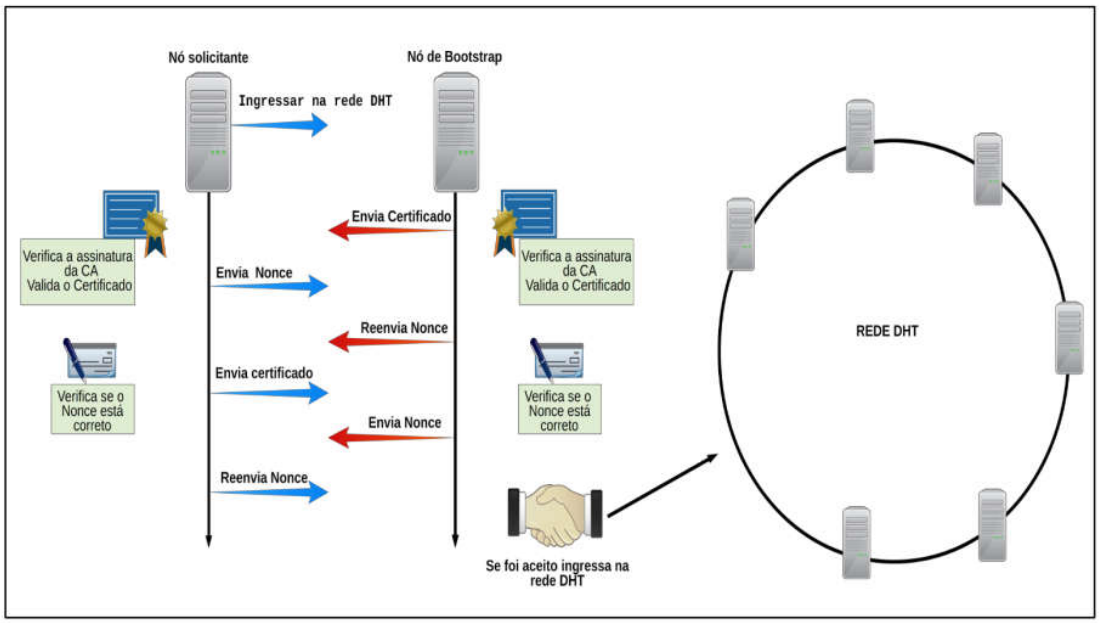

Figura 1 – Modelo de autenticação inicial na rede DHT.

Resultados

Nesta seção serão descritos os resultados obtidos no trabalho, contrapondo-os com um trabalho relacionado proposto por (NAGARAJAN; VARADHARAJAN; TARR, 2014). O trabalho visa aprimorar o design e a aplicação de políticas e mecanismos para controle de acesso, em ambientes distribuídos. Além disso, a ideia principal é permitir que as partes presentes no sistema se comuniquem e classifiquem umas às outras com resultados obtidos de transações realizadas. Cada transação entre as partes, é criada uma pontuação de confiança, esta última será usada para transações futuras. No sistema, segundo (NAGARAJAN; VARADHARAJAN; TARR, 2014) o tempo para que os nós possam verificar a confiança de uma parte com 20 componentes é cerca de 3 segundos, com 30 componentes no sistema o tempo aproximado foi de 6 segundos. O gráfico de resultado do trabalho de (NAGARAJAN; VARADHARAJAN; TARR, 2014) pode ser visualizado na figura 2.

Revista brasileira de iniciação científica
ISSN: 2359-232X

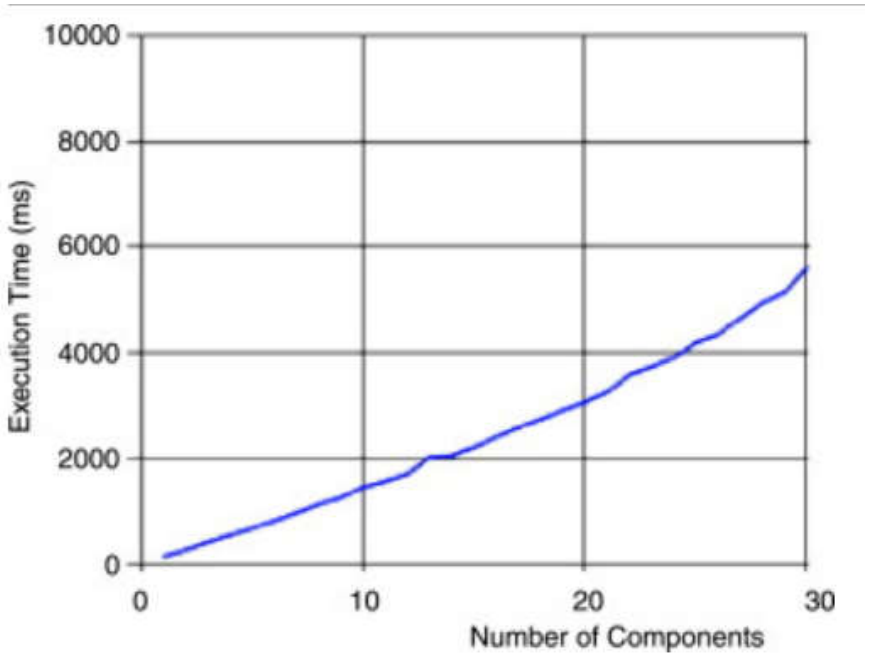

Figura 2 – Resultados obtidos no trabalho relacionado.
Fonte: (NAGARAJAN; VARADHARAJAN; TARR, 2014)

Os resultados obtidos no presente trabalho representados na figura 3, melhoram de forma significativa a abordagem de controle de acesso em ambientes distribuídos, com 20 nós sendo executados no openDHT, o tempo de recebimento da estrutura de controle de autenticação foi de 18 milissegundos. No conjunto de 40 nós o tempo total de recebimento da estrutura de dados de autenticação por todos os nós, foi de 21 milissegundos. Com 60 nós o tempo foi de 23 milissegundos, e com oitenta nós em execução no sistema o tempo foi de 25 milissegundos. Pode-se perceber que o mecanismo é escalável, visto que o ingresso de mais nós no sistema, não aumentou significativamente o tempo de propagação da estrutura de controle AA na rede DHT. A autenticação inicial proposta na rede DHT garante que apenas nós que possuem um certificado válido participem do sistema.

Revista brasileira de iniciação científica
ISSN: 2359-232X

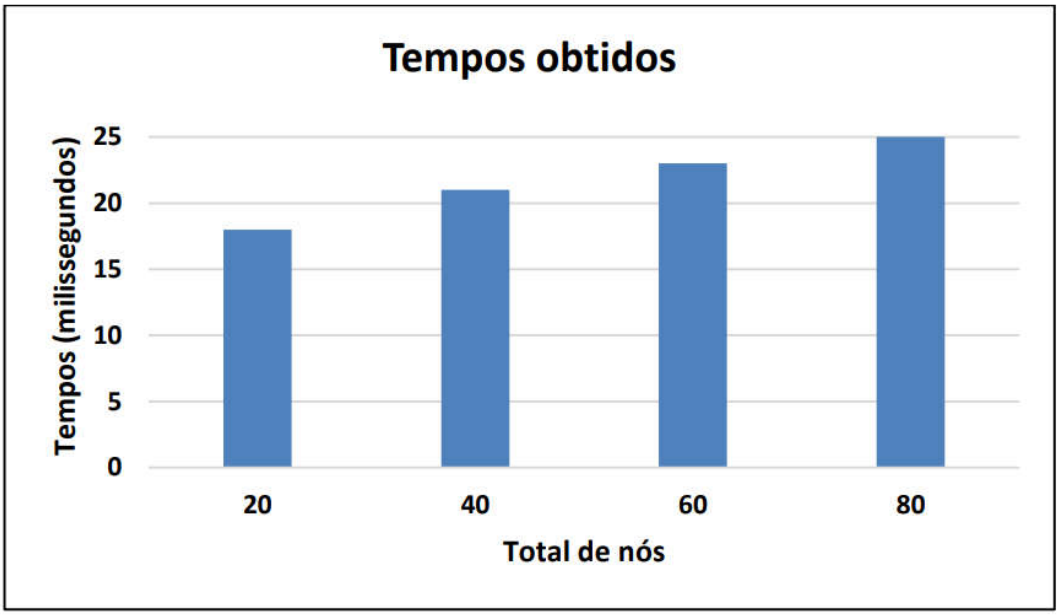

Figura 3 – Resultados obtidos da velocidade de propagação da base de AA.

Conclusão

A vida real e digital convergem para criar uma sociedade inteligente, onde diversas áreas estão sendo afetadas pela tecnologia, como energia, transporte, comércio, etc. Neste contexto, a segurança é primordial. Ela desempenha um papel crucial na preservação de dados de indivíduos e empresas. Além de garantir que esses sistemas continuem oferecendo seus serviços. O sucesso ou fracasso dessa sociedade inteligente dependerá de dois aspectos: segurança e privacidade. Principalmente por uma política de segurança que determine quem tem acesso a quê, e em que condições (OUADDAH et al., 2015).

Diante disso, vulnerabilidades têm sido exploradas atualmente, com técnicas inovadoras de ataques cibernéticos. Como por exemplo os ataques chamados de “Sybils” onde basicamente é criado um grande número de nós falsos e não autênticos na rede, esses nós falsos podem assumir o controle da rede (CHOLEZ et al, 2010). Diante disso, sistemas de segurança são fundamentais e devem possuir alta disponibilidade. Tais sistemas devem possuir mecanismos proativos e reativos. Capazes de mitigar ataques e se proteger deles. Ataques a sistemas de controle de acesso podem trazer consequências irreparáveis ao sistema.

Revista brasileira de iniciação científica
ISSN: 2359-232X

O elemento malicioso uma vez tendo sido autorizado a utilizar o sistema pode realizar diversas alterações indesejadas. Sistemas de controle de acesso, baseados em uma entidade centralizada como uma base LDAP (*Lightweight Directory Access Protocol*) possuem a desvantagem da dependência do servidor central, se este servidor parar de funcionar todo o sistema ficará comprometido.

Em vista disso, uma alternativa é investir em serviços distribuídos para manter redundância do sistema. Redes DHT tem se tornado uma alternativa muito promissora neste sentido. São escaláveis, resilientes, tolerantes a falhas, e asseguram a disponibilidade da rede mesmo com a presença de falhas de até $n - 1$ nós. Além disso, sistemas de controle de acesso devem possuir um desempenho satisfatório no momento de verificar se um elemento possui autorização. A base de AA distribuída possui alto desempenho neste sentido, e podem ser utilizados para sumarizar autorizações de segurança. A solução proposta neste trabalho une as características desejáveis de uma rede DHT, como mecanismo de propagação de informações de autenticação e autorização executadas localmente em cada dispositivo.

Neste sentido, oferece um mecanismo refinado de alto desempenho que poderá ser utilizado para empregar sistemas de controle de acesso com alta disponibilidade. Com base nos resultados obtidos, o mecanismo mostrou um desempenho superior na propagação de estruturas de controle em relação ao trabalho relacionado, no que se refere a persistência de estruturas de controle de acesso e autenticação. Este desempenho é comprovado pela escalabilidade da rede DHT. Em trabalhos futuros espera-se o aperfeiçoamento desta aplicação, inserindo técnicas de rastreabilidade. Dessa forma, as principais contribuições deste trabalho foram a autenticação inicial na rede DHT. Oferecer uma rede segura, para impedir que entidades maliciosas participem do sistema. Além disso, disponibilizar a possibilidade de os nós na rede realizarem as rotinas de controle de acesso localmente. Por conseguinte, realizar essas tarefas com eficiência e escalabilidade sem a necessidade de contato constante com uma entidade centralizada.

Revista brasileira de iniciação científica
ISSN: 2359-232X

Referências

NAGARAJAN, A.; VARADHARAJAN, V.; TARR, N. **Trust enhanced distributed authorisation for web services**. Journal of Computer and System Sciences, v. 80, n. 5, p. 916 – 934, 2014. ISSN 0022-0000. Special Issue on Dependable and Secure Computing. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0022000014000142>. Acesso em: 14 fevereiro de 2019.

MENKE, F. **Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a icp alemã**. Revista de Direito do Consumidor, v. 12, n. 48, 2003.

AVRAMIDIS, A. et al. Chord-pki: **A distributed trust infrastructure based on p2p networks. Computer Networks**, v. 56, n. 1, p. 378 – 398, 2012. ISSN 1389-1286. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1389128611003574>. Acesso em: 14 fevereiro de 2019.

A. Ouaddah, I. Bouij-Pasquier, A. Abou Elkalam and A. Ait Ouahman, **"Security analysis and proposal of new access control model in the Internet of Thing".** International Conference on Electrical and Information Technologies (ICEIT), Marrakech, 2015, pp. 30-35.

T. Cholez, I. Chrisment and O. Festor, **Efficient DHT attack mitigation through peers' ID distribution**. *2010 IEEE International Symposium on Parallel & Distributed Processing, Workshops and Phd Forum (IPDPSW)*, Atlanta, GA, 2010, pp. 1-8. doi: 10.1109/IPDPSW.2010.5470928