Uma Arquitetura para Comunicação Espontânea e Segura para Internet das Coisas Móveis em Cidades Inteligentes*

Gabriel Peres Leopoldino, Ricardo Couto Antunes da Rocha

[1]Departamento de Ciência da Computação – Instituto de Biotecnologia
Universidade Federal de Goiás - Regional Catalão
Catalão – GO – Brasil

gabrielperes97@gmail.com, rcarocha@acm.org

Abstract. *A Smart City comprehends solutions that explore data dissemination to improve citizens' quality of life, based on integration of Internet of Things and software services. Software architectures for smart cities must provide security mechanisms to prevent malicious agents from exploring a city infrastructure to intercept user data or to provoke application misbehavior.This paper presents a secure communication architecture for Internet of Mobile Things in Smart Cities based on a public key infrastructure, which provides services for authentication, confidentiality, and integrity, so as it enables various scenarios for spontaneous connectivity. The proposed work considers that IoT devices connect to the infrastructure that permeates a smart city through the mediation of devices with more processing power and connectivity, such as smartphones.*

Resumo. *Uma Cidade Inteligente compreende soluções que integram Internet das Coisas e serviços de software para permitir a construção de aplicações que explorem a disseminação de informações para melhorar a qualidade de vida da população. Neste cenário, arquiteturas de software devem permitir que dispositivos de IoT se conectem à infraestrutura de software que permeia uma Cidade Inteligente de maneira espontânea e mediada por dispositivos de maior poder computacional, como smartphones. Em contrapartida, tais arquiteturas devem prover serviços de segurança para impedir de agentes maliciosos explorem a infraestrutura e afetem o correto funcionamento das suas aplicações. Este trabalho apresenta uma arquitetura de comunicação segura para Internet das Coisas Móveis em cidades inteligentes baseada em uma infraestrutura de chaves públicas, que provê serviços de autenticação, confidencialidade e integridade das informações consumidas e publicadas por dispositivos e que são adequadas a diversos cenários de conectividade.*

1. Introdução

O conceito de Cidade Inteligente engloba soluções computacionais para a integração de serviços de software e aplicações no escopo de uma cidade ou metrópole para prover serviços que aumentem a qualidade de vida dos cidadãos. Tipicamente, cenários de cidades inteligentes exploram amplamente a coleta e disseminação de dados, como

*Esta pesquisa foi desenvolvida no contexto dos projetos UC-SPACE (FAPEG/FAPs/INRIA/INS2i-CNRS 09/2014) e do INCT de Internet Futura para Cidades Inteligentes (Proc. CNPq 65446/2014-0), e como Iniciação Científica PIBIC e trabalho de conclusão de curso do autor Gabriel Peres Leopoldino.

localização, para permitir que serviços aos cidadãos, como transporte público e tráfego urbano, sejam melhor planejados e geridos por meio de sistemas computacionais.

Diversos experimentos envolvendo universidades e iniciativa privada têm contribuído para o conceito de cidades inteligentes em escala real. Por exemplo, o *SmartSantander* [Sanchez et al. 2014] é um projeto da União Europeia envolvendo a implantação de 20.000 sensores para desenvolver uma cidade inteligente. O *SmartSantander* tem o objetivo de ser uma plataforma experimental de testes de arquitetura, protocolos, serviços e aceitação social de uma cidade inteligente à nível de cidade global. Como infraestrutura de comunicação entre os sensores, atuadores e os serviços da cidade, uma cidade inteligente explora o conceito de Internet das Coisas.

No Brasil, projetos de pesquisa como o *ContextNet* [David et al. 2013] oferecem uma arquitetura para Internet das Coisas e Cidades Inteligentes, provendo uma infraestrutura para disseminação de informações usando o paradigma *publish/subscribe*, além de permitir o gerenciamento de mobilidade e a descoberta espontânea de dispositivos.

A segurança da informação na Internet das Coisas é um requisito fundamental para uma plena implementação de uma cidade inteligente. Aplicações como controle de tráfego, que tenham seus dados manipulados por algum agente malicioso, podem levar a um caos no trânsito, podendo causar vários acidentes. Como exemplo de exploração maliciosa de sistemas de controlam cidades, inclui-se o acionamento noturno de todas as sirenes de emergência da cidade de Dallas[1] e o uso de câmeras de segurança conectadas à Internet para realização de ataques de negação de serviço[2]. As arquiteturas acima mencionadas não implementam primitivas adequadas para a segurança destas informações e flexíveis aos diferentes cenários de segurança das aplicações de uma cidade.

Este artigo descreve uma arquitetura para comunicação espontânea e segura para a Internet das Coisas Móveis no contexto de Cidades Inteligentes, que ofereça além das primitivas fundamentais para descoberta de dispositivos e gerenciamento de mobilidade, primitivas para autenticação, confidencialidade e integridade da comunicação. A arquitetura proposta foi implementada como uma camada de comunicação adicional sobre os protocolos do *ContextNet.*

Este artigo está estruturado da seguinte forma. A seção 2 descreve o cenário da Internet das Coisas Móveis aplicado ao contexto de Cidades Inteligentes, o qual se baseia este trabalho e descreve as principais ameaças de segurança. Na seção 3 descrevemos trabalhos relacionados à segurança para Internet das Coisas. A seção 4 descreve o *middleware* de referência para comunicação em cenários de Internet das Coisas móveis. A seção 5 descreve a arquitetura proposta para comunicação segura em Cidades Inteligentes enquanto que a seção 6 descreve a implementação da arquitetura. Por fim, um resumo das contribuições deste artigo é apresentado na seção 7.

2. Comunicação Oportunista em Internet das Coisas Móveis

No modelo de sistema para Internet das Coisas Móveis (IoMT), objetos inteligentes (fixos ou móveis) se conectam à Internet por meio de um *gateway* móvel [Endler et al. 2017], por meio de uma tecnologia de comunicação sem fio de curto alcance, como *Bluetooth*

[1]http://edition.cnn.com/2017/04/08/us/dallas-alarm-hack/index.html

[2]http://money.cnn.com/2016/10/22/technology/cyberattack-dyn-ddos/index.html

e NFC. Além de intermediarem a comunicação, os gateways enriquecem as informações publicadas pelos objetos inteligentes, anexando informações contextuais da comunicação e do gateway, como localização, com as quais é possível desenvolver aplicações que explorem a percepção de que objetos inteligentes e gateways são um único dispositivo. Devido à sua profusão e poder de conectividade, *smartphones* são candidatos ideais para assumir o papel de gateways em IoMT.

Como objetos inteligentes tipicamente fazem parte do ambiente, enquanto smartphones-como-gateways são intrinsecamente móveis, uma plataforma de IoMT deve permitir que a comunicação entre objetos inteligentes e gateways se dê de forma oportunista, quanto um smartphone encontra-se na área de conectividade de um objeto e está configurado para fazer papel de gateway para todos os dispositivos ou um conjunto que atenda a certa política.

Por exemplo, considere diversos dispositivos disponíveis em um ônibus inteligente, como câmeras de segurança internas, câmeras direcionadas para área externa (captando o tráfego e eventos na cidade), acelerômetros nos eixos do veículo (captando imperfeições nas vias, por exemplo) e botões físicos de pânico. Esses dispositivos podem publicar os dados sensoriados ou pré-processados, explorando oportunisticamente a conectividade disponível por gateways IoMT que poderiam ser tanto smartphones de usuários como gateways estáticos disponíveis na cidade, como em pontos de ônibus inteligentes. As informações publicadas acrescidas do contexto do respectivo gateway, permitem a sua geolocalização e o desenvolvimento de aplicações de gerenciamento de trânsito da cidade, por exemplo. Além disso, no caso de um smartphone-como-gateway, um usuário pode explorá-las em suas próprias aplicações, como redes sociais e mapas de navegação.

Entretanto, neste cenário um ator malicioso pode produzir três ameaças à infraestrutura da cidade inteligentes e seus usuários: (A1) falsificar as informações de contexto anexadas às mensagens enviada por um gateway malicioso, (A2) interceptação e manipulação das mensagens entre objetos inteligentes e gateways, e (A3) falsificação de mensagens de objetos inteligentes.

Um smartphone-como-gateway pode ser oferecido por qualquer pessoa que deseja contribuir com o sistema através de seu próprio smartphone. Por isso, dependendo da aplicação e multiplicidade da oferta da informação, uma aplicação pode considerar as informações contextuais como não confiáveis, visto que podem ser forjadas por um usuário malicioso (A1). Seu impacto depende do contexto do uso destes dados: enquanto que uma aplicação pode fazer o uso da localização para controlar todo o tráfego de uma cidade e serviços de emergência, e por isso exige que apenas sensores confiáveis e previamente conhecidos sejam usados, em outras aplicações o uso pode ser menos crítico, podendo lidar com imprecisões ou mesmo inconsistências entre diversas fontes.

A ameaça A2 considera que um agente malicioso poderia interceptar a conexão entre um *gateway* e um objeto inteligente. Considerando que o *gateway* opera de forma espontânea, sem a necessidade de qualquer intervenção do usuário para descoberta de dispositivos podemos considerar que tanto os dados de um objeto inteligente quanto os dados enviados pelo *gateway* para o objeto inteligente podem ser forjados. No cenário mencionado, um atacante poderia utilizar um objeto inteligente simulando um ônibus,

enviando mensagens de que o mesmo está parado em algum lugar ou mudou de trajeto, ou ainda enviando mensagens falsas ao display no ponto de ônibus utilizando um *gateway* malicioso, prejudicando assim os usuários que confiam neste sistema.

A comunicação entre um *gateway* e uma aplicação na nuvem acontece dentro da Internet, o que aumenta a possibilidade dessa comunicação ser interceptada e manipulada, como acontece em A3. A comunicação com a aplicação poderia ser interceptada para receber dados enviados por *gateways*, ou ainda um atacante poderia enviar mensagens à aplicação como se fosse um *gateway*, inserindo informações falsas a rede ou manipulando atuadores e aplicações, de forma mais fácil que falsificando um objeto inteligente.

3. Trabalhos Correlatos

O trabalho de Mahmoud *et al.* [Mahmoud et al. 2015] apresenta uma visão geral dos princípios e desafios de segurança, desafios tecnológicos e contramedidas propostas para a segurança na Internet das Coisas, como medidas para autenticação, estabelecimento de confiança, arquitetura federada e a conscientização da segurança com seus usuários humanos.

Han e Kim [Han and Kim 2017] apresentam um protocolo leve de autenticação mútua e troca de chaves de sessão utilizando cifras de blocos e criptografia simétrica e chaves pré-compartilhadas. Seu modelo garante autenticação, confidencialidade e integridade dos dados, podendo ser aplicado em A1, na autenticação entre um *gateway* e um objeto inteligente, mas, levando em conta o caráter promíscuo de um *gateway*, a existência de uma chave pré compartilhada entre eles limitaria o número de *gateways* no qual um objeto inteligente poderia utilizar para enviar seus dados, isto em um cenário aonde apenas *gateways* confiáveis teriam esta chave.

Diro *et al* [Diro et al. 2018] especificam uma arquitetura para comunicação segura entre uma névoa (*fog*) e um objeto inteligente utilizando um modelo de re-encriptação em *proxy* baseado em criptografia de curvas elípticas. Este modelo permite uma comunicação segura fim-a-fim em uma arquitetura baseada em computação na névoa, neste modelo um objeto inteligente delega o envio de uma mensagem à um intermediário, de forma criptografada, este intermediário reencripta a mensagem, sem descriptografá-la, e a reencaminha, somente seu destinatário consegue descriptografá-la completamente. Um objeto inteligente pode delegar a tarefa do envio à um intermediário, mas este intermediário não pode delegar esta tarefa. Este modelo trataria parcialmente as ameaças A1, A2 e A3, mas esta arquitetura assume a premissa de que a névoa é confiável o suficiente para armazenar as identidades dos objetos inteligentes, como em um *gateway*. O trabalho não considera o caso em que o *gateway* também pode ser falsificado e nem o estabelecimento espontâneo e oportunista da comunicação.

Endler *et al.* [Endler et al. 2017] apresenta uma arquitetura de segurança para a Internet das Coisas Móveis também se baseando no *middleware ContextNet* e no *MobileHub*. A arquitetura provê medidas para mitigar as ameaças A2 e A3, mas para isso mantém na nuvem um banco de dados com as identidades de cada Objeto Inteligente, sendo consultado durante cada conexão, o que impacta a escalabilidade em um cenário com um grande número de dispositivos, como em uma Cidade Inteligente.

4. Arquitetura de Comunicação do ContextNet

O *middleware ContextNet* [David et al. 2013] oferece serviços de contexto para aplicações colaborativas de larga e grande escala, como monitoramento ou coordenação em linha de atividades de entidades móveis, como smartphones, veículos ou robôs. A Figura mostra a arquitetura do middleware para permitir a comunicação de dispositivos da IoMT.

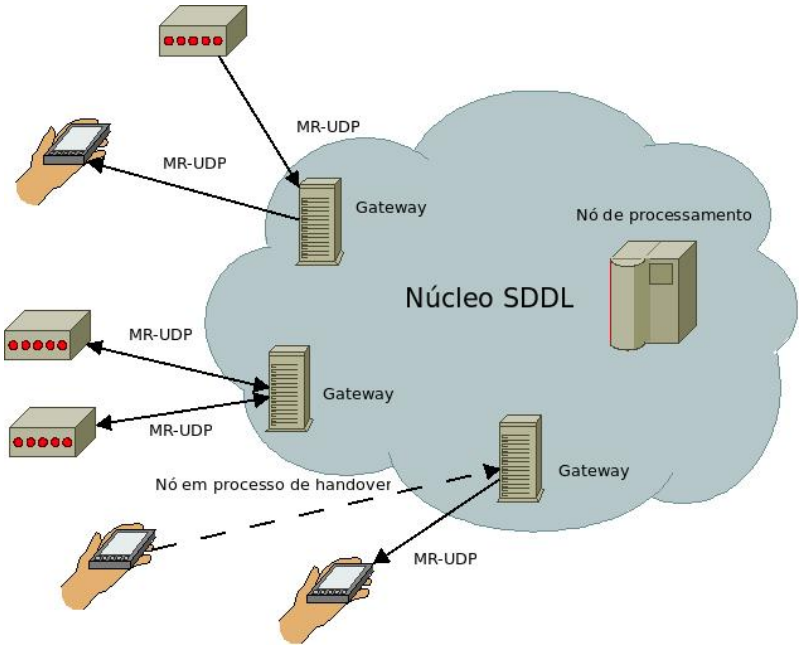

Figura 1. Arquitetura do Middleware ContextNet

O SDDL (*Scalable Data Distribution Layer*) [David et al. 2013] implementa a camada de comunicação do *ContextNet* e é baseada no protocolo DDS para publish/subscribe em tempo real [Foundation 2019]. A infraestrutura permite a comunicação entre nós móveis e nós estacionários em um nuvem ou *cluster*, baseado no paradigma *publish/subscribe*. Os nós estacionários podem executar servidores de aplicação para coletar dados ou controlar atuadores, através de mensagens sobre um nó móvel individual ou um grupo de nós móveis. A comunicação entre os nós móveis e os nós estacionários ao SDDL é mantida através de um protocolo chamado MR-UDP. O *Mobile Reliable UDP* [Nery e Silva et al. 2013] é um protocolo que gerencia a mobilidade entre nós móveis, mantendo a baixa sobrecarga do UDP e provendo o serviço de confiabilidade, o qual não é provido pelo UDP. O MR-UDP mantém uma conexão mesmo que seu cliente mude seu endereço de redes, permitindo uma conexão confiável em comunicações oportunistas.

O *Mobile-Hub* [Talavera et al. 2015] é um serviço de *middleware* responsável por descobrir e oportunamente conectar dispositivos com pouco poder computacional e com tecnologias de comunicação de baixo alcance (como o *Bluetooth*) ao SDDL. Dispositivos com tais características tipicamente são utilizados na Internet das Coisas como sensores e atuadores. O *Mobile-Hub* oferece serviços para localização física aproximada de um objeto inteligente baseado em vizinhança. Em outras palavras, o *Mobile-Hub* funciona como um *proxy* móvel, coletando oportunamente mensagens, anexando informações

contextuais e encaminhando-as ao SDDL tornando-se um intermediário de comunicação oportunista entre o SDDL e os objetos inteligentes.

O *ContextNet* junto ao *Mobile-Hub* implementam uma solução para a Internet das Coisas Móveis, onde os nós estacionários pertencentes ao SDDL fazem o papel de nuvem e o *Mobile-Hub* realiza a função de *gateway* aos Objetos Inteligentes.

Apesar de oferecer primitivas para comunicação móvel e oportunista, o *ContextNet* não oferece primitivas para segurança dos dados trafegados em sua plataforma, o que é dificultado com a entrada e saída espontânea e dinâmica de dispositivos, como sensores. Esse dinamismo da comunicação, embora necessário, abre portas para comportamentos maliciosos, previamente discutidos na Seção 2.

5. Arquitetura Segura para Internet das Coisas em Cidades Inteligentes

Para oferecer uma arquitetura de comunicação espontânea em IoMT que considere as ameaças de segurança discutidas na seção 2, desenvolvemos quatro cenários de comunicação espontânea, com diferentes requisitos de segurança e ilustrados na Figura 2, considerando a implementação de aplicações para cidades inteligentes.

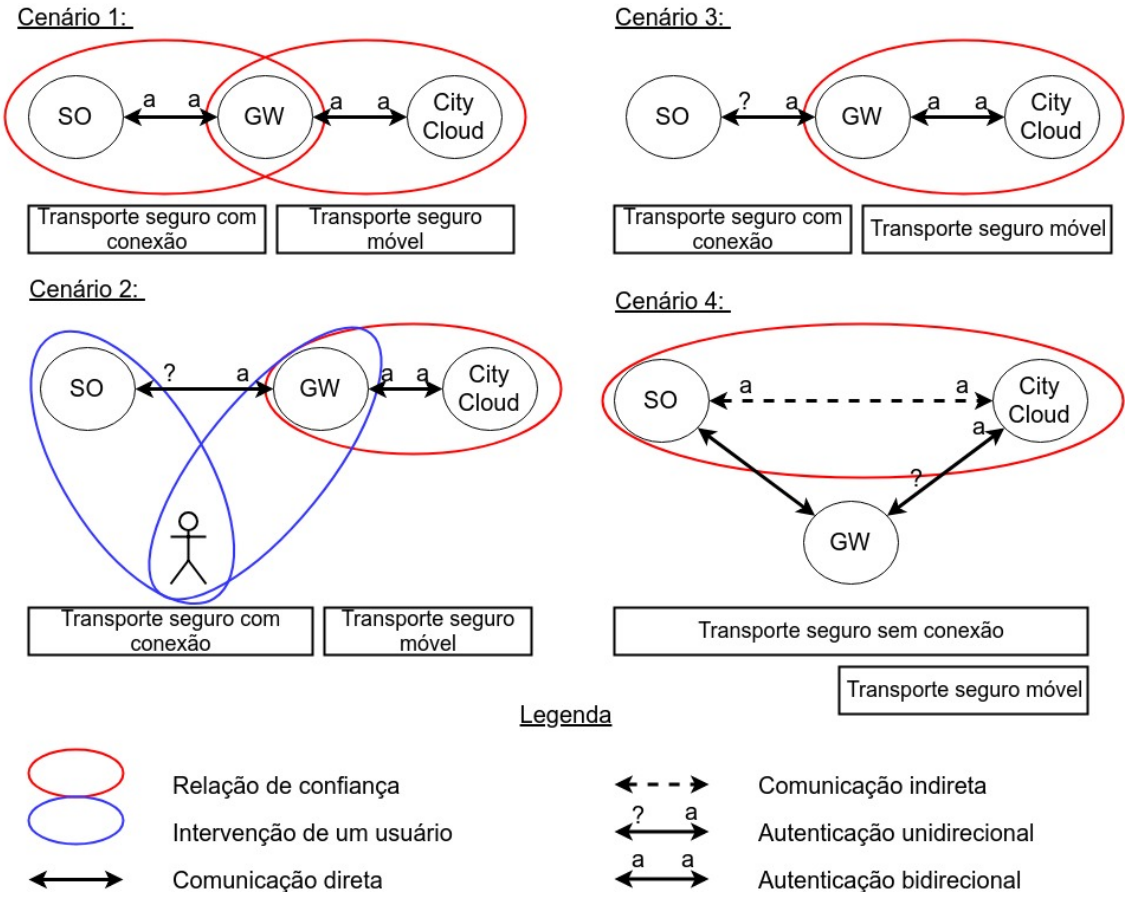

Figura 2. Cenários de Comunicação Espontânea

5.1. Cenário 1: Gateway dedicado

Alguns Objetos Inteligentes pertencentes a infraestrutura da cidade como semáforos, sirenes e radares, necessitam de uma conexão com maior disponibilidade, além de uma

segurança mais rígida. Para isso, estes Objetos Inteligentes precisam de um *gateway* dedicado à eles. Este *gateway* manteria informações sobre identidade dos Objetos Inteligentes autorizados à utilizá-lo e apenas aceitaria conexão destes. Estes Objetos Inteligentes pertencentes a infraestrutura da cidade contém sua própria identidade assinada pela infraestrutura da cidade, a partir disso, toda mensagem enviada por ele pode ser auto assinada garantindo sua integridade. Os *gateways* que se comunicam com estes Objetos Inteligentes certificados também possuem sua própria identidade, e todas as mensagens enviadas por ele também são assinadas por ele.

5.2. Cenário 2: Confiança baseada no usuário

Aplicações podem utilizar Objetos Inteligentes para interagir com usuários através de seus *smartphones*, sob intervenção direta do usuário, por meio de políticas de segurança. Como por exemplo em uma aplicação de painel eletrônico em um ponto de ônibus que mostra informações aos usuários. O painel inteligente tenta utilizar o *gateway* do usuário para transmitir os dados, aonde, dependendo da política de segurança escolhida qualquer objeto pode se conectar, ou o usuário deve escolher entre aceitar ou recusar a conexão com aquele Objeto Inteligente. Assim, a confiança nos Objetos Inteligentes é gerenciada pelo usuário na confiança física dos dispositivos aos quais ele permite conectar às suas interfaces. Neste esquema o usuário tem uma identidade registrada junto a infraestrutura, logo seu *gateway* assinará as mensagens com esta assinatura, identificando qual usuário coletou estes dados.

5.3. Cenário 3: Objeto inteligente anônimo

Aplicações para *crowdsourcing* podem coletar informações voluntárias sobre trânsito a partir de dispositivos de usuários, como GPS de carros, para isso devemos preservar a identidade destes usuários e considera-los como anônimos. *Gateways* confiáveis pela infraestrutura da cidade podem ser instalados em locais estratégicos para coletar estes dados e ainda assim ter uma confiança sobre sua localização. Neste caso os dados enviados pelos Objetos Inteligentes não são assinados, mas o *gateway* pode ainda inserir metadados com sua localização e assiná-los, garantindo que aquele *gateway* confiável, naquela localização capturou estes dados.

5.4. Cenário 4: Gateway SO-nuvem anônimo

Algumas aplicações podem utilizar sensores espalhados pela cidade, como sensores de poluição do ar, ou de rios, onde não é viável uma infraestrutura pré-definida para disseminação de seus dados, como no caso 1, mas ainda manter sua segurança e confiabilidade. Neste esquema temos Objetos Inteligentes com identidade reconhecida pela infraestrutura da cidade *gateways* móveis pertencentes aos cidadãos na cidade. Quando um Objeto Inteligente encontra algum *gateway* móvel disponível ele usa de encriptação fim-a-fim entre o Objeto Inteligente e a infraestrutura da cidade, usando o *gateway* como ponte, para enviar estes dados de forma segura. Este esquema pode ser utilizado também como backup para o caso 1, quando por algum motivo seu *gateway* dedicado estiver indisponível.

6. Implementação

Como resultado dessa pesquisa, foram desenvolvidos serviços adicionais ao middleware ContextNet que permitem implementar cada um dos quatros cenários discutidos na seção

anterior. A implementação dos cenários e da arquitetura proposta envolveu o desenvolvimento de um protocolo de transporte móvel seguro, como uma extensão do protocolo MR-UDP do *ContextNet* e inclusão da camada de segurança via DTLS, e da integração aos mecanismos de autenticação de chave pública com uma infraestrutura de chaves representativa para os cenários e escalável.

6.1. SMR-UDP

Para proteger a comunicação entre um *Mobile-Hub* e o SDDL e mitigar a ameaça A3 desenvolvemos um protocolo que combina o uso do MR-UDP com o *Datagram Transport Layer Security* (DTLS) [Rescorla and Modadugu 2012], um protocolo de comunicação segura que provê autenticação e confidencialidade, além de outros serviços à camada de transporte. O protocolo desenvolvido é chamado SMR-UDP (*Secure, Mobile and Reliable UDP*) e oferece um canal seguro de comunicação por meio do uso de MR-UDP sobre DTLS.

A comunicação pelo SMR-UDP ocorre em duas fases. Na primeira fase, o protocolo realiza o *handshake* seguro do DTLS, explorando a autenticação do protocolos para implementação a autenticação entre *Mobile-Hub* e objeto inteligente. Na segunda fase, o SMR-UDP entra em efetiva conversação, trocando dados de forma segura através da rede. As garantias de mobilidade, ordenação e retransmissão de pacotes se mantém pelo MR-UDP no topo da pilha. Com isso todos os pacotes do MR-UDP, incluindo os pacotes que informam a troca de endereço IP, são enviados de forma segura.

Para realizar a autenticação adequada a cada cenário, cada *Mobile-Hub* e cada nó estacionário SDDL possui um certificado digital, assinado por uma Autoridade Certificadora dentro do *ContextNet*. A falta de garantia de entrega de pacotes no DTLS é suprida pela correspondente garantia provida pelo serviço do MR-UDP.

6.2. Identificação de Entidades IoT

Para oferecer os cenários de comunicação descritos na seção 5, os protocolos desenvolvidos fazem uso da hierarquia de certificação de chaves públicas da figura 3 composta dos seguintes nós certificadores:

- **CA**: nó de certificação raiz, reconhecido por todas as entidades e representante da infraestrutura de cidade inteligente.
- **MobileHub CA**: nós de certificação dos *Mobile-Hubs* responsável por certificar as chaves de cada *Mobile-Hub* para cenários de 1 a 3. Por sua vez, cada *Mobile-Hub* pode certificar as chaves de objetos inteligentes que se conectam unicamente por este *Mobile-Hub* e são previamente conhecidos, conforme cenário 1.
- **OrphanObj CA**: nó de certificação de objetos inteligentes órfãos, ou seja, que podem ser reconhecidos diretamente pela infraestrutura, sem a necessidade de autenticação mediada por um *Mobile-Hub*.
- **User CA**: nó de certificação de usuários utilizado no cenário 2.
- **Gateway CA**: nó de certificação das chaves dos *gateways* SDDL da infraestrutura de cidades inteligentes, com os quais a comunicação na nuvem da cidade é autenticada em todos os cenários.

Em todos os cenários, os protocolos seguem o modelo de autenticação de chave pública utilizando o *handshake* do DTLS. Os certificados são identificados pelo UUID

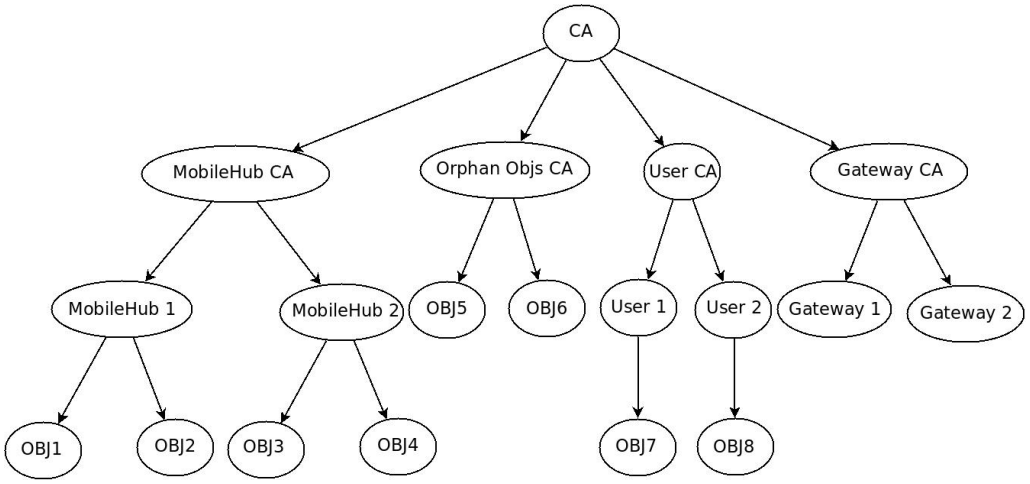

Figura 3. Hierarquia de Certificação para IoT

dos dispositivos, utilizado no CN (*Common Name*) do certificado x509. Exceto pelos objetos inteligentes órfãos, o gerenciamento hierárquico das identidades permite delegar aos *Mobile-Hubs* o controle das identidades das objetos inteligentes, conferindo escalabilidade ao gerenciador de identidades da infraestrutura da cidade inteligente.

6.3. Transporte de Mensagens ContextNet

Nos cenários de 1 a 3, as mensagens trocadas com os objetos inteligentes são disseminadas diretamente no *ContextNet*, já que o *Mobile-Hub* intermediário está autenticado na infraestrutura. Do ponto de vista da entrega de mensagens, a única diferença em relação à entrega já usada no *ContextNet* é a inclusão de assinatura das mensagens no cenário 1, com a qual a infraestrutura ou destinatários das mensagens (*subscribers*) são capazes de certificar a origem da mensagem. A assinatura é incluída em metainformações acrescentadas nas publicações SDDL, nos campos `MHub Signature` e `MObj Signature`, indicando respectivamente a assinatura do *Mobile-Hub* e do objeto inteligente, como no seguinte exemplo:

```
{
  "uuid":"78905b55-9584-4ad7-9ce0-d69cc9bd18ed",
  "mobj uuid":"11064610-edc6-43cc-9b72-c0917d47367e",
  "sensor_name":"Temperatura",
  "sensor_value":"23.68053746977472",
  "MHub Signature":"g2sbQU8oCHwt...Cw44GoCgcZdw2af4xJs82==",
  "MObj Signature":"3TwqUMgM3m96...93gEdvO6evjPhts3y2CV0=="
}
```

No cenário 4, o protocolo SMR-UDP realiza o tunelamento das mensagens encriptadas pelo DTLS entre o objeto inteligente e o gateway da infraestrutura no MR-UDP.

7. Conclusão

Aplicações para Internet das Coisas Móveis podem possuir diferentes requisitos de segurança para comunicação oportunista e disseminação de informações, o que exige

que arquiteturas de comunicação baseadas em paradigmas de propósito geral, como publish/subscribe, se adequem às políticas de segurança tanto dos objetos inteligentes como dos intermediários de comunicação (gateways). Este artigo apresentou uma arquitetura segura para Internet das Coisas Móveis, baseada no middleware ContextNet, e que oferece serviços de confidencialidade, autenticação e integridade. A arquitetura desenvolvida oferece quatro cenários de autenticação diferentes: *gateway* dedicado, confiança baseada no usuário, objeto inteligente anônimo e *gateway* anônimo. A implementação das identidades dos participantes e a sua autenticação faz o uso de uma infraestrutura de chaves públicas que estabeleceu diferentes categorias de entidades para a cidade inteligente. Com essa solução, foi possível garantir a escalabilidade no gerenciamento de identidades e na autenticação. Como próximos passos nesta pesquisa, avaliaremos os atrasos introduzidos pela arquitetura nas mensagens DDS.

Referências

David, L., Vasconcelos, R., Alves, L., André, R., and Endler, M. (2013). A dds-based middleware for scalable tracking, communication and collaboration of mobile nodes. *Journal of Internet Services and Applications*, 4(1):16.

Diro, A. A., Chilamkurti, N., and Nam, Y. (2018). Analysis of lightweight encryption scheme for fog-to-things communication. *IEEE Access*, 6:26820–26830.

Endler, M., Silva, A., and Cruz, R. A. M. S. (2017). An approach for secure edge computing in the internet of things. In *2017 1st Cyber Security in Networking Conference (CSNet)*, pages 1–8.

Foundation, D. (2019). *Data Distribution Service for Real-time Systems Specifications*. `https://www.dds-foundation.org/`.

Han, J. H. and Kim, J. (2017). A lightweight authentication mechanism between iot devices. In *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pages 1153–1155.

Mahmoud, R., Yousuf, T., Aloul, F., and Zualkernan, I. (2015). Internet of things (iot) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341.

Nery e Silva, L., Endler, M., and Roriz, M. (2013). Mr-udp: Yet another reliable user datagram protocol, now for mobile nodes.

Rescorla, E. and Modadugu, N. (2012). Datagram transport layer security version 1.2. RFC 6347.

Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., Ramdhany, R., Gluhak, A., Krco, S., Theodoridis, E., and Pfisterer, D. (2014). Smartsantander: Iot experimentation over a smart city testbed. *Computer Networks*, 61:217 – 238. Special issue on Future Internet Testbeds – Part I.

Talavera, L. E., Endler, M., Vasconcelos, I., Vasconcelos, R., Cunha, M., and d. S. e. Silva, F. J. (2015). The mobile hub concept: Enabling applications for the internet of mobile things. In *2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pages 123–128.