Integração segura de redes sem fio heterogêneas através de Redes Definidas por Software

Cíntia Borges Margi
{cintia@usp.br}
Professor Doutor
Depto. de Eng. de Computação e Sistemas Digitais (PCS)
Escola Politécnica da Universidade de São Paulo (EPUSP)
2013

19 de junho de 2018

Resumo

As redes sem fio são tecnologias valiosas para o desenvolvimento de aplicações em diversas áreas, desde monitoramento ambiental a redes sociais. Características como mobilidade e heterogeneidade da rede e de dispositivos apresentam novos desafios a serem superados para a implantação de protocolos de comunicação.

Esta proposta possui como objetivo projetar e implementar protocolos que forneçam serviços básicos de segurança para redes sem fio heterogêneas, bem como de Redes de Sensores sem Fio, considerando o paradigma das redes definidas por software.

OpenFlow é o bloco básico no desenvolvimento desta proposta e, tanto quanto pudemos avaliar, é a primeira a tratar serviços de segurança nesse contexto. Nosso objetivo é incluir serviços como controle de admissão segura, autenticação de dados e confidencialidade tanto para usuários finais como para dispositivos OpenFlow.

Assim, teremos uma solução flexível, que facilite a adaptação de redes sem fio heterogêneas a possíveis mudanças de topologia e a reconfiguração para a execução de novas tarefas, garantindo os serviços de segurança associados.

Palavras-chave: redes de sensores sem fio, redes definidas por software, segurança, confidencialidade, autenticidade de dados.

Heterogeneous wireless networks secure integration through Software Defined Networks

Cíntia Borges Margi
{cintia@usp.br}
Department of Computer Engineering and Digital Systems
Escola Politécnica da Universidade de São Paulo (EPUSP)
2013

Resumo

Wireless networks in general are valuable technologies to develop and support applications in several areas, from environmental monitoring to social networks. Characteristics such as mobility and heterogeneity, both from the network as well as from the devices, present new challenges to communication protocols deployment.

Our main goal is to design and implement protocols to provide basic security services in heterogeneous wireless networks, as well as Wireless Sensor Networks, given the software defined network paradigm.

OpenFlow is a building block for this proposal and, to the best of our knowledge, is the first to consider these security services. Our goal is to include secure node admission control, confidentiality, data authenticity and integrity both for end users as well as OpenFlow devices.

Therefore, we will provide a flexible solution, which eases the heterogeneous wireless networks adaptation to topology changes and to task reconfiguration, while assuring the associated security services.

Keywords: wireless sensor networks, software defined networks, security, confidentiality, data authenticity.

1 Enunciado do problema

As redes sem fio em geral, e as de sensores em particular, são tecnologias valiosas para o desenvolvimento de aplicações em diversas áreas, como monitoramento ambiental [17], saúde [37] e redes sociais [3]. As redes de sensores sem fio (RSSFs) podem ser classificadas como um tipo especial de rede ad hoc de múltiplos saltos, já que apresentam características em comum com estas, mas possuem desafios adicionais a serem tratados, tais como fonte de energia e recursos computacionais limitados [5].

A diversidade das aplicações emergentes para redes sem fio vem tornando-as cada vez mais heterogêneas. Isto significa que uma única rede é constituída por diversas tecnologias de camada de enlace e física, e diferentes topologias, interligando muitos dispositivos com capacidades computacionais diferentes entre si e com a Internet, permitindo uma grande variedade de serviços [6].

Os dispositivos, ou nós, que compõem uma rede sem fio heterogênea, comumente utilizam diferentes sistemas operacionais e protocolos de comunicação, o que pode impor grandes desafios ao estabelecimento da interoperabilidade. Por exemplo, em uma rede heterogênea pode haver uma estação de trabalho, equipada com uma interface de rede sem fio no padrão IEEE 802.11 [11] rodando um sistema operacional Linux, que exibe para o usuário os dados coletados por um conjunto de sensores sem fio, equipados com módulos de rádio no padrão IEEE 802.15.4 [12] rodando o sistema operacional TinyOS [10].

Adicionalmente, as redes sem fio podem apresentar mobilidade, o que pode causar desconexões e mudanças na topologia, aumentando a dificuldade de estabelecer e manter rotas fim-a-fim e garantir a continuidade dos serviços.

Tanto a heterogeneidade de dispositivos quanto a mobilidade impactam diretamente no projeto de protocolos, dado que as arquiteturas de redes precisam ser dimensionadas para lidar com as diferentes capacidades dos dispositivos, diversos sistemas operacionais e protocolos, e com a possibilidade de desconexões.

Dadas as características das redes sem fio heterogêneas, que incluem as RSSFs, é complexo estabelecer soluções flexíveis, que facilitem a adaptação de uma rede deste tipo a possíveis mudanças de topologia e a reconfiguração para a execução de novas tarefas. Contudo, o conceito de redes definidas por software (ou *Software Defined Networks* - SDN) tem sido apontado como uma possível solução para prover a flexibilidade necessária [14] e aprimorar o gerenciamento das redes heterogêneas [23].

As redes definidas por software, ou especificamente o OpenFlow [20] que é um de seus principais exemplos, possibilitam a criação de aplicações que gerenciam os dispositivos de encaminhamento, permitindo o provisionamento de serviços de forma transparente para sistemas finais de diferentes tipos (dispositivos com diferentes combinações de capacidade de desempenho, sistema operacional, etc).

A principal ideia que suporta o conceito de redes definidas por software é dissociar o plano de dados do plano de controle a partir das seguintes medidas [23]:

1. remoção de decisões de controle dos nós de encaminhamento (ou nós intermediários),

2. permitir a programação dos nós de encaminhamento através de uma interface aberta, e

3. ter uma entidade separada chamada "controlador", que define por software o comportamento de toda a rede, configurando os fluxos de encaminhamento de dados em cada um dos nós encaminhadores, criando assim uma "rede definida por software".

As primeiras iniciativas de implementação de redes definidas por software tiveram como alvo as redes cabeadas, mas atualmente o conceito tem despertado interesse na comunidade de redes sem fio. De fato, a literatura já apresenta algumas discussões sobre a utilização de redes definidas por software no contexto das redes heterogêneas, como em [23], e propostas para o caso específico das RSSFs como os trabalhos Flow-Sensor [16], Sensor OpenFlow [14] e SDWN [4]. Ainda, um número crescente de empresas que desenvolvem soluções de comunicações sem fio e redes móveis vêm aderindo a iniciativas relacionadas às redes definidas por software [4].

O Flow-Sensor [16] foi a primeira iniciativa de aplicação do conceito das redes definidas por software sobre RSSFs. Trata-se de uma arquitetura que tem como único objetivo portar as funcionalidades básicas do OpenFlow para um cenário de RSSFs. A validação foi feita através de simulação e não foi apresentada uma análise da ferramenta funcionando sobre uma plataforma real. Em um artigo mais recente é feita uma avaliação do comportamento da arquitetura frente à mobilidade e ao estabelecimento de fluxos *multicast*, também limitado a simulação [15].

O Sensor OpenFlow [14] é uma arquitetura que tem como objetivo, além de aplicar as funcionalidades básicas do OpenFlow em RSSFs, adicionar a funcionalidade de programação do plano de dados pelo controlador. Esta arquitetura é composta por dois componentes, sendo um deles responsável pela separação do plano de dados do plano de controle, e o outro por estabelecer um protocolo de comunicação entre os dois planos. Os autores destacam os dois principais problemas que pretendem tratar a partir da adoção da abordagem: a subutilização dos recursos da RSSFs, que comumente são implantadas para a execução de uma única tarefa; e a contraprodutividade, promovendo o reuso de funcionalidades implementadas, o que acelera a prototipação. Além disso, apontam sua abordagem como uma solução mais avançada para o gerenciamento de RSSFs. No artigo não são apresentados detalhes de implementação ou análise de desempenho.

O SDWN [4] é uma proposta mais avançada que, além de incluir todos os recursos presentes no Sensor OpenFlow, prove outras funcionalidades importantes para as RSSFs, como agregação de dados na rede, definição de ciclos de trabalho, flexibilidade para definição de regras e ações que permitem otimizações *cross-layer*. A arquitetura define dois tipos de dispositivos: o nó genérico, no qual são instanciadas as tabelas de fluxos e aplicações que gerenciam as tarefas dos sensores; e o nó sorvedouro, composto por dois subsistemas, sendo um a interface de comunicação com os nós genéricos e o outro um sistema embarcado mais poderoso, que acumula as tarefas de controlador e virtualização da rede. Na época da publicação do artigo não havia implementação da arquitetura, agora, no período de elaboração desta proposta, o site do projeto (`http://www.diit.unict.it/users/gmorabi/sdwnWebSite/sdwn.html`) apresenta a descrição de um protótipo mas não há qualquer software disponível para download.

No contexto das RSSFs, o aumento do tráfego de dados de controle e o consequente aumento do consumo de energia são questões a serem tratadas. Uma possível abordagem para lidar com este desafio é a utilização de controle distribuído e a exploração da localidade como na proposta apresentada em [36]. Desta forma, seria possível aproximar os controladores dos nós controlados, utilizando nós líderes de grupo (ou *cluter heads*) como controladores, diminuindo assim o tráfego de dados de controle.

Um outro cenário interessante utilizando redes definidas por software sobre redes sem fio heterogêneas é o de extensão da área de cobertura ou compartilhamento de banda [23], ilustrado na Figura 1. Neste cenário um usuário (`Bob`) conectado a um ponto de acesso sem fio é utilizado como provedor de serviço (ou *gateway*) para outro usuário (`Alice`) que não possui conectividade, estendendo a área de cobertura de serviço. O usuário que se oferece como *gateway* poderia receber incentivos de provedores de serviço, como aumento da velocidade de conexão. Isso é possível devido à existência de aplicações "sobre o OpenFlow", as quais podem ser notificadas da existência de usuários que atuam como *gateways* e gerenciá-los.

Em um cenário tradicional, mesmo se assumirmos que a rede ad hoc aprende a rota para `Bob` como um *gateway*, e `Bob` permitir que seu dispositivo seja usado como um roteador por terceiros, o Provedor de Serviços de Internet não teria o conhecimento da existência de `Alice`, assim seria impossível a atribuição de maior largura de banda a `Bob` como incentivo pela prestação do serviço, o que possivelmente degradaria o desempenho de `Bob`. Além disso, o Provedor de Serviços de Internet não é capaz de diferenciar `Alice` de `Bob`, não podendo aplicar quaisquer regras de qualidade de serviço (ou QoS), restrição de acesso ou qualquer outro tipo de políticas a `Alice` sem também aplicá-la a `Bob`. Por fim, `Bob` seria responsabilizado pelo tráfego de `Alice` em caso de mal comportamento na rede ou atividade ilegal.

Fornecer serviços de segurança como confidencialidade e autenticidade dos dados é uma tarefa que se torna complicada ao se considerar as características das redes

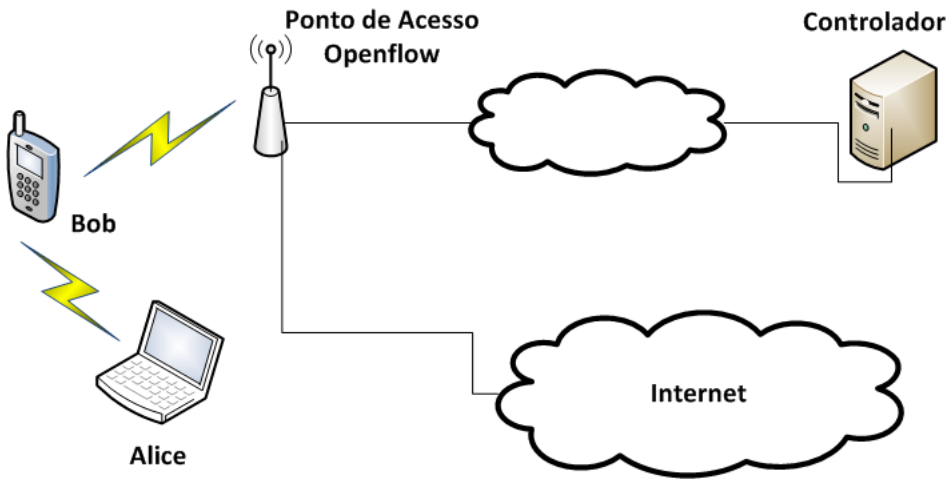

Figura 1: Extensão da área de cobertura do serviço em um cenário baseado em redes definidas por software sobre uma rede heterogênea.

heterogêneas e móveis. Além disso, a disposição dos nós em uma região geográfica não monitorada também facilita ataques de adversários [26].

Mendonça et al. [23] destacam que em uma rede não infraestruturada, como é o caso das redes sem fio heterogêneas, com dispositivos finais independentes que também atuam como nós de encaminhamento, pode ser difícil estabelecer a confiança e garantir canais fim-a-fim seguros, sendo necessário adotar um esquema de segurança com uma abordagem multi-camadas.

Além disso, os dispositivos da rede e os controladores devem descobrir uns aos outros sem o conhecimento prévio da topologia da rede. Desta forma, garantir a entrega das mensagens entre controladores e dispositivos com segurança não é suficiente, e ambos os terminais devem ser capazes de verificar a legitimidade uns dos outros, ou seja, antes de aceitar um controlador os nós de encaminhamento precisam ser capazes de confiar que o mesmo não é um adversário. Da mesma forma, o controlador deve ser capaz de confiar que os nós de encaminhamento que aceitaram o controle vão executar as tarefas a eles delegadas. Para esta confiança existir, os mecanismos devem garantir a legitimidade de nós e controladores, a autenticidade do controle de tráfego e a verificação que os dispositivos funcionem como esperado em resposta às instruções. Recentemente propusemos uma arquitetura de segurança para este tipo de cenário, atendendo a estes requisitos [33].

Para prover serviços de segurança sem a necessidade de uma infraestrutura de chave pública, que implica em custos de processamento e comunicação que inviabilizam sua adoção em RSSFs, um alternativa é o uso de métodos de *Authenticated Key-Agreement* (AKA) utilizando o protocolo SOK [30], como o TinyPBC [27]. Uma outra possibilidade inclui o uso de criptografia baseada em identidade (IBC - *Identity-based Cryptography*) e emparelhamentos para autenticação segura para *handover* de usuários em

redes sem fio [9].

Alguns trabalhos no contexto de redes de encaminhamento cooperativas (*cooperative relay networks*) utilizam-se de mecanismos de segurança associados ao protocolo de acesso ao meio [1] ou de camada física [13]. Contudo, essas soluções não são suficientes para o contexto das redes definidas por softwares pois não garantem a segurança fim-a-fim.

Além da segurança, no projeto de protocolo é importante considerar mecanismos que maximizem a confiabilidade da rede, no sentido de que se tenha o menor esforço para a entrega de dados para os controladores, com a premissa de que isso não represente impacto significativo no desempenho da rede. Entre os mecanismos possíveis para confiabilidade ou qualidade de serviço podemos destacar o uso de protocolos de roteamento multicaminho.

Em trabalhos anteriores, a proponente coordenou a pesquisa, projeto e desenvolvimento de aplicações de RSSFs para saúde [2], experimentos sobre consumo de energia em plataformas de RSSFs [18, 19], ferramenta para gerenciamento de energia em RSSFs [28, 29], arcabouço de segurança para RSSFs [25], análise de distribuição de chaves criptográficas em diversas topologias de RSSFs [26] e mecanismos para sobrevivência de dados em RSSFs [31, 32, 34, 35].

Esta proposta possui como objetivo projetar e implementar protocolos que forneçam serviços básicos de segurança em redes sem fio heterogêneas, bem como RSSFs, considerando o paradigma das redes definidas por software. Nossa proposta baseia-se principalmente no OpenFlow e, tanto quanto pudemos avaliar, é a primeira a tratar serviços de segurança nesse contexto. Nosso objetivo é incluir serviços como controle de admissão segura, autenticação de dados, e confidencialidade para os usuários finais e dispositivos OpenFlow. Tal proposta irá prover uma solução flexível, que facilite a adaptação de redes sem fio heterogêneas a possíveis mudanças de topologia e a reconfiguração para a execução de novas tarefas, garantindo os serviços de segurança associados.

Dadas as características típicas dos nós de RSSFs (fonte de energia e recursos computacionais limitados) todo o projeto de protocolos, mecanismos e software para estes ambientes deve ser otimizado para minimizar o consumo de energia, bem como o *overhead* de processamento e comunicação.

2 Resultados Esperados

Os resultados esperados para esta proposta possuem viés teórico, já que se propõe criar novos protocolos de rede e segurança, e prático, visto que é parte dos objetivo é associar os mecanismos aqui propostos a uma implantação em redes sem fio heterogênea, bem como RSSFs.

Inicialmente, serão executadas a implementação e a validação do protocolo já proposto para o cenário de compartilhamento de banda utilizando SDNs [33], bem como realização de testes e obtenção de métricas de desempenho utilizando a plataforma de testes a ser desenvolvida no modelo de redes definidas por software sobre Redes sem Fio.

Após a primeira implementação será projetado um novo protocolo tendo como plataforma alvo dispositivos com menor capacidade computacional, como módulos de RSSFs, outros dispositivos de Internet das Coisas (IoT - *Internet of Things*) e equipamentos de rede mais simples. Para validar a solução será necessário o estabelecimento de uma plataforma de testes, ou *testbed*, no modelo de redes definidas por software sobre Redes de Sensores sem Fio para execução de testes de provas de conceito e extração de métricas de desempenho. Dada a indisponibilidade de implementação de redes definidas por software para RSSFs, no momento de elaboração desta proposta, será necessário implementar uma solução de separação do plano de controle do plano de dados, utilizando tabelas de fluxos no formato do OpenFlow para a plataforma em questão.

Além disso, serão executados projeto e validação de um novo modelo comportamental e parametrizável para o padrão IEEE 802.15.4 [12], onde seja possível discriminar a existência de cada componente da rede na modelagem, de forma que a interação entre os nós fique explícita.

Por fim, um switch WiNoC (*Wireless NoC*), que tem potencial de facilitar a integração de RSSFs ao modelo de redes definidas por software, será projetado, implementado e validado.

3 Desafios científicos e tecnológicos e os meios e métodos para superá-los

Conforme discutido na Seção 1, a literatura apresenta algumas discussões sobre a utilização de redes definidas por software no contexto das redes heterogêneas [23] e propostas para o caso específico das RSSFs [16], [14] e [4].

Para o caso de utilização de redes definidas por software no contexto das redes heterogêneas [23], recentemente propusemos uma arquitetura de segurança para este tipo de cenário [33], atendendo a requisitos de garantia de legitimidade de nós e controladores, autenticidade do controle de tráfego e verificação de que os dispositivos funcionem como esperado em resposta às instruções. O próximo passo neste trabalho em colaboração é a implementação e experimentação da arquitetura proposta (primeiro item dos resultados esperados nesta proposta).

Com relação a propostas de utilização de redes definidas por software para o caso

específico das RSSFs [4, 14, 16], os trabalhos existentes até o presente momento não consideram os requisitos de segurança identificados [23] em seu projeto, e também não possuem implementações disponíveis.

Os Sistemas em chip (SOC - *System on a Chip*) são um conjunto de componentes eletrônicos acoplados em um único dispositivo com função dedicada. São utilizados em dispositivos embarcados, muitas vezes dotados de sensores e sendo aplicados em sistemas distribuídos. Com o objetivo de melhorar a infraestrutura tradicional de comunicação de SOCs baseada em barramentos, surge a ideia de NOCs (*Network on a Chip*) [24]. Diversos problemas associados a topologia e protocolos de comunicação em NoCs são próximos a problemas similares em RSSF. Ainda, a necessidade de implementar dispositivos embarcados capazes de realizar a integração do ambiente de RSSF a ambientes de rede tradionais, indica que o uso de SoCs e NoCs é bastante promissor.

3.1 Metodologia

Esta seção apresenta a metodologia que será adotada para cumprir o plano de trabalho e atingir os objetivos do projeto. Adicionalmente, apresenta-se um detalhamento das tarefas planejadas.

Para desenvolver o projeto e alcançar as metas propostas, o primeiro passo é realizar a revisão bibliográfica, de maneira a identificar o estado a arte e como as contribuições esperadas podem ser desenvolvidas. Em seguida, quando aplicável, realizar-se-ão testes iniciais, seguidos de análise comparativa dos seus resultados.

Após essas etapas iniciais, segue-se a elaboração da especificação dos protocolos ou mecanismos almejados. Em seguida, realiza-se a implementação, seguida de testes de desempenho, consumo de energia e alocação de memória. Finalmente, segue-se a implantação e experimentação em campo.

As principais atividades a serem executadas, com indicação dos principais envolvidos, são:

- Estabelecimento de uma plataforma de testes, ou *testbed*, no modelo de redes definidas por software sobre redes sem fio para execução de testes de provas de conceito e extração de métricas de desempenho.
  Envolvidos: Fulana (pesquisadora principal), WWWW (colaborador), XXXX (pesquisador associado), YYYY, ZZZZ, bolsista TT4A.

- Implementação do protocolo proposto em uma plataforma real, utilizando dispositivos sem fio de maior poder computacional, como *notebooks*, *desktops* e *smartphones*.
  Envolvidos: Fulana (pesquisadora principal), WWWW (colaborador), XXX (pesquisadora associada), YYYY, ZZZZ, bolsista TT4A.

- Testes da implementação e obtenção de métricas de desempenho utilizando a plataforma de testes.
  Envolvidos: Fulana (pesquisadora principal), WWWW (colaborador), XXXX (pesquisador associado), YYYY, ZZZZ, bolsista TT4A.

- Projeto de protocolo tendo como plataforma alvo dispositivos com menor capacidade computacional, como módulos de RSSFs, outros dispositivos de Internet das Coisas e equipamentos de rede mais simples.
  Envolvidos: Fulana (pesquisadora principal), ZZZZ, bolsista TT4A, bolsista TT1.

- Estabelecimento de uma plataforma de testes, ou *testbed*, no modelo de redes definidas por software sobre Redes de Sensores sem Fio para execução de testes de provas de conceito e extração de métricas de desempenho. Dada a indisponibilidade de implementação de redes definidas por software para RSSFs, no momento de elaboração desta proposta, será necessário implementar uma solução de separação do plano de controle do plano de dados, utilizando tabelas de fluxos no formato do OpenFlow para a plataforma em questão.
  Envolvidos: Fulana (pesquisadora principal), XXXX (pesquisador associado), ZZZZ, bolsista TT4A, bolsista TT1.

- Testes da implementação e obtenção de métricas de desempenho utilizando a plataforma de testes em RSSFs.
  Envolvidos: Fulana (pesquisadora principal), ZZZZ, bolsista TT4A, bolsista TT1.

- Projeto de um novo modelo comportamental e parametrizável para o padrão IEEE 802.15.4 [12] utilizando Redes de Petri.
  Envolvidos: Fulana (pesquisadora principal), TTTT.

- Validação através de simulações e medições do novo modelo comportamental e parametrizável para o padrão IEEE 802.15.4 [12] utilizando Redes de Petri.
  Envolvidos: Fulana (pesquisadora principal), TTTT.

- Projeto, especificação e testes de uma plataforma de simulação para WiNoCs.
  Envolvidos: Fulana (pesquisadora principal), UUUU.

- Projeto e implementação de switch WiNoC, com avaliação por meio do uso da plataforma de simulação desenvolvida.
  Envolvidos: Fulana (pesquisadora principal), VVVVV (pesquisador associado), UUUU.

3.2 Equipe

A equipe que desenvolverá este projeto será composta por:

- Profa. Dra. Fulana - coordenadora e pesquisadora principal do projeto;
- ...

Além destes participantes, solicitamos duas bolsas TT, sendo uma TT-4a e uma TT-1. Estes bolsistas terão papel importante no desenvolvimento e implementação da plataforma de testes no modelo de redes definidas por software sobre Redes de Sensores sem Fio.

3.3 Materiais

A implementação de aplicações, protocolos e mecanismos propostos será desenvolvida utilizando a *testbed* existente no LAB, grupo de pesquisa ao qual a proponente é vinculada. Esta *testbed* utiliza os nós sensores MicaZ [21] e TelosB [22], rodando os sistemas operacionais Contiki [7] e TinyOS [10], bem como os dispositivos Arduíno e .NET Gadgeteer com a placa FEZ Spider [8].

No entanto, os dispositivos existentes atualmente proveem suporte somente a parte correspondente a RSSFs. Para realizar testes com o controlador OpenFlow e a interligação a rede sem fio, será necessário a aquisição de notebooks, dispositivos RasperryPi e placas de redes sem fio padrão IEEE 802.11 e IEEE 802.15.4 (padrão das RSSFs), módulos que serão utilizados para fazer a integração entre as duas tecnologias de camadas de enlace e física.

Também será necessária a aquisição de um kit de desenvolvimento com FPGA de alta capacidade de células lógicas e memória, que será utilizada para a implementação e testes do switch WNoC. Também poderá ser utilizada no desenvolvimento do componente embarcado de integração de RSSF com controlador OpenFlow.

Os itens a serem adquiridos como material permanente e custeio estão identificados na Tabela 1.

Ainda, para facilitar o desenvolvimento do protótipo relativo ao trabalho em colaboração com WWWW, planeja-se duas viagens curtas de trabalho (15 dias cada). Também planejamos receber duas visitas de WWWW no período de execução do projeto.

Tabela 1: Material a ser adquirido.

Descrição	**Valor**
Material de Consumo	
2 Adaptadores de rede sem fio padrão IEEE 802.11b/g/n com suporte aos modos Ad-Hoc e Infra-estrutura para desktop	R$ 500,00
2 Adaptadores de rede sem fio padrão IEEE 802.11b/g/n com suporte aos modos Ad-Hoc e Infra-estrutura e conexão USB	R$ 500,00
3 Adaptadores de rede sem fio padrão IEEE 802.15.4 com conector USB	R$ 1.500,00
Material Permanente	
3 Notebooks - configuração igual ou superior a processador Intel Core i7, 4GB de RAM, 256GB SSD e tela de LED	R$ 12.000,00
1 Kit de desenvolviento com FPGA de alta capacidade de células lógicas e memória	R$ 12.000,00
5 Rasperry Pi modelo B	R$1.250,00
Total	R$ 27.750,00

4 Cronograma de Execução do Projeto

Este projeto tem duração prevista de 24 meses. Consideram-se os seguintes eventos principais:

1. Implementação do protocolo proposto [33] para uma plataforma real.
2. Estabelecimento de uma plataforma de testes no modelo de redes definidas por software sobre redes sem fio heterogêneas com dispositivos sem fio de maior poder computacional.
3. Testes da implementação e obtenção de métricas de desempenho utilizando a plataforma de testes.
4. Projeto e implementação de protocolo de segurança para RSSFs e Internet das Coisas utilizando o paradigma de redes definidas por software.
5. Estabelecimento de uma plataforma de testes no modelo de redes definidas por software sobre Redes de Sensores sem Fio.
6. Testes da implementação e obtenção de métricas de desempenho utilizando a plataforma de testes em RSSFs.
7. Projeto de um novo modelo comportamental e parametrizável para o padrão IEEE 802.15.4.

8. Validação do novo modelo comportamental e parametrizável para o padrão IEEE 802.15.4.

9. Projeto, especificação e testes de uma plataforma de simulação para WiNoCs.

10. Projeto, implementação e avaliação por simulação de switch WiNoC.

11. Elaboração de artigos para a divulgação dos resultados.

O cronograma de execução, associado aos eventos principais, é apresentado na Tabela 2.

Tabela 2: Cronograma de execução.

	Quadrimestre					
Tarefa	1	2	3	4	5	6
1	X	X				
2	X	X				
3		X	X			
4	X	X	X			
5				X	X	
6					X	X
7	X					
8	X	X				
9	X	X	X			
10	X	X	X			
11	X	X	X	X	X	X

Ao longo do projeto, artigos com os resultados obtidos serão submetidos para publicação em conferências e/ou periódicos relevantes à área. A escrita e envio de relatórios a Fapesp será realizada anualmente, conforme exigências do processo.

4.1 Colaborações e parcerias já estabelecidas

Parte importante neste projeto de pesquisa é a colaboração com WWWW. Este grupo destacou-se recentemente com diversos artigos relacionados a Redes Definidas por Software e cenários de interesse para sua aplicação. A contrapartida institucional esperada da colaboradora – infraestrutura e espaço físico – é plenamente atendida.

.....

4.2 Cronograma físico-financeiro

O cronograma físico-financeiro é apresentado na Tabela 3.

Tabela 3: Cronograma físico-financeiro.

Valor	**Ano**
Viagens e diárias	
Visita técnica a UCSC	
1 passagem para EUA - R$ 3.000,00	2014
15 diárias internacionais (US$250 cada)	2014
1 passagem para EUA - R$ 3.000,00	2015
15 diárias internacionais (US$250 cada)	2015
Pesquisador visitante no Brasil	
1 passagem a partir dos EUA - US$ 1.500,00	2014
5 diárias nacionais	2014
1 passagem a partir dos EUA - US$ 1.500,00	2015
5 diárias nacionais	2015
Material Permanente e Custeio	
3 Notebooks - R$ 12.000,00	2013
Placas de rede sem fio padrão IEEE 802.11 para desktop - R$ 500,00	2013
Placas de rede sem fio padrão IEEE 802.11 com conector USB - R$ 500,00	2013
Módulos de rede IEEE 802.15.4 com conector USB - R$ 1.500,00	2013
1 Kit de desenvolviento com FPGA - R$ 12.000,00	2013
5 Rasperry Pi modelo B- R$1.250,00	2013

5 Disseminação e avaliação

Os resultados obtidos ao longo deste projeto serão organizados em forma de artigos a serem submetidos a conferências e periódicos de relevância à área. Dentre estas conferências destacam-se ACM SIGCOMM, ACM SenSys, ACM MobiCom, IEEE Infocom, IEEE MASS, IEEE SECON e no âmbito nacional SBRC e SBrT.

Além de publicações, os resultados também serão disseminados através de seminários de pesquisa na própria instituição.

As métricas utilizadas para avaliação dos mecanismos propostos incluem tempo de execução, consumo de energia, atraso inserido na aplicação pelo uso do mesmo, atraso e *overhead* introduzidos na comunicação entre os nós da RSSF. Sempre que viável, os resultados dos mecanismos propostos serão comparados com mecanismos existentes que possuam propósito similar.

5.1 Projeção da necessidade de solicitações complementares

Dada a expectativa de disseminação dos resultados do projeto, a equipe pretende participar de, pelo menos, três reuniões científicas ou tecnológicas, ao longo dos dois anos, para apresentar trabalho científico ligado ao projeto.

O custo estimado de cada viagem é de US$3.050,00, e inclui passagem aérea

(US$1.500,00), taxa de inscrição em conferência (US$600,00), seguro saúde (conforme tabela vigente FAPESP US$50,00), e 4 (quatro) diárias (conforme tabela de diárias FAPESP, US$ 250,00 a diária).

6 Outros apoios

Informações de bolsistas do projeto removidas para preservar privacidade.

Referências

[1] H. Adam, W. Elmenreich, C. Bettstetter, and S.M. Senouci. Core-mac: A mac-protocol for cooperative relaying in wireless networks. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6, 2009.

[2] Renan C. A. Alves, Fabíola Santos, Bruno T. de Oliveira, and Cíntia B. Margi. Sistema de monitoramento de amplitude de movimento baseado em redes de sensores sem fio aplicado. In *Anais do VIII Simpósio Brasileiro de Sistemas de Informação (SBSI 2012)*, 2012.

[3] John G. Breslin, Stefan Decker, Manfred Hauswirth, Gearoid Hynes, Danh Le Phuoc, Alexandre Passant, Axel Polleres, Cornelius Rabsch, and Vinny Reynolds. Integrating social networks and sensor networks. In *W3C Workshop on the Future of Social Networking*, January 2009.

[4] Salvatore Costanzo, Laura Galluccio, Giacomo Morabito, and Sergio Palazzo. Software defined wireless networks: Unbridling sdns. In *Proceedings of the 2012 European Workshop on Software Defined Networking*, EWSDN '12, pages 1–6, Washington, DC, USA, 2012. IEEE Computer Society.

[5] David Culler, Deborah Estrin, and Mani Srivastava. Overview of sensor networks. *Computer Magazine*, 37(8):41–49, 2004.

[6] A. Delphinanto, T. Koonen, and F. den Hartog. End-to-end available bandwidth probing in heterogeneous ip home networks. In *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, pages 431–435, 2011.

[7] Adam Dunkels, Bjorn Gronvall, and Thiemo Voigt. Contiki - a lightweight and flexible operating system for tiny networked sensors. In *LCN '04: Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*, pages 455–462, Washington, DC, USA, 2004. IEEE Computer Society.

[8] GHI Electronics. Fez spider mainboard. `http://www.ghielectronics.com/catalog/product/269`, 2012.

[9] Daojing He, Chun Chen, S. Chan, and Jiajun Bu. Secure and efficient handover authentication based on bilinear pairing functions. *Wireless Communications, IEEE Transactions on*, 11(1):48–53, 2012.

[10] Jason Hill, Robert Szewczyk, Alec Woo, Seth Hollar, David Culler, and Kristofer Pister. System architecture directions for networked sensors. *SIGPLAN Notices*, 35(11):93–104, 2000.

[11] IEEE Standard. *IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Nov 1997. P802.11.

[12] IEEE Standard. IEEE 802.15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs), 2006.

[13] I. Krikidis, J.S. Thompson, and S. McLaughlin. Relay selection for secure cooperative networks with jamming. *Wireless Communications, IEEE Transactions on*, 8(10):5003–5011, 2009.

[14] Tie Luo, Hwee-Pink Tan, and Tony Q. S. Quek. Sensor openflow: Enabling software-defined wireless sensor networks. *IEEE Communications Letters*, 16(11):1896–1899, 2012.

[15] A. Mahmud, T. Kanter, and R. Rahmani. Flow-sensor mobility and multicast support in internet of things' virtualization. In *ICT Convergence (ICTC), 2012 International Conference on*, pages 16–22, 2012.

[16] A. Mahmud and R. Rahmani. Exploitation of openflow in wireless sensor networks. In *Computer Science and Network Technology (ICCSNT), 2011 International Conference on*, volume 1, pages 594–600, 2011.

[17] Alan Mainwaring, Joseph Polastre, Robert Szewczyk, David Culler, and John Anderson. Wireless sensor networks for habitat monitoring. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pages 88–97, New York, NY, USA, 2002. ACM.

[18] Cíntia B. Margi, Bruno T. de Oliveira, Gustavo T. de Sousa, Marcos A. Simplicio Jr, Paulo S. L. M. Barreto, Tereza C. M. B. Carvalho, Mats Naslund, and Richard Gold. Impact of operating systems on wireless sensor networks (security) applications and testbeds. pages 1 –6, aug. 2010.

[19] Cintia Borges Margi. *Energy Consumption Trade-offs in Power Constrained Networks*. PhD thesis, University of California Santa Cruz, 2006.

[20] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74, March 2008.

[21] MEMSIC Inc. Micaz product details, 2012. 6020-0065-05 Rev A.

[22] MEMSIC Inc. telosb product details, 2012. 6020-0094-04 Rev B.

[23] Marc Mendonça, Bruno Astuto A. Nunes, Katia Obraczka, and Thiery Turletti. Software defined networking for heterogeneous networks. *IEEE COMSOC MMTC E-Letter*, 2013.

[24] Umit Y. Ogras, Jingcao Hu, and Radu Marculescu. Key research problems in NoC design: a holistic perspective. In *Proceedings of the 3rd IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis*, CODES+ISSS '05, pages 69–74, New York, NY, USA, 2005. ACM.

[25] Bruno T. Oliveira and Cintia B. Margi. WSN-ETESec: Criptografia fim-a-fim em redes de sensores sem fio. In *Anais do XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) - Trilha Principal e Salão de Ferramentas*, pages 930–937, 2012.

[26] Bruno T. Oliveira, Cintia B. Margi, and Wilson V. Ruggiero. Poster abstract: Topology and deployment impact on key distribution in wireless sensor networks. EWSN 2012 Poster and Demo Proceedings `http://ewsn12.disi.unitn.it/ewsn2012_poster_and_demo_proceedings.pdf`, Fevereiro 2012.

[27] L. B. Oliveira, D. F. Aranha, C. P. L. Gouvêa, M. Scott, D. F. Câmara, J. López, and R. Dahab. TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks. *Computer Communications*, 2010. To appear.

[28] André H. Pereira and Cintia B. Margi. EM: Energy management tool for wireless sensor networks. In *Anais do XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC) - Trilha Principal e Salão de Ferramentas*, pages 922–929, 2012.

[29] André Hahn Pereira and Cintia B. Margi. Energy management for wireless sensor networks. In *SenSys*, pages 329–330, 2012.

[30] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security (SCIS'00)*, pages 26–28, 2000.

[31] M.A.S. Santos and C.B. Margi. Design and implementation of data survival in unattended wireless sensor networks. In *Performance Computing and Communications Conference (IPCCC), 2011 IEEE 30th International*, pages 1 –6, nov. 2011.

[32] M.A.S. Santos and C.B. Margi. A secure multi-party protocol for sharing valuable information in public safety networks. In *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*, pages 935 –940, oct. 2011.

[33] Mateus A. S. Santos, Bruno T. de Oliveira, Cíntia B. Margi, Bruno Nunes, Thierry Turletti, and Katia Obraczka. Software-defined networking based capacity sharing in hybrid networks. In *Proceedings of Capacity Sharing Workshop (CSWS'13), In conjunction with ICNP'13*, May 2013.

[34] Mateus A. S. Santos and Cintia B. Margi. Tinysharing: Uma ferramenta para compartilhamento de segredos em redes de sensores sem fio. In *Salão de Ferramentas do Simpósio Brasileiro de Redes de Computadores (SBRC 2011)*, pages 949–956, 2011.

[35] Mateus A.S. Santos, Cintia B. Margi, M.A. Simplicio, Geovandro C.C.F. Pereira, and B.T. de Oliveira. Implementation of data survival in unattended wireless sensor networks using cryptography. In *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, pages 961 –967, oct. 2010.

[36] Stefan Schmid and Jukka Suomela. Exploiting locality in distributed SDN control. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, HotSDN '13, pages 121–126, New York, NY, USA, 2013. ACM.

[37] UVA Computer Science. AlarmNet - wireless sensor networks for smart healthcare. `http://www.cs.virginia.edu/wsn/medical/`, 2010.