Desenvolvimento de uma aplicação segura de sensoriamento através de redes oportunísticas

Lucas S. dos Santos[1], **Paulo Roberto de M. Nascimento**[2]
Raphael C. S. Machado[2] **e Claudio L. Amorim** [1]

[1]Universidade Federal do Rio de Janeiro
Rio de Janeiro – RJ – Brasil

[2]Instituto Nacional de Metrologia, Qualidade e Tecnologia
Duque de Caxias - RJ - Brasil

{lseveriano,amorim}@cos.ufrj.br {prnascimento,rcmachado}@inmetro.gov.br

Abstract. *The Internet of Things has making the Internet even more present in people routine by allowing the integration of a variety of physical objects and devices in the network. This new paradigm presents new challenges related to systems architectures design and the inherent risks in information security. Given this, we present an Internet of Things application based on an opportunistic communication network, as well as the security requirements to be evaluated.*

Resumo. *Internet das Coisas vem tornando a Internet cada vez mais presente no cotidiano das pessoas ao permitir a integração de uma variedade de objetos físicos e dispositivos na rede. Este novo paradigma apresenta novos desafios relacionados ao projeto da arquitetura do sistema e riscos inerentes à segurança da informação. Diante disso, apresentamos uma aplicação de Internet das Coisas baseada em uma rede oportunística de comunicação, assim como os requisitos de segurança a serem avaliados*[1].

1. Introdução

A proliferação de objetos físicos interconectados vem crescendo em função do avanço de diversas áreas como Sistemas Embarcados, Microeletrônica, Comunicação e Sensoriamento [Al-Fuqaha et al. 2015] [Santos et al. 2016]. Neste contexto, Internet das Coisas – *Internet of Things* (IoT) se apresenta como um novo paradigma da Tecnologia da Informação e Comunicação (TIC), no qual um grande número de dispositivos, incluindo medidores, sensores e atuadores, são interconectados em rede de modo a cooperar uns com os outros com a finalidade de alcançar um objetivo em comum [Atzori et al. 2010].

O conceito de Internet das Coisas torna a Internet ainda mais imersiva e abrangente ao permitir acesso e interação a uma variedade de dispositivos nos quais geram dados abertos para consumo por terceiros [Zanella et al. 2014]. Este paradigma pode ser empregado a diversos ambientes e aplicações como automação residencial, assistência médica, sistemas de transporte e/ou resposta de emergência a catástrofes. Notavelmente, o paradigma de Internet das Coisas oferece um extraordinário potencial, porém introduz novos desafios aos desenvolvedores de sistemas no que se refere a escalabilidade, mobilidade e interoperabilidade [Amadeo et al. 2016] [Li et al. 2014].

[1]Trabalho apoiado por CNPq, Faperj e Projeto SHCDCiber.

A Internet das Coisas apresenta, também, novas ameaças e desafios relacionados a segurança, privacidade, confiabilidade, integridade e disponibilidade, visto que este cenário é composto por diversos dispositivos com capacidade de monitoramento e controle de objetos físicos [Al-Fuqaha et al. 2015] [Andrea et al. 2015]. Portanto, é necessário que os dispositivos presentes na rede atendam a uma série de requisitos de segurança especificados de acordo com o risco da aplicação. Complementarmente, as limitações do endereçamento IP, que funciona tanto como localizador quanto como identificador da informação, e a necessidade de um sistema de resolução, suporte de mobilidade complexo e acesso massivo, tornam a pilha de protocolos TCP/IP ineficiente diante do cenário de Internet das Coisas [Amadeo et al. 2016] [Li et al. 2014].

Diante deste cenário, este trabalho propõe uma aplicação de sensoriamento que utiliza uma rede oportunística como mecanismo de transmissão de dados. Entre as vantagens desta abordagem destacamos a redundância e a sua utilização em ambientes sem infraestrutura de redes previamente estabelecida. Além disso, especificamos os requisitos de segurança a serem avaliados no contexto da aplicação proposta. O restante deste trabalho está organizado da seguinte forma: A seção 2 é apresentado os trabalhos relacionados. A seção 3 descreve os conceitos fundamentais sobre redes oportunísticas e o protocolo RadNet. A seção 4 apresenta a aplicação de sensoriamento proposta neste trabalho. A seção 5 aponta as especificações de requisitos de segurança da aplicação proposta. Finalmente, a seção 6 apresenta as considerações finais e trabalhos futuros.

2. Trabalhos Relacionados

Sistemas de monitoramento de ambiente, em geral, controlam e monitoram grandezas físicas como temperatura e umidade. Um número considerável de estudos vem sendo conduzidos a fim de solucionar problemas referentes ao monitoramento de ambiente [Othman and Shazali 2012]. [Hudhajanto et al. 2018] implementou uma Rede de Sensores sem Fio para monitoramento de ambiente em tempo real. Cada nó sensor é composto por sensores de temperatura, umidade e CO2 conectados a um Arduino. Na topologia proposta, os nós sensores enviam os dados, provenientes dos sensores, para um *gateway* através do padrão IEEE 802.15.4 (Xbee). O *Gateway*, por sua vez, consiste de um *Rasperry Pi* no qual é responsável por sincronizar os dados coletados e armazenados (numa base de dados MySQL) com um serviço em nuvem através do protocolo TCP/IP.

O trabalho desenvolvido em [Shkurti et al. 2017] apresenta um sistema de monitoramento baseado em Web utilizando tecnologia de Redes de Sensores sem Fio. Os dispositivos, acoplados com sensores, coletam dados e os enviam, utilizando um roteador Wi-Fi, para uma aplicação em nuvem onde os dados serão persistidos numa base de dados.

Em [Del Campo et al. 2016] é realizada uma análise sobre a aplicabilidade do protocolo *Message Queuing Telemetry transport* (MQTT) em ambientes de vida assistida –*Ambient-Assisted Living* (AAL) [Montanini et al. 2016]. Os resultados obtidos e a estimativa de consumo de energia fornecida para cada caso mostram que o MQTT foi efetivamente adotado para um distribuição rápida e confiável de mensagens de notificação entre os diferentes agentes envolvidos na plataforma.

Em [Dasios et al. 2015] é apresentado o UbiCare, um sistema de assistência domiciliar para idosos. Neste sistema, o monitoramento é baseado no registro de parâmetros

ambientais, como temperatura e luminosidade, além de prover monitoramento e registro de atividades diárias. A rede é composta por dispositivos instalados num cômodo principal de uma casa, um dispositivo vestível (*wearable*), um nó atuador e um dispositivo para processamento centralizado (coordenador).

Os trabalhos apresentaram resultados promissores em relação as soluções propostas para desenvolvimento de sistemas de monitoramento ambiental. Contudo, tais soluções utilizam a pilha de protocolos TCP/IP o que torna o sistema dependente de uma infraestrutura previamente estabelecida para realizar a comunicação entre os dispositivos. Ademais, as soluções dos trabalhos relacionados não apresentam características de redes oportunísticas.

3. Conceitos Fundamentais

Nesta seção são apresentados os conceitos fundamentais que foram utilizados como base para o desenvolvimento do sistema de sensoriamento proposto neste trabalho. A seção está dividida em duas categorias: Redes oportunísticas e Protocolo RadNet.

3.1. Redes oportunísticas

Redes oportunísticas - *Opportunistic networks (OppNets)* são um tipo especial de rede *ad hoc* móvel - *Mobile Ad hoc Network (MANET)* onde os dispositivos móveis armazenam as informações e as carregam de acordo com a mobilidade do dispositivo até que ocorra uma oportunidade de comunicação para encaminhar os dados armazenados [Trifunovic et al. 2017]. Nesta categoria de redes, não há o pressuposto de que exista um caminho estabelecido entre dois dispositivos, ou nós, que se comuniquem. Deste modo, os nós de origem e destino podem nunca estar conectados à mesma rede e ao mesmo tempo. [Pelusi et al. 2006].

O paradigma de armazenar, carregar e encaminhar dados foi introduzido primeiramente no âmbito das redes tolerante a atraso — *Delay Tolerant Networks* (DTN) [Fall 2003]. Em uma DTN a arquitetura é constituída por uma rede independente de conectividade com a Internet onde a comunicação entre os dispositivos ocorre eventualmente ou de modo oportunístico. Neste cenário, cada comunicação oportunística pode ocorrer de forma agendada ou não determinística [Pelusi et al. 2006].

De acordo com este paradigma, os dados são ”movidos”pela rede, não apenas através do encaminhamento de mensagens entre os nós, mas também pela mobilidade dos próprios dispositivos que transportam mensagens enquanto esperam entrar na faixa de rádio dos nós intermediários ou do nó destinatário. Desta forma, redes oportunísticas são tradicionalmente consideradas como principal mecanismo para prover serviços de comunicação entre dispositivos portáteis onde não há uma infraestrutura de rede estabelecida [Conti et al. 2015].

3.2. Protocolo Radnet

Embora abordagens baseadas no pilha de protocolos TCP/IP sejam amplamente utilizadas na Internet, existem outras abordagens que não se baseiam no endereçamento IP para realizar a comunicação entre os dispositivos [Amadeo and Molinaro 2011] [Koponen et al. 2007] [Jacobson et al. 2009] [Gonçalves et al. 2016]. Uma destas arquiteturas, propostas na literatura, são as Redes *Ad Hoc* Centradas em Interesse - RadNets.

De acordo com [de Castro Dutra 2012], uma RadNet pode assumir as características de uma rede oportunística. Deste modo, a RadNet pode ser definida como um protocolo de redes oportunísticas a qual se enquadra no modelo *Publisher / Subscriber* (Publicador / Subscritor - Pub/Sub). Um nó publica uma mensagem com um determinado interesse na rede, em seguida, o nó que possuir o mesmo interesse registrado em sua aplicação recebe a mensagem publicada.

O protocolo Radnet foi originalmente proposto para uso em redes de comunicação MANETS (*Mobile Ad-hoc NETworkS*) com pouca ou nenhuma infraestrutura [Dutra et al. 2012]. Em uma RadNet os nós participantes utilizam de um mecanismo de nomeação chamado Prefixo Ativo (PA) que tem a finalidade de compensar a falta de infraestrutura básica de uma MANET. O PA (Figura 1) (a) é uma estrutura de dados implementado na camada de rede do dispositivo e é composto pelo prefixo do dispositivo e pelo interesse da aplicação. Nesta perspectiva, o prefixo é construído de modo a permitir a identificação do nó, encaminhamento probabilístico de mensagem e endereçamento. Complementarmente, o interesse da aplicação é utilizado para identificação do conteúdo que se deseja compartilhar. Por fim, a Figura 1 (b) exibe o cabeçalho da mensagem o qual é composto pela versão do protocolo, um limite de saltos, comprimento do cabeçalho, identificação da mensagem, dois prefixos que identificam os nós de origem e destino e um interesse da aplicação. [Dutra et al. 2012]

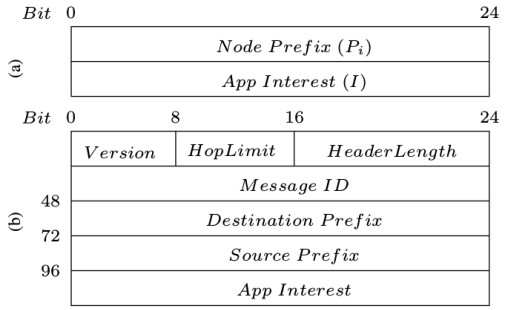

Figura 1. Elementos da RadNet: (a)Prefixo Ativo e (b) Cabeçalho da mensagem - Extraído de [Dutra et al. 2012]

Exemplo de comunicação em uma RadNet

A Figura 2 apresenta um exemplo de transmissão de pacotes entre quatro dispositivos na RadNet, onde cada nó tem um raio de alcance de transmissão delimitado pela circunferência tracejada. Nesse cenário, cada nó contém um PA formado por dois campos numéricos, e um interesse registrado na camada de rede. A comunicação é iniciada através do envio da mensagem do nó A com prefixo [1;5] e interesse [Futebol]. O nó B, no raio de alcance da transmissão de A, recebe o pacote proveniente de A, e encaminha a mensagem de A por haver casamento de prefixos de A com B (ex. critério de casamento: ambos PAs tem o mesmo valor 5 no 2º campo). O nó A recebe o pacote de volta encaminhado por B, porém detecta que o pacote já foi processado anteriormente e o descarta. O Nó C, recebe e encaminha a mensagem de A por haver casamento de prefixos no 1º campo(=1). Finalmente, o nó D, ao receber o pacote, detecta que possui o mesmo interesse (Futebol)

e o repassa para a aplicação local, mas não há casamento de prefixos, logo a mensagem não é repassada.

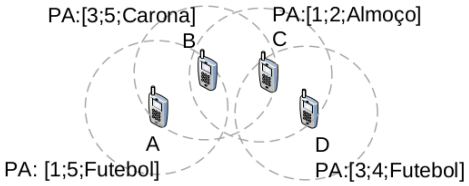

Figura 2. Exemplo de comunicação usando Radnet - Extraído de [Salles 2014]

4. Sistema Hermes

O Laboratório de Informática (Lainf), do Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro), é responsável pelo desenvolvimento do Sistema Hermes: um sistema de sensoriamento que implementa uma rede oportunística para transmissão de dados entre os dispositivos. Entre as características da abordagem adotada para este sistema destacamos a aplicabilidade em ambientes onde não há disponibilidade de infraestrutura de redes, além de garantir a disponibilidade do serviço de monitoramento mesmo quando ocorrem ataques de indisponibilidade na rede baseada na camada TCP/IP.

Como indicado na Figura 3, o sistema de sensoriamento proposto é composto por três categorias de agentes: Coletor, Mensageiro e Servidor. Portanto, estes agentes possuem como finalidade coletar, transportar e armazenar informações de ambiente, respectivamente. Neste cenário foram utilizados dispositivos Raspberry Pi, modelo 3 B+, como agentes Coletores, os quais foram conectados à sensores para realizar a coleta e registro de dados de sensoriamento, armazenando temporariamente as informações geradas. No escopo deste trabalho, o agente Mensageiro é composto por um dispositivo Raspberry PI acoplado a um Drone, para realizar o transporte dos dados até um servidor. O agente Servidor é responsável por armazenar os dados recebidos pelo agente Mensageiro, disponibilizá-los para outros serviços e aplicações disponíveis na rede e gerenciar o banco de dados.

Neste projeto, o agente Mensageiro é composto por um Drone, o qual é utilizado para realizar o transporte oportunístico das informações geradas pelos agentes Coletores. Porém, vale ressaltar que o agente Mensageiro pode ser qualquer dispositivo que possua capacidade de mobilidade, como o *smartphone* de uma pessoa que percorre um campus universitário ou um laptop em uso sendo transportado dentro de um carro, por exemplo.

4.1. Exemplo de comunicação no Sistema Hermes

A Figura 4 ilustra o procedimento de comunicação entre os agentes Coletor, Mensageiro e Servidor. O Coletor possui o prefixo *Pc* e o interesse *Ic = app-collector://request*. O Mensageiro contém o prefixo *Pm* e interesse Im = app-messenger://data. Finalmente, o Servidor tem o prefixo *Ps* e interesse *Is = app-server://store*. Portanto, o interesse de cada agente indica a sua função no projeto.

1. O mensageiro elabora o cabeçalho da mensagem com o prefixo de destino *null*, indicando uma mensagem *broadcast*, prefixo de origem *Pm*, interesse *Ic = app-*

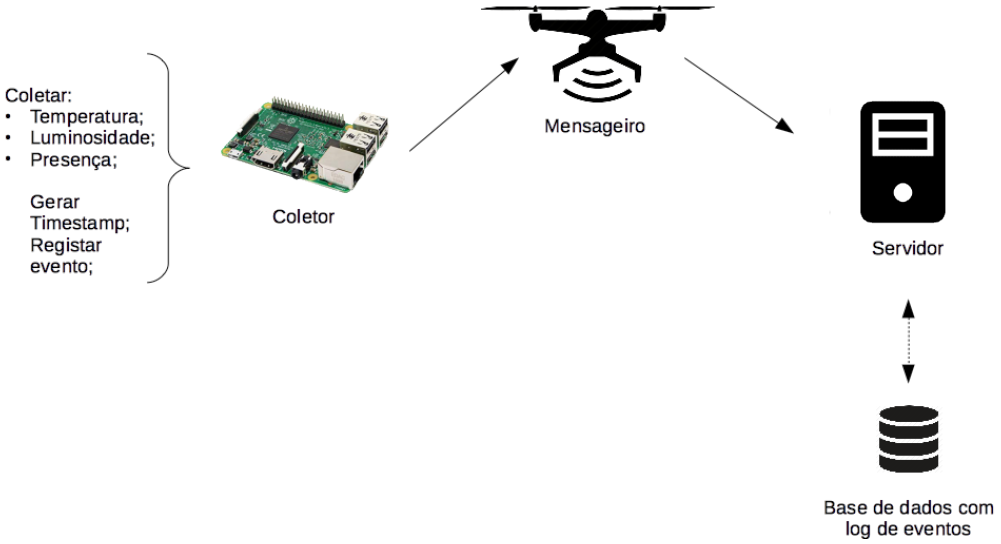

Figura 3. Representação em alto nível de aplicação de monitoramento

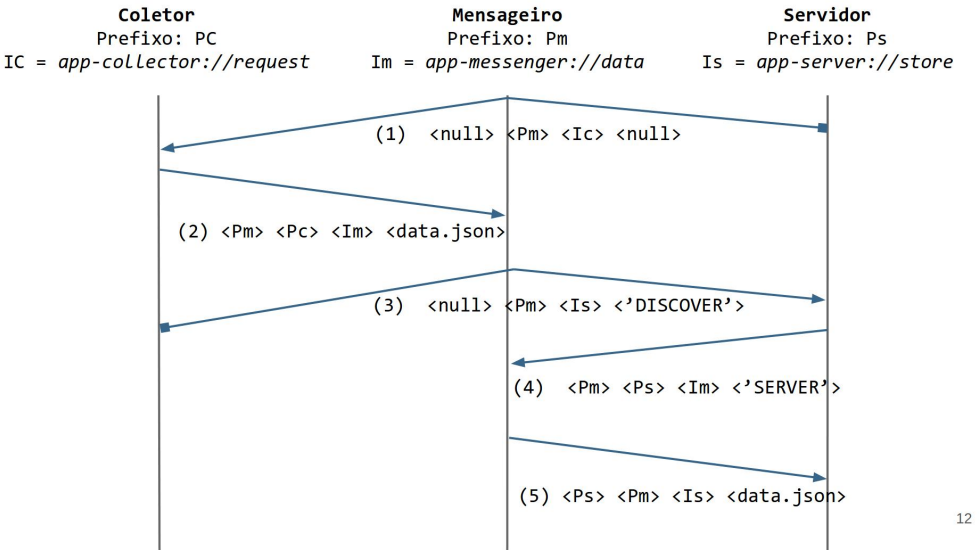

Figura 4. Exemplo de comunicação entre agentes

collector://request e *payload null*. Em seguida, a mensagem é enviada pelo Mensageiro através do protocolo Radnet. A mensagem é descartada pelo Servidor por não haver correspondência de interesse;

2. O Coletor, em contrapartida, recebe a mensagem do Mensageiro, pois existe correspondência de interesse. Logo, o Coletor monta a mensagem com prefixo de destino *Pm*, indicando que o destino final é o Mensageiro, prefixo de origem *Pc* e interesse *Im*. Neste caso, o *payload* da mensagem é composto pelas leituras do sensoriamento de ambiente. Por fim, o Mensageiro recebe e armazena temporariamente os dados de leitura do Coletor.
3. Dado que o Mensageiro possui dados armazenados, é montado um pacote para identificar a presença de algum servidor disponível. Neste sentido, é montada

a mensagem com interesse *Is* e *payload* 'DISCOVER' que indica ao servidor a intenção do Mensageiro iniciar o envio dos dados armazenados. Esta mensagem é descartada pelo Coletor por não haver correspondência de interesse.

4. O servidor recebe a mensagem, dado a correspondência de interesse. Logo, o servidor envia uma mensagem com *payload* 'SERVER' diretamente ao Mensageiro por meio do prefixo de destino *Pm*. O *payload* indica ao Mensageiro que existe um servidor disponível para receber os dados.
5. Finalmente, o Mensageiro envia os dados armazenados diretamente para o Servidor, que é responsável por persistir estas informações numa base de dados.

É interessante observar nesta estrutura que o agente Servidor se encontra em estado de *stand by*, sem emitir qualquer mensagem, permitindo que não seja descoberto até que outro dispositivo envie uma mensagem com o interesse registrado no agente Servidor, o que impede o acesso por dispositivos que não foram cadastrados na rede.

5. Especificação de Requisitos de Segurança

Aplicações de Internet das Coisas produzem dados que afetam diretamente as decisões tomadas tanto no contexto industrial quanto no cotidiano dos usuários finais. Portanto, é imprescindível que os serviços de Internet das Coisas implementem mecanismos de segurança visto que tais serviços se tornam alvos ao serem acessíveis através da rede local e Internet.

Com base na especificação da aplicação de monitoramento proposta neste trabalho, apresentamos os requisitos de segurança e apontamos os mecanismos que devem ser considerados e implementados para atender aos requisitos propostos: [Kaur and Mathur 2016] [Suo et al. 2012]:

- Proteção dos dispositivos - Técnicas de autenticação, autorização, prevenção de intrusão e detecção de intrusão deverão ser implementadas para garantir a proteção dos dispositivos;
- Confidencialidade dos dados - A confidencialidade dos dados está relacionada com o mecanismo de proteção da informação trafegada entre os dispositivos da rede, de forma que um dispositivo intruso não consiga interpretá-las e modificá-las. Para a aplicação de monitoramento apresentada na seção anterior, deverão ser implementadas técnicas de criptografia dos dados, assim como uma metodologia para distribuição de chaves públicas, de forma a assegurar que um dispositivo malicioso não divulgue sua chave pública pela rede;
- Integridade dos dados - A integridade poderá ser assegurada através de mecanismos de assinatura digital. Tendo em vista que no Sistema Hermes foram utilizados dispositivos *Raspberry Pi*, os quais possuem um poder computacional considerável, o custo para computação da assinatura não será relevante;
- Resistência contra ataques - A rede deverá ser resistente aos seguintes tipos de ataques:
    1. *Man in the middle* - Um dispositivo malicioso poderá se infiltrar na rede se passando por um dos dispositivos cadastrados. Contudo, no modelo proposto pela RadNet a transmissão dos dados ocorre na forma de um *broadcast*, permitindo que a informação alcance seu destino de forma redundante por diferentes rotas;

2. Desvios de pacotes - Dispositivos maliciosos podem causar a perda de pacotes, porém a redundância da rede permite contornar este problema;
3. *Denial of Service* (DoS) - Os dispositivos poderão enviar inúmeras mensagens para estabelecer uma conexão com os agentes Mensageiro e Servidor, impedindo que dados importantes sejam transferidos e armazenados. Este cenário poderá ser evitado limitando o número de mensagens aceitas por dispositivos;
4. Falsificação de ID - Dispositivos maliciosos poderão enviar mensagens utilizando diversos IDs. Para mitigar este ataque os dispositivos já autenticados na rede deverão verificar os IDs dos outros dispositivos para identificar a falsificação;

- Detecção de intrusão - Dispositivos maliciosos inseridos na rede poderão causar desvios de pacotes, não roteamento de pacotes e atraso nas respostas. Na aplicação proposta neste trabalho, deverão ser implementadas técnicas que permitam aos dispositivos analisarem a troca de mensagens com outros dispositivos da rede e identificarem o comportamento malicioso, como apresentado por [Subramaniyan et al. 2014].

6. Considerações Finais e Trabalhos Futuros

Embora a pilha de protocolos TCP/IP sejam amplamente utilizada na Internet, existem abordagens alternativas que não se baseiam no endereçamento IP. Neste trabalho, foi apresentado o Sistema Hermes, uma aplicação de sensoriamento que utiliza um protocolo de redes oportunísticas centrada em interesse, denominada RadNet. A aplicação proposta mostrou como essa rede pode operar em cenários onde não existem uma infraestrutura pré-estabelecida e como podem ser enviadas informações de monitoramento caso a infraestrutura da rede local existente seja comprometida.

A aplicação de sensoriamento permitiu implementar o protocolo RadNet em uma nova arquitetura onde os agentes Coletor, Mensageiro e Servidor foram desenvolvidos especificamente para esse cenário de sensoriamento, utilizando um Drone no transporte de dados entre os pontos distantes. Contudo, a mesma arquitetura poderá ser adaptada, substituindo o Drone por outros dispositivos móveis, em cenários de monitoramento ambiental e prevenção de catástrofes, aplicações de Internet das Coisas voltadas para a área de saúde ou mobilidade de veículos, por exemplo.

A implementação de uma rede oportunística para Internet das Coisas levanta diversos questionamentos sobre requisitos de segurança que deverão ser atendidos para evitar ataques que possam impedir o correto funcionamento da aplicação. Neste trabalho foram identificados pontos a serem avaliados que trarão maior resistência aos principais ataques conhecidos pela comunidade científica, assim como as medidas para mitigar as ocorrências e consequências desses ataques.

Para trabalhos futuros serão investigadas e analisadas as implementações de mecanismos de segurança adequados na coleta de dados, transmissão de mensagens criptografadas, técnicas de distribuição de chaves para assegurar a comunicação entre os nós da rede e a autenticação dos dispositivos utilizando o protocolo RadNet.

Referências

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., and Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, 17(4):2347–2376.

Amadeo, M., Campolo, C., Quevedo, J., Corujo, D., Molinaro, A., Iera, A., Aguiar, R. L., and Vasilakos, A. V. (2016). Information-centric networking for the internet of things: challenges and opportunities. *IEEE Network*, 30(2):92–100.

Amadeo, M. and Molinaro, A. (2011). Chanet: A content-centric architecture for ieee 802.11 manets. In *2011 International Conference on the Network of the Future*, pages 122–127. IEEE.

Andrea, I., Chrysostomou, C., and Hadjichristofi, G. (2015). Internet of things: Security vulnerabilities and challenges. In *2015 IEEE Symposium on Computers and Communication (ISCC)*, pages 180–187. IEEE.

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer networks*, 54(15):2787–2805.

Conti, M., Boldrini, C., Kanhere, S. S., Mingozzi, E., Pagani, E., Ruiz, P. M., and Younis, M. (2015). From manet to people-centric networking: Milestones and open research challenges. *Computer Communications*, 71:1–21.

Dasios, A., Gavalas, D., Pantziou, G., and Konstantopoulos, C. (2015). Hands-on experiences in deploying cost-effective ambient-assisted living systems. *Sensors*, 15(6):14487–14512.

de Castro Dutra, R. (2012). *REDES AD HOC CENTRADAS EM INTERESSES PARA AMBIENTES MOVEIS*. PhD thesis, Universidade Federal do Rio de Janeiro.

Del Campo, A., Gambi, E., Montanini, L., Perla, D., Raffaeli, L., and Spinsante, S. (2016). Mqtt in aal systems for home monitoring of people with dementia. In *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1–6. IEEE.

Dutra, R. C., Moraes, H. F., and Amorim, C. L. (2012). Interest-centric mobile ad hoc networks. In *Network Computing and Applications (NCA), 2012 11th IEEE International Symposium on*, pages 130–138. IEEE.

Fall, K. (2003). A delay-tolerant network architecture for challenged internets. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 27–34. ACM.

Gonçalves, F. B., França, F. M., and de Amorim, C. L. (2016). Interest-centric vehicular ad hoc network. In *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 1–10. IEEE.

Hudhajanto, R. P., Fahmi, N., Prayitno, E., et al. (2018). Real-time monitoring for environmental through wireless sensor network technology. In *2018 International Conference on Applied Engineering (ICAE)*, pages 1–5. IEEE.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., and Braynard, R. L. (2009). Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 1–12. ACM.

Kaur, N. and Mathur, G. (2016). Opportunistic networks: A review. *IOSR Journal of Computer Engineering (IOSR-ICE)*, 18(2):20–26.

Koponen, T., Chawla, M., Chun, B.-G., Ermolinskiy, A., Kim, K. H., Shenker, S., and Stoica, I. (2007). A data-oriented (and beyond) network architecture. *ACM SIGCOMM Computer Communication Review*, 37(4):181–192.

Li, S., Zhang, Y., Raychaudhuri, D., and Ravindran, R. (2014). A comparative study of mobilityfirst and ndn based icn-iot architectures. In *10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, pages 158–163. IEEE.

Montanini, L., Raffaeli, L., De Santis, A., Del Campo, A., Chiatti, C., Rascioni, G., Gambi, E., and Spinsante, S. (2016). Overnight supervision of alzheimer's disease patients in nursing homes: System development and field trial. In *2nd International Conference on Information and Communication Technologies for Ageing Well and e-Health, ICT4AWE 2016*, pages 15–25. SciTePress.

Othman, M. F. and Shazali, K. (2012). Wireless sensor network applications: A study in environment monitoring system. *Procedia Engineering*, 41:1204–1210.

Pelusi, L., Passarella, A., and Conti, M. (2006). Opportunistic networking: data forwarding in disconnected mobile ad hoc networks. *IEEE communications Magazine*, 44(11):134–141.

Salles, R. C. (2014). Avaliação de capacidade e consumo de energia de rede móvel ad hoc centrada em interesse. Master's thesis, Universidade Federal do Rio de Janeiro. https://www.cos.ufrj.br/index.php/pt-BR/publicacoes-pesquisa/details/15/2497.

Santos, B. P., Silva, L., Celes, C., Borges, J. B., Neto, B. S. P., Vieira, M. A. M., Vieira, L. F. M., Goussevskaia, O. N., and Loureiro, A. (2016). Internet das coisas: da teoria a prática. *Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos*.

Shkurti, L., Bajrami, X., Canhasi, E., Limani, B., Krrabaj, S., and Hulaj, A. (2017). Development of ambient environmental monitoring system through wireless sensor network (wsn) using nodemcu and "wsn monitoring". In *2017 6th Mediterranean Conference on Embedded Computing (MECO)*, pages 1–5. IEEE.

Subramaniyan, S., Johnson, W., and Subramaniyan, K. (2014). A distributed framework for detecting selfish nodes in manet using record-and trust-based detection (rtbd) technique. *EURASIP Journal on Wireless Communications and Networking*, 2014(1):205.

Suo, H., Wan, J., Zou, C., and Liu, J. (2012). Security in the internet of things: a review. In *2012 international conference on computer science and electronics engineering*, volume 3, pages 648–651. IEEE.

Trifunovic, S., Kouyoumdjieva, S. T., Distl, B., Pajevic, L., Karlsson, G., and Plattner, B. (2017). A decade of research in opportunistic networks: challenges, relevance, and future directions. *IEEE Communications Magazine*, 55(1):168–173.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., and Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things journal*, 1(1):22–32.