Revisão Sistemática sobre Segurança Adaptativa Ciente de Contexto para a Internet das Coisas

Ricardo Borges Almeida[1], **Roger da Silva Machado**[1], **Adenauer Corrêa Yamin**[1], **Ana Marilza Pernas**[1]

[1]Programa de Pós-Graduação em Computação (PPGC)
Universidade Federal de Pelotas (UFPel), Pelotas – RS – Brasil

{rbalmeida,rdsmachado,adenauer,marilza}@inf.ufpel.edu.br

Abstract. *The Internet of Things (IoT) consists of an ecosystem that combines wireless sensor networks, cloud computing, analytical data, interactive technologies as well as intelligent devices. Promoting security over this dynamic and heterogeneous environment with pre-defined and static mechanisms is a challenging task which requires adaptive security solutions. The objectives of this paper are: (i) systematize and present the concepts of adaptive security for IoT, including its relation with studies in context awareness; (ii) carry out a systematic review of the literature in order to identify the state of the art; and (iii) develop a critical analysis over the identified papers in an effort to list research opportunities.*

Resumo. *A Internet das Coisas (IoT) consiste em um ecossistema que combina redes de sensores sem fio, computação em nuvem, dados analíticos, tecnologias interativas, bem como dispositivos inteligentes. Promover a segurança sobre este ambiente dinâmico e heterogêneo com mecanismos pré-definidos e estáticos pode resultar em decisões inadequadas, o que implica na necessidade de soluções para segurança adaptativa. Tendo isto em vista, os objetivos deste trabalho consistem em: (i) sistematizar e apresentar os conceitos sobre segurança adaptativa para IoT, incluindo a sua relação com os estudos em ciência de contexto; (ii) realizar uma revisão sistemática da literatura buscando identificar o estado da arte; e (iii) desenvolver uma análise crítica sobre os trabalhos identificados, em um esforço para elencar oportunidades de pesquisa.*

1. Introdução

Uma materialização da Computação Ubíqua (UbiComp) que vem ganhando destaque é a Internet das Coisas, do inglês *Internet of Things* (IoT). Apesar das inúmeras contribuições que a IoT tem proporcionado, a decorrente proliferação de dispositivos conectados criou novas demandas na segurança da informação. Este mercado tem inspirado novas tecnologias, no entanto, na tentativa de manterem-se competitivos, os fabricantes buscam diminuir o tempo de produção destes dispositivos, o que torna questionável o nível de segurança no ciclo de vida do desenvolvimento [Kliarsky and Leune 2017].

Adicionalmente, as organizações muitas vezes implementam tecnologias de propósitos específicos para promover a segurança de seus ambientes computacionais, no entanto, elas se limitam a analisar informações contextuais específicas, não fornecendo um contexto holístico para análise de risco, resultando em decisões inadequadas de

adaptação para mitigação [Aman 2016]. Esses desafios, visões e vantagens impulsionam a investigação por soluções de segurança efetivas para os ambientes da IoT, uma vez que os atuais controles de segurança tradicionais são ineficientes e insuficientes para essa rede dinâmica e heterogênea em desenvolvimento.

Este trabalho concentra-se especialmente na exploração dos mecanismos de adaptação aplicados para promover a segurança de ambientes da IoT, ou seja, na segurança adaptativa para IoT. Observa-se que, especialmente devido as características da IoT, a aplicação dos conceitos de ciência de contexto e a integralização das diferentes soluções de segurança se mostram demandas oportunas.

Os objetivos deste trabalho consistem em: (i) sistematizar e apresentar os conceitos sobre adaptação ciente de contexto para IoT, incluindo a sua relação com a segurança da informação; (ii) realizar uma revisão sistemática da literatura buscando identificar o estado da arte em segurança adaptativa ciente de contexto baseada em eventos para IoT; e (iii) desenvolver uma análise crítica sobre os trabalhos identificados em um esforço para elencar as lacunas existentes nesta área.

Este trabalho foi organizado em 7 seções. Nesta primeira seção foi apresentada uma breve introdução ao tema central da pesquisa, suas motivações e objetivos. Na sequência, nas seções 2, 3 e 4 são discutidos os conceitos em torno da segurança adaptativa ciente de contexto para IoT. A seção 5 apresenta o estado da arte, para na seção 6 serem discutidos os trabalhos selecionados e as oportunidades de pesquisa. Por fim, a seção 7 discute as considerações finais.

2. Internet das Coisas

A Internet das Coisas consiste da onipresença de vários objetos ou coisas, incluindo tecnologias de sensores e dispositivos móveis físicos, sem e com fio, que interagem uns com os outros para cumprir objetivos comuns [Giusto et al. 2010]. A IoT é entendida como um ambiente inteligente que pode reagir às mudanças ou eventos que ela percebe em seu ecossistema.

A IoT, ao menos na teoria, visa tornar o cotidiano das pessoas mais simples, prático e produtivo, o que justifica a sua crescente popularidade. Desde a introdução de RFID como uma das tecnologias no âmbito da IoT, uma infinidade de outros sensores e objetos móveis são introduzidos para ampliar sua visão. Para exemplificar alguns dos dispositivos associados a esta afirmação é possível citar os relógios inteligentes, carros, cafeteiras, geladeiras, robôs aspiradores, entre outros. Este ambiente permite uma integração dos objetos físicos, móveis e de sensoriamento na infraestrutura tradicional, criando assim novas oportunidades de negócio. A eHealth[1], os edifícios inteligentes, as redes inteligentes e os sensores de meio ambiente são alguns exemplos de serviços e aplicações habilitadas pela IoT em diferentes campos [Aman 2016].

Para fornecer suporte a este ambiente dinâmico, considerando o escopo deste trabalho e, em especial, a necessidade de segurança em torno da IoT, exemplos de recursos que devem ser almejados incluem [Miorandi et al. 2012]: suporte à heterogeneidade de dispositivos em diferentes níveis da arquitetura (protocolos, eventos, aplicação); escalabilidade, permitindo o tratamento de um crescente volume de dados, e; autonomia, uma

[1]Uso de tecnologia da informação para saúde.

vez que a complexidade, a dinâmica e as especificidades que muitos cenários da IoT apresentam implicam na necessidade de que os dispositivos (ou parte deles) sejam capazes de reagir de maneira autônoma às diferentes situações, buscando minimizar a intervenção humana.

Apesar dos benefícios fornecidos, algumas questões ainda não foram abordadas, como a visibilidade global, o gerenciamento autônomo em tempo real, a regularização, a padronização, a interoperabilidade dos sistemas, o consumo de recursos, a distribuição, o suporte à QoS, a privacidade dos dados e a segurança [Miorandi et al. 2012]. Algumas dessas preocupações, como as questões de QoS e os consumos de recursos, são, em última instância, um problema de segurança, pois influenciam ou são influenciados direta ou indiretamente. Assim, pode-se estabelecer que a segurança é um dos problemas críticos que precisa ser adequadamente abordado [Miorandi et al. 2012, Sicari et al. 2015].

3. Segurança Adaptativa

A adaptação, dinâmica ou em tempo de execução, consiste na capacidade de um sistema em monitorar e regular, de forma autônoma, seu comportamento de acordo com as situações de interesse ou alterações sob observação [Aman 2016]. Esta propriedade auxilia na complexidade dos ambientes computacionais compostos pela IoT, utilizando a tecnologia para gerenciar a tecnologia, buscando-se minimizar a necessidade de intervenção humana. Com isto, a segurança adaptativa é a capacidade de um sistema observar os ambientes sob sua gerência, analisar quaisquer potenciais ameaças de segurança e responder de forma autônoma aos riscos que estas representam e as falhas dos sistemas que compõem o ambiente, visando reduzir seus possíveis impactos [Aman 2016].

Muitas equipes de segurança da informação operam sob um comportamento alinhado à "resposta a incidentes", o que é importante para área. No entanto, com os atuais ambientes computacionais, em especial devido as mudanças consequentes da IoT, é necessário operar seguindo uma "resposta contínua", onde os sistemas são assumidos como comprometidos e exigem monitoramento e correção contínua, em tempo de execução.

A literatura defende o uso de métodos formais para fornecer evidências de que as mudanças nas situações do ambiente monitorado satisfaçam os objetivos de segurança de um sistema [Aman 2016]. Uma abordagem promissora para segurança adaptativa considerando os ambientes da IoT é o emprego de um ciclo de *feedback*.

Em uma tentativa de lidar com as complexidades dos sistemas modernos de computação a *International Business Machines* (IBM) sugeriu o modelo *Monitor-Analyze-Plan-Execute plus Knowledge* (MAPE-K), conforme apresentado na Figura 1. O MAPE-K utiliza as atividades Monitorar, Analizar, Planejar e Executar empregando um ciclo de controle em conjunto com o componente Conhecimento que fornece as informações necessárias para realizar a adaptação [Aman 2016].

O componente Monitor coleta os dados apropriados dos recursos gerenciados por meio dos sensores. Os dados são correlacionados, filtrados e/ou agregados e o sintoma descoberto é passado para o componente Analisar. Sintomas e outros dados também podem ser armazenados em uma base de conhecimento compartilhada. O analisador determina se uma mudança precisa ser feita com base no conhecimento compartilhado (potencialmente uma política) e nos sintomas. Caso pertinente, uma solicitação de mudança

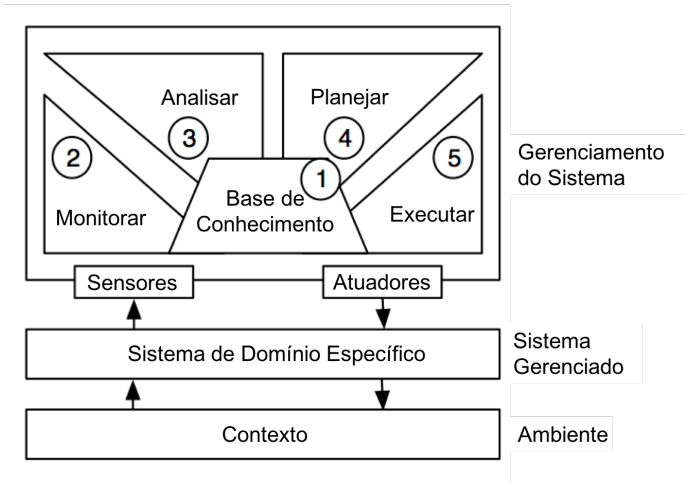

Figura 1. MAPE-K - Modelo para sistemas adaptativos
Fonte: IGLESIA; WEYNS, 2015

no ambiente é passada para o componente Planejar. O planejador gera os comandos ou fluxos de trabalho necessários na forma de um plano de alteração que é passado para o componente Executar. O executor aplica o plano de mudança no recurso de gerenciamento usando os atuadores. Caso necessário, a base de conhecimento pode ser atualizada, fornecendo dados do impacto da adaptação para serem aplicados como *feedback* para o próximo ciclo.

Em [Evesti 2014], os autores mencionam dois atributos oportunos para promover a segurança adaptativa, a autoconsciência (*self-awareness*) e a ciência de contexto (*context awareness*). A autoconsciência é a capacidade do sistema em conhecer seu próprio estado, seus componentes, capacidades, limites, recursos e comportamento. Já a ciência do contexto, consiste do conhecimento sobre o ambiente operacional ao qual o sistema está inserido.

4. Ciência de Contexto na Segurança Adaptativa

A ciência de contexto está presente nas pesquisas relacionadas a UbiComp, sendo um dos grandes desafios no desenvolvimento de aplicações nesta área. Para entender o seu significado, primeiramente é necessário definir **contexto**, que de acordo com Dey (2001) é qualquer informação que pode ser usada para caracterizar a situação de uma entidade (pessoa, local ou objeto) que seja considerada relevante para a interação entre o usuário e a aplicação, incluindo o próprio usuário e a aplicação. Contexto é o que contribui para a correta interpretação de uma ação ou evento, sem, no entanto, ser parte dessa ação/evento.

A ciência de contexto vem sendo foco de um grande número de pesquisas em diferentes áreas, consequentemente assumindo diferentes significados. Dessa forma, neste texto entende-se por **ciência de contexto** a capacidade de um sistema em usar o contexto para prover serviços e/ou informações relevantes para o usuário [Dey 2001].

Ao se construir e executar aplicações cientes de contexto há uma série de funcionalidades que devem ser providas, envolvendo desde a aquisição de informações contextuais, a partir do conjunto de fontes heterogêneas e distribuídas, até a representação dessas informações, seu processamento, armazenamento, e a realização de inferências para seu

uso em tomadas de decisão [Bellavista et al. 2012]. Tais tarefas se alinham ao ciclo de *feedback* empregado na formalização da segurança adaptativa.

Os sistemas cientes de contexto devem ser flexíveis, se adaptarem, e serem capazes de atuar automaticamente para ajudar o usuário na realização de suas atividades, o que está diretamente associado às necessidades das soluções para segurança da informação. Algumas motivações para usar a ciência de contexto são: auxilia na compreensão da realidade; facilita na adaptação de sistemas; auxilia no processo de transformação dos dados em informação, e; apoia a compreensão de eventos e de situações.

No que tange a segurança adaptativa, caso os contextos relevantes para a identificação das situações a serem avaliadas não sejam adequadamente considerados, pode haver uma influência adversa no ambiente impactando nos serviços oferecidos. A ciência de contexto é especialmente crítica nos cenários da IoT, em particular na adaptação, pois esta consiste em uma comunicação máquina para máquina, a priori sem a inteligência (envolvimento direto) dos humanos. Caso sejam empregados contextos irrelevantes, incorretos ou insuficientes, a adaptação pode não ser eficiente [Aman 2016].

5. Estado da Arte

Esta seção tem como objetivo apresentar o estado da arte em pesquisas que empregam ciência de contexto para segurança adaptativa na IoT. Para isto, foi realizada uma revisão sistemática da literatura sobre o tema. Desta forma, na subseção seguinte é apresentado o protocolo executado para posteriormente discutir os trabalhos selecionados.

5.1. Revisão Sistemática da Literatura

A revisão sistemática realizada neste trabalho aplicou um processo que estabelece uma série de atividades a serem executadas e registradas, permitindo que o estudo feito seja reproduzido por outros pesquisadores. A revisão adotou o teste de confiabilidade entre avaliadores, onde o autor principal deste trabalho realizou a seleção dos artigos de forma completa, e uma amostra dos artigos resultantes do processo foi disponibilizada aos co-autores.

Para auxiliar no desenvolvimento desta revisão foi utilizada a ferramenta StArt[2]. Como primeira etapa, seguindo o processo mencionado, foram definidas as seguintes questões de pesquisa: (Q1) Quais os atuais desafios de segurança adaptativa em IoT?; (Q2) Quais as estratégias utilizadas para avaliação das propostas?; (Q3) Quais as informações contextuais consideradas para adaptações?, e; (Q4) Quais os mecanismos para escolha da adaptação considerando diferentes contextos?

Com isto, as bases acadêmicas selecionadas para a identificação dos estudos primários foram: ACM Digital Library, Science Direct, IEEE Xplore, Web of Science e Scopus. A base Springer havia sido selecionada inicialmente, no entanto, ela foi excluída por não possibilitar a pesquisa usando operadores lógicos nos campos título, resumo e palavras-chaves.

O processo de busca pelos artigos seguiu um fluxo de execução onde, inicialmente, foi estabelecida a sequinte *string* de pesquisa: adapt* AND security AND context* AND (“internet of things” OR iot).

[2]http://lapes.dc.ufscar.br/tools/start_tool

Na sequência a *string* foi aplicada em cada base observando as particularidades de cada uma para realização deste processo nos campos título, resumo e palavras-chave. Posteriormente, para a triagem dos artigos, buscando delimitar os anos a serem considerados, foi realizada a investigação de um possível auge ou de um aumento considerável de um ano para o outro no número de artigos publicados. Desta forma, foi possível observar que em 2013 houve um aumento considerável para 2012 no volume de artigos, sendo então analisados nesta revisão sistemática artigos publicados de 2013 à outubro de 2018 (data da aplicação da string nas bases).

Com a submissão das *strings* nas bases, foi realizada a exportação para o formato .bib e importação para a ferramenta StArt. Um total de 239 artigos foram inicialmente identificados. A tabela 1 apresenta o número de artigos (I)ncluídos ou (E)xcluídos, de acordo com os critérios estabelecidos. Durante o processo de triagem, 217 foram excluídos após a análise do resumo e os 23 restantes tiveram suas seções de introdução, concepção do projeto e conclusão analisadas, sendo selecionados 5 artigos ao final do protocolo.

Tabela 1. Número de artigos por critério

Critério	Número de artigos
(E) artigo duplicado	90
(E) foi publicado antes de 2013	2
(E) não é um artigo de conferência ou periódico	36
(E) não apresenta um novo modelo ou *framework* para segurança adaptativa aplicada à IoT	79
(E) segurança adaptativa voltada para problema específico como autenticação, autorização, entre outros	19
(E) artigo mais atual apresenta modificações deste artigo	2
(I) explora conceitos relacionados à ciência de contexto	4
(I) explora conceitos sobre avaliação de risco	1
(E) O artigo não possui nenhum dos critérios de inclusão	6

Buscando uma melhor compreensão da amplitude dos 5 trabalhos identificados até esta etapa, uma busca pela produção bibliográfica dos autores junto à análise das principais referências utilizadas foi realizada. Com isso, para a revisão dos trabalhos, além da consideração de outros artigos e testes publicadas pelos mesmos autores dos 5 primeiros selecionados, o artigo [Evesti 2014] foi adicionado em razão das referências analisadas nos demais. Observa-se neste último caso que os artigos indexados nas bases consideradas publicados pelo mesmo autor [Evesti and Frantti 2015, Evesti et al. 2014] não foram retornados na pesquisa por não utilizaram os termos IoT e contexto em seus resumos, no entanto, os conceitos abordados e os objetivos do autor se adequam para consideração nesta revisão.

Como resultado da revisão sistemática da literatura foram selecionados 6 artigos, os quais são apresentados na subseção a seguir. Destaca-se que a análise contemplou não apenas os artigos selecionados após a aplicação do protocolo de revisão, mas sim toda a

produção bibliográfica dos autores associadas aos modelos propostos.

5.2. Trabalhos Selecionados

Esta subseção tem como objetivo descrever os trabalhos selecionados após a revisão sistemática. Desta forma, são apresentados os objetivos de cada proposta junto a uma análise crítica para, na seção 6, apresentar uma comparação entre estes trabalhos junto a possíveis oportunidades de pesquisa.

5.2.1. Adaptive security in smart spaces

A tese de doutorado de Antti Evesti (2014) apresenta uma arquitetura para segurança adaptativa em espaços inteligentes [Evesti 2014]. A abordagem combina um ciclo de adaptação, uma ontologia denominada *Information Security Measuring Ontology* (ISMO) e um modelo de controle de segurança para espaços inteligentes. O ciclo de adaptação inclui as fases de monitoramento, análise, planejamento e execução de mudanças no espaço inteligente. De acordo com os autores, a abordagem se diferencia por definir todo o ciclo de adaptação e o conhecimento necessário em cada etapa. As contribuições são validadas como parte do protótipo de um espaço inteligente. A abordagem oferece meios reutilizáveis e extensíveis para alcançar a segurança adaptativa em espaços inteligentes.

Apesar de inicialmente a arquitetura ser explorada por meio de políticas dinâmicas de controle de acesso, o trabalho foi estendido incluindo outros cenários de uso, sendo um voltado para sistemas de controle industrial. Ou seja, a segurança adaptativa pode ser aplicada em vários domínios, sendo uma abordagem de adaptação genérica, consequentemente habilitando a sua adoção para diferentes objetivos de segurança, incluindo ambientes da IoT.

De acordo com Evesti, a fase de monitoramento é definida em um nível detalhado, no entanto, as fases de análise e planejamento precisam de refinamentos. A fase de análise deve reconhecer o nível de segurança obtido com base nos resultados do monitoramento e deduzir o nível necessário a partir das informações de contexto. Aprimorar estas duas tarefas garantiria a identificação dos requisitos de segurança e as necessidades de adaptação em diferentes situações. Além disso, a fase de planejamento da adaptação necessita de algoritmos de tomada de decisão mais sofisticados, por exemplo, em situações complexas em que diferentes objetivos de segurança devem ser levados em conta. Finalmente, o autor menciona a necessidade de descentralização da abordagem, especialmente considerando o desenvolvimento das limitações aqui mencionadas que podem implicar em uma necessidade maior de poder computacional, seja de armazenamento ou processamento.

5.2.2. Managing Context Information for Adaptive Security in IoT Environments

O trabalho de Ramos et al. (2015) aborda os desafios de modelagem e desenvolvimento de mecanismos de segurança cientes de contexto para a IoT por meio da definição de dois objetivos. Por um lado, o trabalho visa fornecer uma visão geral das implicações de segurança para os estágios do ciclo de vida do gerenciamento de contexto na IoT. Por outro lado, com base em um *framework* de segurança para IoT proposto em [Bernabe et al. 2014], busca apresentar como as informações contextuais podem ser

usadas por outros componentes deste *framework* para capacitar objetos inteligentes com ciência de contexto ao tomar decisões de segurança [Ramos et al. 2015].

O trabalho apresentado em [Ramos et al. 2015] tem como foco o Gerenciador de Contexto (*Context Manager*), bem como as principais interações com outros componentes de segurança, a fim de tornar as decisões de segurança de objetos inteligentes cientes de contexto. Além disso, são propostos diferentes estágios para o ciclo de vida do gerenciamento de contexto, bem como um conjunto de diretrizes sobre implicações de segurança durante essas fases. O artigo apresenta como cada módulo proposto pode ser utilizado para aquisição, modelagem, organização, raciocínio, combinação e inferência de informações contextuais.

Finalmente, os autores discutem a necessidade de implementação das etapas do gerenciamento de contexto e das interações propostas com outros componentes de segurança, de modo a demonstrar a integração de mecanismos de segurança flexíveis, leves e adaptativos em diferentes cenários.

5.2.3. Adaptive Security in the Internet of Things

O trabalho de Waqas Aman (2016) apresenta a concepção de uma solução autônoma para o gerenciamento de risco adaptativo para a IoT que permite analisar situações adversas em um contexto distinto e gerenciar o risco envolvido de forma inteligente para que as preferências do usuário final, a qualidade do serviço e a segurança sejam preservados. Com isto, é apresentado o modelo de segurança adaptativa orientado a eventos para IoT, denominado *Event Driven Adaptive Security* (EDAS), o qual é aplicado em um cenário de eHealth para proteger o ambiente de ameaças em tempo de execução.

Para realizar o monitoramento dos eventos de segurança foi utilizada a solução *Open Source Security Information Management* (OSSIM[3]). No que tange as adaptações das configurações de segurança, de modo que as preferências de usuários e serviços sejam preservadas, os autores propõem uma ontologia que aproveita as informações de risco da correlação de eventos.

É possível afirmar que ao utilizar o OSSIM, o suporte à heterogeneidade fica limitado, uma vez que é necessário criar as regras para normalização usando uma sintaxe similar à XML por meio da edição de arquivos. Além disso, o OSSIM é reconhecido por apresentar limitações quanto a estabilidade e escalabilidade [Rochford and Kavanagh 2015]. De acordo com o próprio autor, os componentes de adaptação são meramente compostos por um analisador de *strings* e chamadas à API, sendo necessária uma abordagem independente de plataforma para fornecer interoperabilidade na IoT. Finalmente, a EDAS não considera possíveis vulnerabilidades que possam impedir eventuais ameaças no ambiente.

5.2.4. Efficient Security Adaptation Framework for Internet of Things

O artigo [El-Maliki and Seigne 2016] apresenta um *framework* genérico denominado *Security Adaptation Reference Monitor* (SARM) que emprega o paradigma autonômico,

[3]https://www.alienvault.com/products/ossim

sendo desenvolvido especialmente para ambientes suportados por redes sem fio altamente dinâmicas [El-Maliki and Seigne 2016]. O SARM realiza os ajustes dos parâmetros de segurança considerando o risco do ambiente atual e o desempenho do sistema, especialmente no que se refere à otimização do seu consumo de energia. Isto ocorre sob as políticas e as restrições de intervenção em tempo de execução dos usuários.

A proposta foi concebida seguindo uma metodologia de construção modular em blocos, de modo a facilitar a integração e ocultar a complexidade interna do sistema. Além disso, essa abordagem permite uma expansão gradual para atender aos novos requisitos da IoT devido à sua constante evolução. Para reagir em tempo real a qualquer ameaça, o SARM baseia-se em informação de *feedback*, buscando reduzir a intervenção humana.

Apesar de o SARM ser proposto como um modelo genérico, a sua descrição é apresentada em um alto nível, não sendo especificados detalhes de como os blocos modulares são implementados, ou ainda, como eles se comunicam. Os autores destacam que novas pesquisas são oportunas para suportar mais parâmetros de adaptação (como processamento e uso de memória). Além disso, eles mencionam a possibilidade de desenvolvimento do SARM diretamente no sistema operacional, o que vai contra algumas das premissas da IoT. Funções alternativas para tomada de decisão, como funções fuzzy e não lineares, poderiam aumentar a flexibilidade do SARM. Aumentar o número de informações contextuais para tomada de decisão pode melhorar a qualidade das adaptações, no entanto, aumentando o consumo energético. Os autores também consideram que qualquer contradição levantada pelas políticas, preferências do usuário e decisão do sistema deve ser abordada em tempo de execução, o que não é suportado completamente. Finalmente, questões de escalabilidade do SARM também devem ser consideradas com maior profundidade para melhorar a credibilidade do *framework*.

5.2.5. An Ontology-Based Cybersecurity Framework for the Internet of Things

O trabalho de Mozzaquatro et al. (2018) propõe uma arquitetura para *framework* de segurança adaptativa baseada no modelo MAPE-K utilizando uma ontologia para a tomada de decisões visando melhorar a segurança da informação em sistemas industriais [Mozzaquatro et al. 2018]. O *framework* contempla duas abordagens, uma em tempo de projeto e outra em tempo de execução.

A abordagem em tempo de execução, foco desta análise, monitora os dispositivos da IoT com base em métricas e atributos de segurança para identificar comportamentos maliciosos no ambiente. Consequentemente, quando os alertas são acionados por ferramentas de segurança as configurações e/ou regras precisam ser adaptadas de acordo com a ontologia. Para isso, a ontologia contribui ao identificar as relações entre ameaça, ativos, vulnerabilidades, mecanismos e propriedades de segurança.

Apesar dos trabalhos de Mozzaquatro proporem a concepção de um *framework* integrado ao projeto C2NET, eles não detalham esta integração, comprometendo o ciclo MAPE-K, ou seja, é possível destacar que eles são especialmente direcionados à base de conhecimento do ciclo. Os autores apenas mencionam que a utilização de ferramentas de segurança oferecem informações sobre diferentes tipos de alertas. Com isso, não são fornecidos detalhes sobre a implantação e interação entre as ferramentas. Consequen-

temente, não é possível afirmar maiores detalhes sobre os requisitos de escalabilidade e distribuição do *framework*. Reforçando isto, uma importante limitação destacada pelos autores em [Mozzaquatro et al. 2018] é a incapacidade de lidar com desafios reais visto a necessidade de adoção de uma avaliação contínua de risco adaptativo que vise permitir a tomada de decisões em tempo de execução com respostas adaptativas. Finalmente, destaca-se que a proposta não considera diferentes fontes de informações contextuais, sendo focada apenas em questões de segurança.

5.2.6. Ontology-based automation of security guidelines for smart homes

Em [Khan and Ndubuaku 2018], uma ontologia é proposta para representar o conhecimento sobre as diretrizes de segurança para interoperabilidade e entendimento entre os usuários de casas inteligentes. Além disso, uma ontologia baseada em contexto é desenvolvida, a qual se adapta às mudanças de informações contextuais, como as preferências do usuário e características do ambiente físico. Diferentes casos de uso criados com a linguagem de consulta SPARQL demonstram a aplicação de diretrizes de segurança em casas inteligentes e destacam como o contexto pode ajudar o usuário a executar essas diretrizes automaticamente.

A ontologia proposta, denominada *Cyber Security Guidelines Ontology* (CSGO), apresenta uma maneira padronizada de representar o conhecimento sobre as diretrizes de segurança para a implementação do usuário na casa inteligente. A ontologia foi proposta seguindo uma investigação de diretrizes de segurança de várias fontes. Na sequência, visando automatizar o processo de agir sobre essas diretrizes para ajudar o usuário a executar as diretrizes de segurança, os autores apresentam a ontologia baseada em contexto para incorporar o usuário, fornecendo assim subsídio para a automação do gerenciamento de segurança e o envolvimento do usuário para suportar uma modelagem incremental das diretrizes de segurança.

Ainda que seja prevista a execução automática e semiautomática de ações na ontologia, o trabalho não apresenta a integração da mesma em um *framework* para automação e análise em tempo de execução. Os autores ainda destacam a necessidade de implementar a automação proposta no cenário real. Além disso, eles mencionam a possibilidade de integração da CSGO com ontologias existentes e banco de dados de segurança externos para aplicações mais abrangentes. No entanto, ao empregar ontologias, é necessária uma preocupação quanto à distribuição do *framework* a ser proposto visando possíveis limitações de escalabilidade.

6. Discussão dos Trabalhos Selecionados

A tabela 2 ilustra a análise comparativa entre os projetos discutidos nesta seção. Visando otimizar o espaço ocupado pela tabela, os trabalhos foram identificados pelo sobrenome do primeiro autor e o respectivo ano de publicação. Os seguintes critérios foram considerados para nortear a discussão posteriormente apresentada:

- R1 - suporte à heterogeneidade pelas propostas;
- R2 - aderência ao ciclo de *feedback* MAPE-K;
- R3 - provimento de estratégias para aplicação de adaptações no ambiente;
- R4 - utilização de análise de risco como subsídio para tomada de decisão;

- R5 - estratégia utilizada para escolha da adaptação entre diferentes opções;
- R6 - área do estudo de caso;
- R7 - escalabilidade do modelo ou *framework*;
- R8 - possibilidade de distribuição da proposta;
- R9 - fontes de informações contextuais consideradas.

Tabela 2. Tabela comparativa

	EVESTI, 2014	RAMOS, 2015	AMAN, 2016	EL-MALIKI, 2016	MOZZA-QUATRO, 2018	KHAN, 2018
R1	Limitada	Sim	Limitada	Não	Sim	-
R2	MAPE-K	-	MAPE-K	MAPE	MAPE-**K**	K
R3	Não	Não	Limitada	Limitada	Limitada	Prevista
R4	Não	Não	Fórmula	-	Não	Não
R5	Conjuntos Fuzzy	-	Ontologia	-	Ontologia	Ontologia
R6	Ambientes Inteligentes	Não	eHealth	Redes de Sensores sem Fio	Indústria Me-talúrgica	Não
R7	Não	-	Não	Não	-	-
R8	Não	-	Sim	Não	-	-
R9	Segurança	Segurança	Usuário, QoS e Segurança	Usuário, QoS e Segurança	Segurança	Segurança

Por meio da análise da tabela, bem como pela descrição dos trabalhos, percebe-se que o suporte à heterogeneidade, ainda que contemplado por alguns trabalhos, apenas em [Aman 2016] são apresentados detalhes suficientes que permitem replicar o estudo e identificar os pontos fortes e fracos da abordagem realizada. Neste sentido, existe uma oportunidade nos *frameworks* para segurança adaptativa, especialmente na etapa de monitoramento do ciclo MAPE-K.

Reforçando esta afirmação, ao analisar o segundo requisito, aderência ao ciclo de *feedback*, ainda com exceção de [Aman 2016], apesar de a maioria dos trabalhos apresentarem em seu modelo as etapas MAPE, eles não fornecem especificações suficientes que permitam a replicação das avaliações ou ainda que possibilitem a prototipação fidedigna do modelo. É possível afirmar também que, em uma análise alto nível, visto até mesmo o da profundidade da descrição dos modelos, eles se assemelham em grande parte. Além disso, a maior parte dos trabalhos se restringe a detalhar as ontologias propostas, as quais se referem exclusivamente à base de conhecimento do ciclo.

Quanto ao fornecimento de estratégias que permitam a adaptação do ambiente da IoT, seja automático ou semiautomático, nenhum dos trabalhos contempla de maneira satisfatória esta propriedade. Ou seja, apesar dos trabalhos possuírem como objetivo o fornecimento de segurança adaptativa, parte deles suporta este requisito de forma limitada, por meio de scripts personalizados como em [Aman 2016] ou de códigos desenvolvidos especificamente para a avaliação [El-Maliki and Seigne 2016, Mozzaquatro et al. 2018].

A análise de risco, a qual deve nortear as adaptações a serem realizadas, também é fornecida apenas em [Aman 2016]. Ainda assim, a mesma não contempla informações contextuais externas, restringindo-se apenas ao cálculo do risco com base nos eventos analisados e nas regras especificadas.

No que diz respeito à estratégia adotada para escolha entre as diferentes opções de adaptação, a maior parte dos trabalhos tem empregado ontologias, abordagem também utilizada para base de conhecimento (K do ciclo MAPE-K). Contudo, percebe-se que um dos principais benefícios do uso de ontologias, o reuso, não tem sido efetivamente explorado [Mozzaquatro et al. 2018], tendo este aparentemente se tornado um problema na área [Caldarola and Rinaldi 2016]. A adoção de ontologias também implica em limitações de desempenho, o que pode inviabilizar a utilização das propostas em cenários da IoT.

De forma geral, percebe-se que não há um cenário específico para avaliação dos modelos, sendo geralmente utilizados os mais familiares a experiência adquirida pelos grupos de pesquisa e respectivas parcerias em projetos. Também observa-se a necessidade de propostas que contemplem a distribuição e a escalabilidade dos *frameworks*, possibilitando suas aplicações em cenários de crescente volume de dados, como na IoT.

Finalmente, outra oportunidade de pesquisa é a concepção de trabalhos que propiciem a resolução de conflitos em diferentes requisitos, sejam eles de segurança, dos usuários, entre outros. Por exemplo, em um cenário de ataque de força bruta em um *smartphone*, a solução de segurança adaptativa deve considerar: (i) no que diz respeito aos requisitos de segurança, as possibilidades de alterar o tamanho da senha utilizada, solicitar *captcha*, bloquear a conta por determinado tempo, entre outras; (ii) como preferências do usuário destaca-se a escolha pelo mesmo entre os diferentes tipos de autenticação como padrão (geralmente envolve desenhos formados pela ligação entre pontos), senha numérica ou impressão digital, além disto, o tamanho da senha escolhida; (iii) finalmente, no que tange a qualidade do serviço, o fato de que ao alterar algoritmos de criptografia ocorrerá um maior consumo de energia, ou ainda aumentar o tamanho da senha pode dificultar o sucesso ao acessar o dispositivo, em ambos os casos impactando na disponibilidade do ativo ao usuário.

A tabela 2 e a discussão apresentada forneceu subsídio para discutir e responder às questões estabelecidas nesta revisão:

- "(Q1) Quais os atuais desafios de segurança adaptativa em IoT?" - limitações das propostas discutidas ao analisar a tabela 2;
- "(Q2) Quais as estratégias utilizadas para avaliação das propostas?" - percebe-se que, em geral são utilizados estudos de caso em diferentes áreas da IoT;
- "(Q3) Quais as informações contextuais utilizadas para adaptações?" - muitos trabalhos exploram apenas o uso de requisitos de segurança, no entanto, novos estudos estão sendo desenvolvidos, indicando esta como uma questão ainda em aberto para novas pesquisas;
- "(Q4) Quais os mecanismos para escolha da adaptação considerando diferentes contextos?" - alguns trabalhos apresentam o uso de ontologias, porém, este também permanece um tópico a ser estudado explorando novos algoritmos.

7. Considerações Finais

O presente trabalho buscou apresentar uma revisão conceitual sobre segurança adaptativa ciente de contexto para IoT. No decorrer da revisão foi possível perceber os diferentes desafios existentes na IoT que potencializam a segurança da informação enquanto estratégia para viabilização dos inúmeros benefícios decorrentes deste paradigma.

Com isso, foi encaminhada a necessidade de modelos ou *frameworks* para segurança adaptativa que promovam a adaptação dinâmica dos mecanismos de segurança de forma que as mudanças aplicadas não prejudiquem a eficiência, a flexibilidade, a confiabilidade e a segurança dos ambientes da IoT. Tendo em vista a natureza pervasiva, distribuída e dinâmica da IoT, as informações contextuais devem ser um dos principais componentes para conduzir o comportamento dos dispositivos, a fim de tornar as decisões de segurança adequadas ao ambiente.

Atualmente, existem várias abordagens para segurança adaptativa. No entanto, muitas das abordagens desenvolvidas se concentram em objetivos de segurança específicos [Ferrera et al. 2016, Villarreal-Vasquez et al. 2017, Le et al. 2018]. Percebe-se também a falta no tratamento completo do ciclo de *feedback*, ou seja, as abordagens não definem todo o ciclo MAPE-K. Além disso, as arquiteturas genéricas analisadas não detalham os métodos usados em cada componente, o que dificulta a reutilização e a extensibilidade das abordagens propostas. Com a revisão sistemática realizada neste trabalho, foi possível identificar que apesar dos avanços nas pesquisas em segurança adaptativa em diferentes frentes, os desafios mencionados continuam em aberto, existindo ainda poucas abordagens genéricas que detalhem a sua concepção, prototipação e estratégias de avaliação.

Visando a continuidade desta pesquisa, destaca-se como trabalhos futuros: (i) determinar qual das possíveis oportunidades de pesquisa será considerada; (ii) estudar as possíveis estratégias a serem empregadas considerando o desafio elencado; (iii) conceber uma estratégia para tratar o problema; (iv) realizar a prototipação e testes da proposta concebida, e (v) reavaliar os trabalhos selecionados, comparando-os com o modelo proposto.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001 e da FAPERGS (Programa Pesquisador Gaúcho - PqG).

Referências

Aman, W. (2016). *Adaptive Security in the Internet of Things*. PhD thesis, Norwegian University of Science and Technology, Trondheim, Norway.

Bellavista, P., Corradi, A., Fanelli, M., and Foschini, L. (2012). A survey of context data distribution for mobile ubiquitous systems. *ACM Comput. Surv.*, 44(4):24:1–24:45.

Bernabe, J. B., Hernández, J. L., Moreno, M. V., and Gomez, A. F. S. (2014). Privacy-preserving security framework for a social-aware internet of things. In *Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services*, pages 408–415, Cham. Springer International Publishing.

Caldarola, E. G. and Rinaldi, A. M. (2016). An approach to ontology integration for ontology reuse. In *IEEE 17th International Conference on IRI*, pages 384–393.

Dey, A. K. (2001). Understanding and using context. *Personal and Ubiquitous Computing*, 5:4–7.

El-Maliki, T. and Seigne, J. M. (2016). Efficient security adaptation framework for internet of things. In *International Conference on CSCI*, pages 206–211.

Evesti, A. (2014). *Adaptive Security in Smart Spaces*. PhD thesis, University of Oulu.

Evesti, A., Abie, H., and Savola, R. (2014). Security measuring for self-adaptive security. In *Proceedings of the ECSAW*, pages 5:1–5:7, New York, NY, USA. ACM.

Evesti, A. and Frantti, T. (2015). Situational awareness for security adaptation in industrial control systems. In *2015 Seventh International Conference on Ubiquitous and Future Networks*, pages 1–6.

Ferrera, E., Rossini, R., Conzon, D., Tassone, S., and Pastrone, C. (2016). Adaptive security framework for resource-constrained internet-of-things platforms.

Giusto, D., Iera, A., Morabito, G., and Atzori, L. (2010). *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*. Springer New York.

Iglesia, D. G. D. L. and Weyns, D. (2015). Mape-k formal templates to rigorously design behaviors for self-adaptive systems. *ACM Trans. Auton. Adapt. Syst.*, 10(3):15:1–15:31.

Khan, Y. and Ndubuaku, M. (2018). Ontology-based automation of security guidelines for smart homes. volume 2018-January, pages 35–40.

Kliarsky, A. and Leune, K. (2017). Detecting attacks against the internet of things. *SANS Institute. InfoSec Reading Room*.

Le, A., Maple, C., and Watson, T. (2018). A profile-driven dynamic risk assessment framework for connected and autonomous vehicles. volume 2018.

Miorandi, D., Sicari, S., Pellegrini, F. D., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7):1497 – 1516.

Mozzaquatro, B. A., Agostinho, C., Goncalves, D., Martins, J., and Jardim-Goncalves, R. (2018). An ontology-based cybersecurity framework for the internet of things. *Sensors*, 18(9).

Ramos, J. L. H., Bernabe, J. B., and Skarmeta, A. F. (2015). Managing context information for adaptive security in iot environments. In *AINA Workshops*, pages 676–681. IEEE Computer Society.

Rochford, O. and Kavanagh, K. M. (2015). Magic quadrant for security information and event management. Technical report, Gartner Group.

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

Villarreal-Vasquez, M., Bhargava, B., and Angin, P. (2017). Adaptable safety and security in v2x systems. In *IEEE ICIOT*, pages 17–24.