Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

JONATHAN DOS SANTOS MARTINS

EXPLORAÇÃO DE VULNERABILIDADES EM REDES IOT

ASSIS-SP

2018

JONATHAN DOS SANTOS MARTINS

EXPLORAÇÃO DE VULNERABILIDADES EM REDES IOT

Exame de Qualificação do projeto de pesquisa apresentado ao Curso de BACHAREL EM CIÊNCIAS DA COMPUTAÇÃO do Instituto Municipal de Ensino Superior de Assis – IMESA e à Fundação Educacional do Município de Assis – FEMA, como requisito parcial para a obtenção do Certificado de Conclusão.

Orientando: Jonathan dos Santos Martins

Orientador: Prof. Me. Fábio Eder Cardoso

ASSIS-SP

2018

EXPLORAÇÃO DE VULNERABILIDADES EM REDES IOT

JONATHAN DOS SANTOS MARTINS

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____

Prof. Me. Fábio Eder Cardoso

Examinador: _____

Prof. Dr. Luiz Carlos Begosso

Assis/SP

2018

DEDICATÓRIA

Dedico este trabalho este trabalho as pessoas que me são mais próximas e queridas. Aos meus pais, Claudemir e Quitéria, a meu irmão Ryan e aos amigos que sempre me apoiaram, Alan, Thales, Rose e Juliana.

AGRADECIMENTOS

Primeiramente gostaria de agradecer minha família pelo apoio, pelas cobranças, aos meus pais por terem se esforçado para que eu e meu irmão tivéssemos a oportunidade de estudar e conquistar vidas dignas como as deles.

Agradecer também a meu orientador, o professor Fábio Eder Cardoso pelo auxilio na elaboração, desenvolvimento e conclusão deste trabalho e aos demais professores cujo os quais sem a ajuda não chegaria até esta etapa.

Por fim, mas não menos importante, gostaria também de agradecer aos colegas de curso, Pedro Foganholi, Abílio Leocadio, Carlos Roberto e Silvio Marcelino que muito me ajudaram nos momentos mais difíceis do curso e com quem dei boas risadas ao longo desses anos.

RESUMO

O presente trabalho faz uma análise das soluções relacionadas à segurança da informação na área de *Internet of Things* (IoT), devido à expansão da utilização deste paradigma nas últimas décadas por empresas dos mais variados setores da economia. Além de elencar as vulnerabilidades apresentadas pelo mesmo devido a suas peculiaridades e limitações, fatos que se apresentam como desafios a serem superados para que seu uso seja feito de forma mais ampla e eficaz garantindo a sua segurança sem que o desempenho dos serviços ofertados sofra grande impacto.

Palavra-chave: Iot; Vulnerabilidades; Segurança.

ABSTRACT

The present work analyzes the solutions related to information security in the area of Internet of Things (IoT), due to the expansion of the use of this paradigm in the last decades by companies of the most varied sectors of the economy. In addition to listing the vulnerabilities presented by it due to its peculiarities and limitations, facts that present themselves as challenges to be overcome so that their use is made in a broader and more effective way, guaranteeing their security without the performance of the services offered will suffer a great impact.

Keywords: Iot; Vulnerabilities; Security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

Iot – Internet das Coisas

RFID – Radio Frequency ID

SSL – Secure Socket Layer

DDoS – Distributed Denial of Service

IEEE – Institute of Electrical and Electronic Engineers

ITU – International Telecommunication Union

IETF – Internet Engineering Task Force

IPv4 – Internet Protocol Version 4

IPv6 – Internet Protocol Version 6

ETSI – European Telecommunications Standards Institute

IETF – Internet Engineering Task Force

NIST – National Institute of Standards and Technology

FTC – Federal Trade Commission

CES – Consumer Electronics Show

E2E – End-to-End

M2M – Machine-to-Machine

CTS – Clear to Send

RTS – Request to Send

RAM – Random Access Memory

ROM – Read Only Memory

RPL – Routing Protocol for Low Power and Lossy Networks

LLN – Low power and Lossy Networks

DAG - Directed Acyclic Graph

DODAG – Destinatin-Oriented Directed Acyclic Graph

DIO – DODAG Information Object

DIS – DODAG Information Solicitation

DAO – Destination Advertisement Object

SUMÁRIO

1. INTRODUÇÃO

Com o passar das últimas décadas o número de dispositivos conectados a rede vêm aumentando gradualmente graças ao avanço dos sistemas de comunicação sem fio, como por exemplo, *Wi-fi*, 4G, entre outros. Em geral estes dispositivos são utilizados de forma conjunta no monitoramento inteligente e no controle de aplicações. Tal cenário forma um paradigma conhecido como *Internet* das Coisas (*Internet of Things*), ou IoT (MIORANDI et al., 2012).

Sistemas IoT são multifacetados, pois incorporam vários tipos diferentes de tecnologias, padrões e serviços. Uma definição lógica para IoT foi realizada por Atzori et al (2010): uma infraestrutura de rede dinâmica com capacidades de autoconfiguração, que se baseia em protocolos de comunicação padronizados e interoperáveis, em que são atribuídas identidades a “coisas” físicas e virtuais, atributos físicos e personalidades virtuais. Tais coisas estão naturalmente integradas à internet e usam interfaces inteligentes para comunicação. As coisas, ou objetos, devem interagir trocando entre si as informações coletadas, reagindo aos estímulos do ambiente de forma autônoma e em certa medida o influenciando sem a ajuda humana. Sendo assim, para cumprir um objetivo, sistemas IoT podem fazer com que os mais variados tipos de arquiteturas, tecnologias e metodologias se comuniquem (GRIECO et al., 2014).

Porém o alto nível de heterogeneidade aliado a escala dos sistemas IoT possui um preço. O aumento no número de ameaças devido à constante interação, em qualquer combinação, entre máquinas, robôs e seres humanos. Devido a peculiaridades como o limitado poder de processamento, energia e memória dos dispositivos e os problemas de escalabilidade que surgem em decorrência da quantidade de entidades interconectadas, medidas de segurança utilizadas em redes tradicionais não podem ser diretamente aplicadas em *Internet* das Coisas. Portanto, faz-se necessário a criação de modelos de segurança, privacidade e validação confiáveis que se adaptem ao contexto de IoT (WANGHAM et al., 2013).

É importante frisar que em *Internet* das Coisas adaptação e autorregulação cumprem um papel importante, tendo que lidar com mudanças, tanto as esperadas quanto as inesperadas, em seu ambiente de trabalho. Portanto, questões de segurança devem ser tratadas com certo grau de flexibilidade, sendo assim, há a necessidade de fornecer

segurança incorporada aos dispositivos em conjunto com as soluções mais convencionais para que os parâmetros de proteção, privacidade, diagnostico, isolamento e contramedidas a respeito de violação sejam satisfeitos de forma dinâmica como destacado por Babar et al. (2011).

1.1. OBJETIVO

Com base no panorama acima apresentado, o presente trabalho tem por objetivos fazer um estudo das principais soluções relacionadas ao quesito segurança no contexto de IoT e um levantamento das vulnerabilidades mais comuns nos sistemas de *Interne*t das Coisas, tanto as que podem ser exploradas por atacantes externos quanto às que podem ser utilizadas por adversários em âmbito interno através de falhas de codificação (*exploits*).

Para que as demandas levantadas no presente trabalho sejam cumpridas, foram realizados testes de vulnerabilidade, e a partir de seus resultados feitas buscas por vulnerabilidades desconhecidas ou pouco exploradas.

1.2. JUSTIFICATIVA

A pesquisa na área de segurança em dispositivos de *internet* das coisas apresenta grande relevância devido à crescente adoção de soluções IoT por empresas de diferentes setores da economia, portanto, é imperativo que as vulnerabilidades de tais sistemas possam ser contornadas no intuito de garantir a integridade dos dados coletados, a privacidade de seus usuários e a confiabilidade nestas tecnologias.

1.3. MOTIVAÇÃO

As motivações para o presente trabalho são a atualidade do tema, *Internet of Things,* e a possibilidade de explorar diferentes tecnologias para alcançar padrões de segurança

satisfatórios no contexto de IoT, tendo em vista sua heterogeneidade e suas características próprias, como por exemplo, o menor poder de processamento, memória e fonte limitada de energia dos dispositivos, em comparação com os computadores tradicionais (ATZORI et al., 2010). Além de outros fatores que tornam necessário o desenvolvimento de tecnologias que incrementem os níveis de segurança sem que sistemas IoT percam eficiência e dinamismo.

1.4. PERSPECTIVA DE CONTRIBUIÇÃO

As possíveis contribuições deste trabalho são: com o apontamento das vulnerabilidades em IoT, trabalhos futuros nesta área podem ser desenvolvidos no intuito de sanar estas brechas, assim como a seleção dos métodos de segurança já existentes ou em desenvolvimento por parte de empresas, públicas e privadas, pode ser melhor desempenhada de acordo com os resultados obtidos em pesquisas como este trabalho.

1.5. METODOLOGIA

A pesquisa inicia com um levantamento bibliográfico a respeito de IoT e seus principais conceitos. Em seguida, a literatura acadêmica será consultada no que tange a questão da segurança nessa área em específico. A esta primeira etapa será dada grande ênfase para que sirva à construção de sólida base de conhecimento para que a progressão as próximas etapas seja feita de forma natural.

Para a etapa seguinte foi realizado um apontamento das vulnerabilidades mais comuns encontradas em IoT. Tanto as que podem ser exploradas por adversários externos quanto ameaças internas.

Ao término desta etapa, o próximo passo foi a realização de estudos de caso das soluções em segurança da informação em IoT que se fizerem disponíveis. A prática foi valiosa ao permitir a utilização dos conceitos estudados na primeira etapa do presente trabalho. Devido à questão orçamentária utilizou-se o Contiki, um sistema operacional de código aberto desenvolvido para aplicações sob o paradigma IoT, focado principalmente em dispositivos de baixo consumo de energia e pouca memória. Seu consumo de

memória RAM é de aproximadamente 10 Kbytes e de memória ROM 30 Kbytes (CONTIKI-OS, 2008).

Juntamente com o Contiki foi utilizado o Cooja que é um emulador de aplicações IoT que acompanha o sistema operacional, pois esta ferramenta permite a construção de topologias, escolha do modelo do dispositivo a ser emulado, dentre outras funcionalidades que possibilitam analisar o comportamento dos dispositivos na rede.

2. IOT – INTERNET DAS COISAS

2.1 HISTÓRIA DA IOT

A história da IoT tem início muito antes da *internet*, com seus fundamentos tendo sido construídos com a tecnologia *RFID – Radio Frequency Identification* que é utilizada em aplicações de identificação de lojas, caixas, roupas, etc. Segundo Minerva et al (2015), os princípios da tecnologia RFID, por sua vez, remontam a Segunda Guerra Mundial como forma de identificar se aviões captados por radar eram amigos ou inimigos. Seu método de funcionamento era o seguinte: ao captar o sinal de radar, o avião, deveria refletir o sinal de acordo com suas características, sistema passivo ou sistema ativo, o que permitiria ao radar compreender a que grupo o avião faria parte.

Após a guerra a tecnologia de rádio frequência se desenvolveu e encontrou usos mais cotidianos e em áreas mais comerciais, como por exemplo, etiquetas de RFID usadas em muitas lojas para evitar roubos (MINERVA et al., 2015).

No ano de 1973, o norte americano Charles Walton utilizou rádio frequência para criar um sistema de controle de acesso sem chaves. Seu sistema funcionava com um cartão que continha um *transponder*. Quando o cartão se aproximava da porta com o leitor de sinal, era feita a verificação de identidade e então a mesma era desbloqueada. Ainda nos 1970, o governo dos Estados Unidos realizou pesquisas com rádio frequência no *Los Alamos National Laboratory* no intuito de criar identificadores militares e apoiar a logistica de transporte e armazenamento de armas, em especial de armas nucleares. Sistemas RFID foram desenvolvidos para utilização em caminhões e portões, com *transponders* contendo identificações dos produtos transportados (MINERVA et al., 2015).

Por volta da mesma época foram desenvolvidos, nesse mesmo laboratório, para o gado produtos de rastreamento de baixa frequência(125 kHz). Tal sistema funcionava de forma passiva, ou seja, a resposta do *transponder* era dada com a energia do sinal recebido. (MINERVA et al, 2015).

No ano de 1999, foi inaugurado o Centro de Estudos *Auto-ID Center*, no *Massachusetts Institute of Technology* (MIT), que anos depois, em 2003, passou a se chamar *Auto-ID Labs*. Segundo Minerva et al (2015), dois professores,David Brock e Sanjay Sarma, desempenharam importante trabalho neste centro de estudos no sentido de obter

etiquetas de RFID com *microchips* de custo mais baixo, permitindo a expansão desse sistema. Seus estudos tinham como objetivo conectar etiquetas RFID, que eles chamavam de "*tags"*, com a *internet* o que permitiria conhecer em tempo real a movimentação dos produtos. Este avanço conceitual e tecnológico fez com que tanto atores publicos quanto privados do mercado americano aderissem no suporte à pesquisa. A agitação causada pela relação entre RFID e conexões com a *internet* desencadearam o que viria a ser conhecido como *Internet* das Coisas. (MATTERN; FLOERKEMEIER., 2010).

Também no MIT em 1999, porém no laboratório *Media Lab*, Neil Gershenfeldt publica o livro *"When the things start to think"*. Alguns anos depois, em 2002, o pesquisador do *Auto-ID Center*, Kevin Ashton, usa o termo *"Internet of Things"* pela primeira vez (FACCIONI FILHO., 2016b). Deste ponto em diante o paradigma vai se consolidando cada vez mais, definindo suas caracteristicas e se concretizando, sendo que em 2008 ocorreu a primeira conferência internacional sobre o tema em Zurich, na Suiça – *First International Conference, IOT 2008*. No evento foram discutidos temas como sensoriamento, tecnologias de conexão, conversão de protocólos, aspectos de negócios e RFID.

2.2. CONCEITOS E DEFINIÇÕES

Segundo Faccioni Filho (2016b), a Internet das Coisas não é uma tecnologia e sim um paradigma, pois se utiliza das tecnologias para cumprir suas funcionalidades. Muitas tecnologias são associadas ao paradigma, como por exemplo, as que se referem à conexão sem fio. Como as funcionalidades IoT já estão presentes no mercado, seja por meio de tecnologias ou protocolos, afinal a tendência é que objetos já existentes sejam integrados à rede, várias empresas têm trabalhado em suas próprias linhas de dispositivos para Internet das Coisas. Segundo Skarpness (2014), esses equipamentos irão compor sistemas inteligentes, integrando bilhões de dispositivos, provendo soluções e análises de decisões fim a fim.

Por outro lado, o do desenvolvimento de aplicações, temos o surgimento das soluções *smart*, como *smart cities, smart buildings, smart grid*, e etc.(FACCIONI FILHO, 2015). No entanto, de acordo com Minerva et al,. (2015) é um domínio que integra diferentes

tecnologias, campos sociais e negócios. Devido a sua heterogeneidade de componentes não há uma definição exata de IoT, paradoxalmente a essa afirmação o paradigma abrange diversas áreas. Na base temos os componentes de “baixo nível” que se espalham pelos mais diversos ambientes. Nestes componentes existe um conjunto de *softwares* como, sistemas operacionais, bancos de dados, interfaces, protocolos de comunicação, sistemas em nuvem e aplicações. Essa camada, a de aplicação, é de extrema importância, pois nela é feito o tratamento de agentes autônomos capazes de autogestão e auto-identificação ao integrarem aplicações, devido ao grande número de componentes que uma plataforma IoT pode ter. Deste ponto advém questões de privacidade e segurança que são centrais em soluções comerciais e de fins estratégicos.

Segundo Faccioni Filho (2016a) para se chegar a uma definição mais acurada sobre IoT e diferenciá-lo de outros tipos de rede de sistemas interconectados podemos partir das características do objeto, ou “coisa”, que pode ser tanto algo físico quanto virtual. Ainda segundo Faccioni Filho (2016b) as funcionalidades de um objeto IoT são nove, porém estão distribuídas em três conjuntos: Características; Relações e Interface.

Vale ressaltar que nem todas as funcionalidades precisam, necessariamente, aparecer simultaneamente no objeto porque isso depende do seu fim e das aplicações em que estão envolvidos. No conjunto das Características encontraremos as atribuições do próprio objeto, como por exemplo, processamento, endereçamento, identificação, localização; no conjunto das Relações estão as funcionalidades que dizem respeito à forma como o objeto interage com outros objetos em rede, por exemplo, comunicação, cooperação, sensoriamento, atuação; e por fim, o conjunto de Interface abarca as funcionalidades que envolvem as relações entre objeto e usuário (FACCIONI FILHO., 2016b).

Observando o cenário acima exposto e considerando que a Internet das Coisas pode englobar sistemas com bilhões de objetos e interconexões, executando vários processos em inúmeros níveis, Minerva, Biru e Rotondi (2015, p. 75) propõem a seguinte definição para IoT:

> “A IoT – Internet of Things – compreende uma rede complexa, adaptativa e auto configurável, que interconecta “coisas” à Internet por meio de protocolos de comunicação normatizados. As “coisas” interconectadas têm representação física ou virtual no mundo digital, capacidade de atuação/sensoriamento, funcionalidade de programação e identificação única. Tal representação contém informações da identidade, status,

> localização e informações privadas ou sociais relevantes da “coisa”. A “coisa” oferece serviços, com ou sem intervenção humana, por meio de identificação única, coleta de dados, comunicação e capacidade de atuação. A exploração dos seus serviços se dá pelo uso de interfaces inteligentes e pode ser feita de qualquer lugar, a qualquer tempo e com segurança”.

Devido a sua a rápida expansão alguns problemas foram surgindo ao longo do desenvolvimento das soluções IoT. Talvez o exemplo mais notável seja o problema de identificação de dispositivos conectados a rede devido ao crescente número de aparelhos a se conectar todos os dias e com a chegada da Internet das Coisas uma nova leva de dispositivos busca se conectar e atuar.

A identificação dos dispositivos é feita através de endereços IP, tais endereços são gerenciados por um protocolo chamado *IPv4 – Internet Protocol Version 4* – que possui um limite máximo de 4,3 bilhões de endereços. No entanto esse número chegou ao fim em 2015, por isso a IETF – *Internet Engineering Task Force* – teve que formular um novo protocolo de identificação, o qual recebeu o nome de *IPv6*, *Internet Protocol Version* 6.

Este novo protocolo possui endereços formados por oito pacotes de 16 bits cada totalizando 128 bits escritos em dígitos hexadecimais, muito mais que seu antecessor que somava apenas 32 bits. Isso permite cerca de 3,4 x 10^3 endereços IP (FACCIONI FILHO., 2016), que é um número imensamente grande e o IoT tira proveito desses números para facilitar sua expansão.

Outro problema oriundo do desenvolvimento das soluções em Internet das Coisas é a questão da heterogeneidade de dispositivos, padrões e protocolos que operam nos sistemas. Por esse motivo faz-se necessário a padronização dos sistemas IoT para que os mesmos possam ser melhorados com freqüência e novas técnicas sejam desenvolvidas. De acordo com Minerva et al., (2015) varias organizações estão empenhadas em definir padrões e normas para Internet das Coisas, como por exemplo: IEEE, ETSI, ITU, IETF, NIST, W3C, entre outros.

2.3. ARQUITETURA IOT

Pelo fato de não ser exatamente uma tecnologia, a arquitetura IoT deve se basear num “consenso” entre as partes impactadas por sua aplicação. Por tal motivo muitas

organizações, institutos, grupos de pesquisa e afins buscam criar normas e padrões para a Internet das Coisas. Dentre as organizações empenhadas em normatizar o IoT, o ITU – *International Telecommunication Union* - estabeleceu bases técnicas para o paradigma em um documento publicado em 2012 chamado "*Recommendation ITU-T Y.2060*" (RECOMMENDATION ITU-T Y.2060., 2012).

Segundo este documento a IoT pode ser vista como tendo dois mundos: um mundo físico e um mundo digital. Cada coisa ou objeto do mundo físico pode ser representada no mundo digital como um elemento virtual, porém pode haver elementos virtuais sem correspondência com objetos do mundo físicos, como ilustrado pela figura 1, logo abaixo:

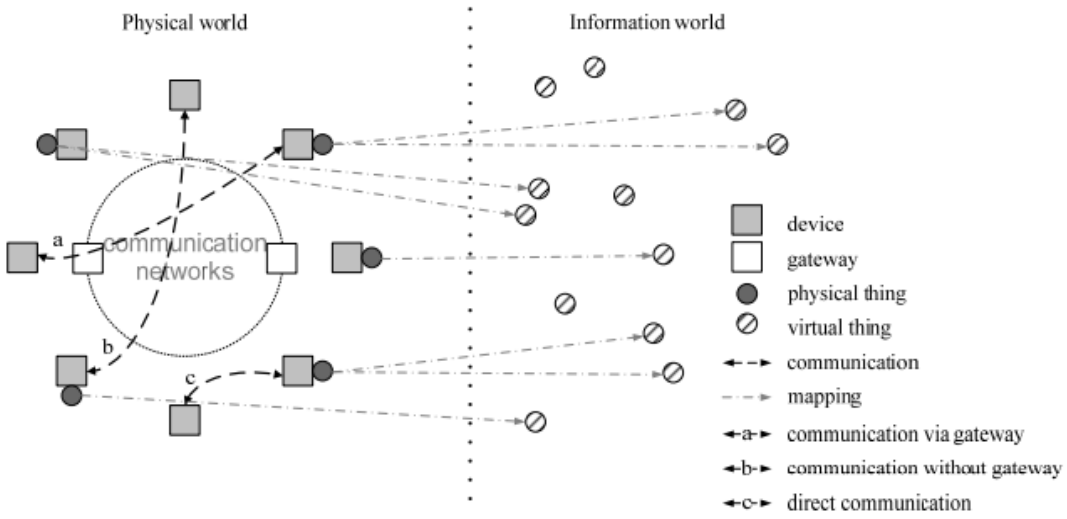

Figura 1: Visão técnica do IoT

Fonte: Recommendation ITU-T Y.2060, 2012, p.3

Uma peça importante nos sistemas IoT é o dispositivo. Dispositivos são objetos com capacidades de comunicação e capacidades opcionais de captura de dados, atuação, sensoriamento, memória e processamento. Estes objetos podem coletar a mais variada gama de informações e direcioná-la a redes de comunicação e informação para processamento futuro. Os dispositivos podem, basicamente, se comunicar de três formas, lembrando que a capacidade de comunicação é um requisito mínimo para que um dispositivo seja considerado parte do paradigma de Internet das Coisas: Caso a) através de *gateways* pela rede; caso b) pela rede sem o uso de *gateways*; e caso c) diretamente, sem passar pela rede de comunicação.

Ainda segundo as recomendações do ITU (RECOMMENDATION ITU-T Y.2060., 2012) os tipos de comunicação podem ser combinados de acordo com a necessidade de

manipulação do dispositivo. Para finalizar a parte dos dispositivos podemos dividi-los em quatro categorias de acordo com o ITU:

- Dispositivos de transporte de dados: Um dispositivo conectado a algo físico possibilitando a comunicação entre o mundo real e a rede de comunicação;

- Dispositivos de captura de dados: Dispositivo conectado ao objeto, capaz de ler dados e escrever informações no objeto;

- Dispositivo sensor ou atuador: Dispositivos capazes de captar informações do ambiente e transformá-las em sinais digitais, ou, transformar sinais digitais vindos da rede em operações;

- Dispositivo geral: Dispositivos com capacidade própria de processamento e comunicação seja com ou sem fio.

As redes de comunicação podem ser tanto redes existentes como redes TCP/IP ou novas gerações de redes que vierem a surgir, e sua função é a transferência de dados dos dispositivos para aplicações e para outros dispositivos e também trazer instruções de maneira confiável das aplicações para os dispositivos. (RECOMMENDATION ITU-T Y.2060., 2012).

As camadas da arquitetura de Internet das Coisas definidas pelo ITU são: Camada de aplicação; Camada de suporte a Serviços e Aplicações; Camada de rede e Camada de Dispositivos. As camadas são compreendidas em questão de gestão e segurança que garantem a estrutura das quatro camadas.

O ITU, partindo do objeto, criou sua própria definição de IoT que se assenta em três princípios: a forma como as coisas interagem por meio de uma rede; as aplicações que usam as coisas, trocando dados e dando ordens; e o suporte para interação entre coisas e aplicações. A estrutura de camadas criada pelo ITU pode ser vista na figura 2:

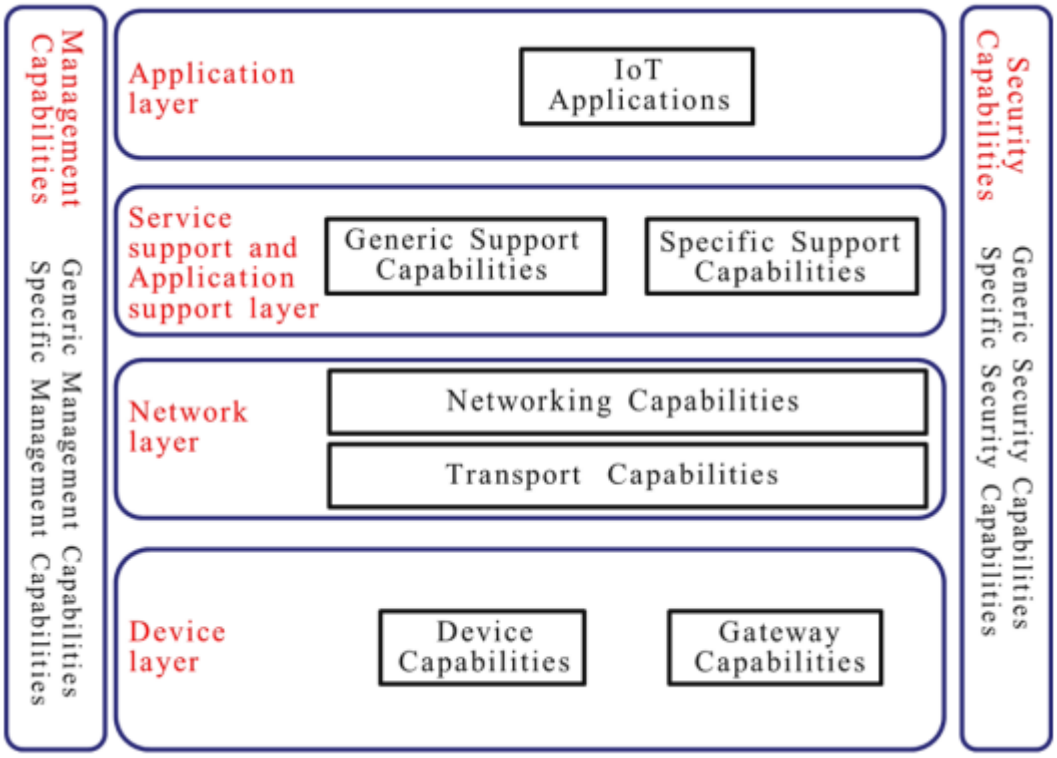

Figura 2: Camadas de arquitetura IoT

Fonte: Recommendation ITU-T Y.2060, 2012, p.7

Como demonstrado pela figura, às aplicações se encontram na camada de aplicação. A camada de suporte a Serviços e Aplicações se constitui de dois grupos de suporte a aplicações: as genéricas são funcionalidades comuns que podem ser usados por várias aplicações IoT e as especificas são funcionalidades com atribuições particulares, exclusivas para certas aplicações.

A camada de rede é composta por dois conjuntos de capacidades segundo o Recommendation ITU-T Y.2060 (2012): as redes de comunicação e o transporte de dados.

No primeiro conjunto estão as funcionalidades para controle de conectividade, como controle de acesso a rede, gestão da mobilidade, autenticação, contabilidade e autorização. Já o segundo conjunto apresenta funções focadas no transporte de dados de aplicações e serviços de IoT.

A camada de dispositivo também é composta por dois conjuntos de capacidades: as relacionadas aos dispositivos e as relacionadas a *gateways*.

As capacidades de dispositivo devem levar em conta as diversas funcionalidades que um dispositivo pode ter como, por exemplo, suas formas de comunicação, direta ou indireta, ou seja, com ou sem o uso de *gateway*, suas capacidades energéticas e etc.

As capacidades de gateway devem suportar diferentes interfaces e protocolos, garantindo à integração de diversos dispositivos a rede.

Quanto às capacidades de Gestão do IoT o Recommendation ITU-T Y.2060 (2012) as divide em dois grupos: genéricas e específicas.

As capacidades genéricas estão ligadas a gestão do dispositivo, sua ativação remota, atualização, diagnóstico, topologia de rede em que está inserido, status de funcionamento, tráfego na rede e aplicação de critérios para serviços críticos.

As capacidades específicas, por sua vez, estão associadas a questões específicas das aplicações.

Seguindo as recomendações do ITU as capacidades de Segurança em Internet das Coisas foram agrupadas em dois tipos: genéricas e específicas.

As capacidades genéricas foram subdivididas em três camadas e não dependem de aplicações:

- Camada de aplicação: responsável pela autorização, autenticação, confidencialidade, proteção e integridade dos dados, proteção da privacidade, auditoria da segurança e antivírus;

- Camada de rede: responsável pela autenticação, autorização, confidencialidade dos dados de uso e de sinalização, e pela proteção à integridade de sinalização;

- Camada de dispositivo: capacidades genéricas de autenticação, controle de acesso, proteção à integridade, confidencialidade de dados, autorização e validade da integridade do dispositivo.

Já as capacidades específicas de segurança são aquelas adotadas por aplicações com requisitos especiais como, por exemplo, aplicações de segurança patrimonial e pagamento móvel. (RECOMMENDATION ITU-T Y.2060, 2012).

No que tange a “coisa”, o objeto em si, que pode ser tanto um objeto físico quanto um objeto virtual as suas funcionalidades e características são o que definem, em essência, a Internet das Coisas. De acordo com Faccioni Filho (2016) são nove as atribuições de um

objeto IoT, porém se dividem em três conjuntos: Conjunto das Características, composto pelas características do próprio objeto; Conjunto das Relações, composto pela forma como o objeto interage com outros objetos na rede; Conjunto da Interface, composto pela relação entre objeto e interface.

No conjunto das Características estão as seguintes atribuições: Identificação, ou seja, cada objeto é único dentro do sistema IoT; Localização, o local especifico em que o objeto está; Endereçamento, capacidades do objeto de ser encontrado, de ser localizado por meio de roteamento; Processamento, capacidade de processamento contida no próprio objeto, tornando-o capaz de responder requisições da IoT e suas aplicações.

O conjunto das Relações é composto por: Cooperação, funcionalidades que permitem ao objeto agir em comum com outros objetos, buscando ações conjuntas e colaborativas; Atuação, funcionalidades que permitem ao objeto agir sobre o ambiente, modificando o meio; Sensoriamento, funcionalidades que possibilitem a captação de dados do ambiente ou de outros objetos por meio de sensores; Comunicação, a capacidade do objeto de receber e/ou enviar mensagens e dados para outros objetos na rede.

O ultimo conjunto, o de Interfaces, contém as funcionalidades relacionadas à interação entre o objeto e o usuário, o que o permite visualizar informações, fazer configurações sobre o objeto e modificar sua situação.

2.4. PROTOCOLO RPL

O protocolo RPL – *Routing Protocol for Low Power and Lossy Networks* – foi projetado pela IETF – *Internet Engineering Task Force* – para redes IPv6 de baixa potência com perda de pacotes (LLN – *Low power and Lossy Networks*). RPL é um protocolo de vetor da distância baseado em teoria dos grafos acíclicos formando assim um DAG (*Directed Acyclic Graph*), para ser mais específico, um DAG orientado ao destino, ou seja, um DODAG – *Destinatin-Oriented Directed Acyclic Graph*. Desta maneira os dados são direcionados a um nó da rede específico denominado raiz (GADDOUR,. 2012).

Segundo Gaddour (2012) o RPL foi pensado para as LLNs devido as suas especificidades, ou seja, para atender as baixas taxas de dados e as altas taxas de erros que tornam a vazão da rede baixa. Além disso, o protocolo precisa levar em conta os

períodos em que os nós ficam inacessíveis, obrigando-o a fornecer rotas alternativas às rotas anteriormente estabelecidas para que o fluxo de dados não seja interrompido.

O RPL se comunica por meio das seguintes mensagens de controle (GADDOUR,. 2012):

- DIO (DODAG *Information Object*): Mensagem utilizada para definir e atualizar as rotas da rede. Nela estão contidos os parâmetros de configuração da rede, como por exemplo OF – *Object Function* - e *rank*;

- DIS (DODAG *Information Solicitation*): Mensagem usada por um nó que ingressa na rede. Os nós que recebem uma mensagem DIS respondem a ela com uma mensagem DIO;

- DAO (*Destination Advertisement Object*): Esta mensagem é enviada pelos nós da rede ao nó raiz com o intuito de informar sua posição. Em alguns casos mensagens DAO podem requisitar confirmação de recebimento, o chamado DAO-ACK.

Na formação do DODAG o nó raiz envia um DIO para toda a rede, tal mensagem é composta por informações como *rank* e OF. OF é um algoritmo que tem por objetivo traduzir as métricas e padrões estabelecidos pelo desenvolvedor em um *rank* que será atribuído a cada nó. Cabe a OF também estabelecer como os nós selecionam seus pais e como otimizam as rotas em instancias RPL (GADDOUR,. 2012). O *rank* é utilizado para indicar a distância lógica entre um nó e o nó raiz. Desta forma o nó raiz terá sempre o menor valor da rede.

Segundo Gaddour (2012) cada nó recebe de seus vizinhos mensagens DIO e com base naquele que informou o menor *rank* escolhe um “pai preferido” que será utilizado para encaminhar os dados. Com base no pai e no OF o nó calcula para si um *rank* e o difunde por meio de mensagem DIO aos demais. Depois de todos terem se comunicado por meio de mensagens DIO, os nós encaminham ao nó raiz uma mensagem DAO para informar suas respectivas posições na rede. Ainda segundo Gaddour (2012) o tempo de atualização da rede é controlado por um algoritmo chamado *Trickle Timer* que aumenta o intervalo de tempo das mensagens de controle caso não ocorram eventos na rede, caso contrário, ou seja, haja alguma alteração na rede o tempo de troca de mensagens retorna ao mínimo.

2.5. TENDÊNCIAS DE MERCADO

Soluções IoT vêm ocupando cada vez mais espaço no cotidiano nos mais variados setores e assim como diversas entidades e instituições tentam encontrar padrões e normas para o paradigma, existem entidades que buscam realizar projeções de tendências relacionadas à área. Hoje, já podemos encontrar sistemas IoT em carros, sistemas de saúde, monitoramento de gado e muitos outros.

A *IEEE Communications Society – ComSoc* – sociedade ligada ao *IEEE – Institute of Electrical and Electronic Engineer* – Instituto responsável por estabelecer normas para as mais diversas tecnologias, tem se debruçado sobre o tema Internet das Coisas e estima que até 2020 cerca de 250 milhões de veículos estarão conectados a internet por meio de diversos serviços e aplicações e cerca de 50 bilhões de “coisas” estarão conectadas a rede. Nos próximos 20 anos, soluções IoT adicionarão quase 15 trilhões de dólares ao PIB global e por volta de 2024 às conexões M2M, Machine-to-Machine, poderão alcançar cerca de 24 bilhões de conexões anuais. (COMSOC, 2015).

Segundo Ahmed Bafana (2015), a Internet das Coisas é a terceira onda de desenvolvimento da internet, sendo as outras duas a expansão no numero de usuários nos 1990 e aumento do numero de celulares conectados a rede nos anos 2000. Para Bafana em 2020 cerca de 28 bilhões de “coisas” estarão conectados a redes de comunicação. Esse grande número de dispositivos aumentará também o número de ocorrências de acessos indevidos e invasão de privacidade no meio digital.

2.6. EXEMPLOS DE IOT

Alguns sistemas de Internet das Coisas já estão em atuação no mercado e nesta sessão serão contextualizadas de forma sucinta algumas delas para demonstrar como, embora IoT tenha ótimas projeções futuras, nesse exato momento vem galgando maior importância.

A primeira solução IoT que veremos será a M2M – Machine-to-Machine – tecnologia que se refere à comunicação entre máquinas ou entidades sem a intervenção do homem (MINERVA et al., 2015). Muitas aplicações possuem esses atributos e por isso M2M pode ser facilmente confundido com IoT em si.

A telemetria pode ser considerada uma das aplicações da M2M e refere-se à coleta de dados, a medição, ao controle e a comunicação com centrais de dados que serão analisados e parametrizados. Para a coleta se utiliza de interfaces em campo, convertendo os dados coletados em sinais digitais para transmissão. Embora seja anterior a IoT, a telemetria teve seu alcance ampliado devido à conexão com a Internet, fator que contribui para sua adoção nos mais variados empreendimentos (FACCIONI FILHO., 2016).

Outra tecnologia muito associada à Internet das Coisas são os *wearables* (“vestíveis”). Equipamentos incorporados a roupas e acessórios usados no dia a dia para praticas diversas. Exemplos destes dispositivos são relógios, óculos e outros acessórios que podem acessar aplicações e disponibilizar informações ao usuário rapidamente (FACCIONI FILHO., 2016).

Aplicativos que funcionam nesse tipo de dispositivo necessitam de capacidade de processamento e conectividade para atuar num ou mais conjuntos de produtos, como celulares, relógios e processadores em camisetas, tênis e etc.

Embora esteja muito associado à incorporação de tecnologia aos acessórios, Richmond (2013) afirma que os *wearables* podem ir além, se aproveitando de nanotecnologia para criar sistemas de processamento, incorporar *gadgets* e memória a sua própria estrutura.

Por ultimo será descrito o conceito de *Fog Computing* (Computação em névoa ou neblina). O conceito, em contraste com a computação em nuvem foi desenvolvido pela Cisco que o lançou junto com um sistema operacional para seus roteadores e *switches*. O foco da Névoa é distribuir a computação para a periferia da rede e mandar apenas anomalias ou processos específicos para a nuvem. A Névoa é uma camada intermediaria entre o objeto e a nuvem, o que permite a distribuição de inteligência dentro da rede (ALLEN, 2014).

Esse conceito nasceu devido ao grande volume de dados produzido a cada dia, o que pode tornar o processamento centralizado custoso demais, então a distribuição dos processos, pelo menos dos de baixo nível, pode ser feita aproveitando que as “coisas” incorporam funcionalidades de processamento, comunicação e armazenamento.

2.7. CONTIKI/COOJA

ContikiOS é um sistema operacional baseado em Ubuntu utilizado por desenvolvedores e pesquisadores na área de redes de sensores sem fio e IoT. O SO (Sistema Operacional) possui um simulador chamado Cooja capaz de executar simulações de dispositivos reais chamados *motes*, para, dessa forma o responsável pela rede pode testar suas limitações antes de realizar as implementações. A versatilidade do Contiki está no suporte a diversos protocolos como o RPL e o 6LoWPAN na camada de rede e o CoAP na camada de aplicação. Além disso, no site oficial do projeto (www.contiki-os.org) está disponível uma máquina virtual chamada *InstantContiki* para facilitar o aprendizado.

3. PENTEST (*PENETRATION TEST*)

3.1. CONCEITOS GERAIS

Nessa sessão será tratado de testes de invasão ou *pentests*, procedimentos realizados para a catalogação de vulnerabilidades. Tais procedimentos visam ataques simulados para explorar potenciais vulnerabilidades (MENEZES et al, 2015).

Pentests ajudam a avaliar quais vulnerabilidades podem ser exploradas e o grau de exposição da informação ou qual o nível de controle da rede um invasor poderia obter caso explore as vulnerabilidades com sucesso. Segundo Mallery (2009) as vulnerabilidades podem ser divididas em duas categorias, as físicas e as lógicas. As vulnerabilidades lógicas estão relacionadas à infraestrutura enquanto as físicas se relacionam ao acesso físico ao disco ou a dispositivos.

Os testes são divididos em internos e externos. Um teste é categorizado como externo se é conduzido fora do alcance da rede ou dos dispositivos, por exemplo, por meio de um servidor web. Por outro lado é categorizado como interno quando é realizado ao alcance da rede ou dos dispositivos. Além disso, existem algumas variações para estes testes que são conhecidas como: *White-Box*, *Gray-Box* e *Black-Box*. Segundo Mallery (2009) o que diferencia cada uma das variações é a quantidade de informação passada previamente ao responsável pelos testes. No *White-Box* são passadas informações sobre toda a estrutura da rede, dessa forma o *pentester* possui uma visão da rede similar ao administrador. No *Gray-Box* apenas algumas informações são disponibilizadas e o responsável pelos testes ganha nível de conhecimento similar ao de um funcionário por exemplo. Por fim, em testes *Black-Box* nenhuma informação sobre a rede ou empresa a ser testada é passada ao testador.

Em geral *pentests* são constituídos por três fases: pré-fase de ataque, fase de ataque, e fase de pós-ataque (MALLERY., 2009):

- Pré-fase de ataque: Essa fase caracteriza-se por varreduras e levantamentos. Nessa etapa é levantado o máximo de informações a respeito da rede e da instituição, como organização, funcionários e localização. Depois do reconhecimento ocorre uma varredura na rede para reconhecer os servidores, computadores e dispositivos conectados a ela, as portas abertas e seus sistemas operacionais;

- Fase de ataque: Nessa fase se tenta comprometer os alvos. Aqui as vulnerabilidades encontradas na fase anterior são atacadas para se testar todas as maneiras de um potencial invasor comprometer o sistema;

- Fase de pós-ataque: Esta fase é exclusiva de testes de invasão e tem por objetivo restaurar o sistema ao seu estado anterior a pré-fase.

3.2. PENTEST EM DISPOSITIVOS IOT

Apesar da diversidade de protocolos, arquiteturas e sistemas operacionais testes de invasão também podem ser empregados em dispositivos IoT. Entretanto, devido a essa diversidade a possibilidade de falha torna-se elevada e, além disso, faz-se necessário por parte do *pentester* alguns conhecimentos adicionais para explorar as potenciais vulnerabilidades encontradas.

Para que as chances de sucesso aumentem, os testes em dispositivos IoT devem englobar características de rede, *firmware*, aplicativos, analise de *hardware* e analise de criptografia (FRANCIS, 2017). Segundo Larry Towell (FRANCIS, 2017), consultor do *Synopsys Software Integrity Group* existem algumas habilidades indispensáveis para se investigar vulnerabilidades em sistemas IoT. Essas habilidades são:

1) Conhecimento a respeito dos protocolos de rede usados em IoT e quais as potenciais informações podem ser obtidas deles;
2) Conhecimento de testes de invasão em *web* para verificar se há vulnerabilidades em interfaces configuradas na mesma;
3) E por fim, conhecimento sobre engenharia reversa para decompilar o *firmware* e assim testar vulnerabilidades.

4. QUESTÕES DE SEGURANÇA EM IOT

4.1. CONTEXTO GERAL

A Internet das Coisas é um paradigma que não se limita apenas a esfera da tecnologia ou a impactar a sociedade do ponto de vista financeiro, mas também a mudar a forma como nós interagimos com a tecnologia em si (BANAFA., 2015). Da perspectiva da segurança e privacidade, o IoT, pode ser um paradigma um tanto “intrusivo” ao adicionar tantos dispositivos em ambientes antes considerados íntimos como casas, carros, roupas e até mesmo dispositivos cirurgicamente introduzidos no corpo ou ingeridos (BANAFA., 2015).

Segundo Banafa (2015) a má configuração de dispositivos como *Smartwatches* e outros *gadgets* já preocupa analistas de segurança, pois podem providenciar *backdoors* para acessos não autorizados a redes corporativas. Assim como seu número cresce exponencialmente sobe também a preocupação com aspectos de segurança, considerando a quantidade de dispositivos interconectados em espaços domésticos ou ambientes de trabalho, por exemplo, e que podem ter acesso a muito mais dados privados do que informações bancarias.

Edith Ramirez, ex-presidente do FTC – *Federal Trade Commission* – órgão norte americano responsável por realizar defesa do consumidor, desenvolver políticas de informação econômica, entre outras, expressou em 2015 durante a CES em Las Vegas sua preocupação com o limitado poder de processamento de muitos dispositivos conectados a rede o que inviabilizaria mecanismos de segurança mais eficientes, atualizações e a adoção de *patches* de correção (RANGER, 2015).

Embora as projeções de várias empresas apontem que o desenvolvimento do IoT trará retornos econômicos que podem chegar à casa do trilhão, à medida que seus dispositivos se proliferarem e seu uso for adotado, a superfície para potenciais ataques cibernéticos também tende a aumentar. Segundo Marc Blackmer (BURT, 2014), gerente de marketing e produtos para soluções industriais da Cisco durante a SECoT – *the security of things* - “mais dispositivos conectados, significa também maior número de dispositivos que precisam de proteção, e no geral sistemas IoT não são desenvolvidos para cyber-segurança”. Em sua exposição sugere ainda que a sofisticação dos criminosos virtuais

esteja cada vez maior e que a tendência é que violações de dados se tornem cada vez mais comuns (BANAFA., 2015).

À medida que a Internet das Coisas entra no mercado e em conseqüência nas nossas vidas, as preocupações com a segurança dos dispositivos vão se tornando mais e mais palpáveis. No Fórum Econômico Mundial de 2015, o então CEO do Google, Eric Schmidt disse que “logo haverá tantos dispositivos a nossa volta, a todo momento que nós nem mais os notaríamos” (SMITH., 2015).

4.2 REQUISITOS DE SEGURANÇA EM IOT

Como vimos nas seções anteriores, dispositivos IoT, conectam-se uns aos outros para prover serviços a qualquer hora e qualquer lugar. E muitos desses dispositivos não estão equipados com mecanismos de segurança eficiente e estão vulneráveis em vários pontos no que tange à segurança, privacidade, integridade dos dados, autenticidade e confidencialidade. Segundo Weber (2010) as redes IoT precisam preencher vários requisitos para se defender de agentes maliciosos. Ainda segundo o autor, quando se trata de segurança e privacidade a literatura recomenda as seguintes características:

- Resiliência a ataques: o sistema deve ser capaz de se recuperar de falhas durante a transmissão de dados;

- Autenticação dos dados: os dados e as informações devem ser autenticadas, ou seja, deve haver um mecanismo que permita que os dados sejam transmitidos apenas para dispositivos confiáveis;

- Controle de acesso: o acesso é dado apenas a pessoas autorizadas. O administrador do sistema deve controlar o acesso dos usuários gerenciando nomes de usuário e senhas para garantir a integridade dos níveis de acesso;

- Privacidade do cliente: os dados dos clientes devem ser acessados apenas por pessoal autorizado, ou seja, usuários sem o devido nível de acesso ou outros clientes não devem ter acesso a dados indevidos.

4.3. PRIVACIDADE, SEGURANÇA E AMEAÇAS

De acordo com Razzaq et al (2017), a maioria das ameaças a segurança estão relacionadas com vazamento de informações e indisponibilidade de serviço, porém em IoT as ameaças afetam diretamente o espaço físico. Como já vimos, sistemas IoT são compostos de vários dispositivos e plataformas com diferentes protocolos e credenciais e cada dispositivo precisa preencher requisitos de segurança que variam de acordo com suas características. Dentro deste contexto, manter a privacidade do usuário é uma tarefa muito importante, pois grande quantidade de informação pessoal é compartilhada entre esses dispositivos.

Além disso, muitos dispositivos se comunicam através de diferentes redes, o que implica em inúmeras questões de segurança condizentes à camada de rede e a privacidade do usuário. Para ilustrar o tema Razzaq et al (2017) apresentam alguns exemplos:

- E2E (*End-to-End*) Ciclo de proteção: Para garantir a segurança em ambientes IoT é necessário providenciar proteção para os dados na rede fim a fim, pois os dados são coletados por dispositivos diferentes interconectados e instantaneamente compartilhados com outros dispositivos. Portanto, é necessário algo, como um *framework*, que faça essa proteção, que gerencie o dado durante seu ciclo de vida para garantir a privacidade e a segurança;

- Planejamento de “coisas” seguras: A comunicação e conexão entre os dispositivos varia de acordo com a situação, entretanto, eles devem ser capazes de manter o nível de segurança. Os dispositivos de uma rede local ao se comunicarem com uma rede externa devem estabelecer contato por meio de políticas de segurança de mesmo nível;

- Segurança e privacidade visível/utilizável: Muitos dos problemas de segurança são causados por má configuração dos usuários, por isso faz-se necessário que políticas de segurança e privacidade sejam aplicadas automaticamente aos dispositivos ou que sejam de mais simples configuração.

A partir de agora serão analisados casos mais específicos, por exemplo, uma casa inteligente (*smart home*). Estes ambientes podem ficar expostos a uma gama de ataques devido à desconsideração dos parâmetros de segurança por parte das provedoras do

serviço desde o seu desenvolvimento inicial ou/e a má configuração por parte do usuário. Dentre as ameaças a segurança que tais sistemas estão sujeitos está espionagem, vazamento de informações, ataques coordenados de negação de serviço (DDoS), acesso de pessoal não autorizado, etc. (RAZZAQ et al., 2017). Vamos ver algumas ameaças em mais detalhes:

- De acordo com Razzaq et al (2017) a primeira ameaça a segurança é conhecida como “Transgressão”. No cenário em que as portas de uma casa estão conectadas a rede, se as mesmas forem afetadas por agentes maliciosos pessoas não autorizadas podem transgredir o ambiente sem a necessidade de arrombamentos físicos. Como conseqüência podem ocorrer roubos, assassinatos entre outros crimes;

- Outro problema que pode ocorrer é a utilização, por agentes maliciosos, dos sistemas de segurança, sensores e sistemas de monitoramento para ter acesso a informações intimas dos habitantes da casa. O intuito desse tipo de ataque poderia ser chantagem ou outro tipo de extorsão;

- Agressores podem realizar ataques de negação de serviço (DDoS/DoS), ou seja, acessar a rede de casas inteligentes e enviar mensagens em massa para os dispositivos inteligentes como, por exemplo, *Clear to Send (*CTS) e *Request to Send* (RTS). Os ataques também podem ter como alvo outros dispositivos conectados a rede da casa, porém o resultado é basicamente o mesmo, tornar o serviço indisponível através da drenagem dos recursos computacionais do sistema;

- Quando dispositivos de uma casa inteligente se comunicam com aplicações no servidor, hackers podem coletar pacotes de dados alterando as tabelas de roteamento. Se a técnica de SSL (*secure socket layer*) não for aplicada corretamente, certificados podem ser falsificados por invasores para obtenção de acesso.

Como pudemos observar, questões relacionadas à segurança são o principal desafio para a Internet das Coisas. Sua aplicação pode ocorrer nos mais diversos setores como empresarial, industrial, comercial e pessoal. No entanto, os dados coletados por essas aplicações devem estar seguros, devem garantir a confidencialidade contra roubos e adulterações (RAZZAQ et al,. 2017). Em sistemas IoT a preocupação não repousa apenas na transmissão dos dados entre os dispositivos, mas na forma como ela é feita pela internet, afinal muitas vezes estes dados podem cruzar fronteiras internacionais

podendo assim ficar sujeitos a atos de regulação de diferentes Estados. Segundo Razzaq et al (2017) os principais desafios no quesito segurança a serem discutidos são:

1) Privacidade dos dados: Garantir que os dados coletados sejam transmitidos pela rede sem comprometer a privacidade dos usuários, por exemplo, que os dados sobre os hábitos televisivos de usuários de *smart* TVs possam trafegar pela rede com sua privacidade assegurada;
2) Segurança dos dados: Enquanto a transmissão dos dados é feita perfeitamente faz-se necessário oculta-los de dispositivos de escuta na internet;
3) Preocupação com seguros: Empresas do segmento de seguros estão instalando dispositivos IoT para coletar dados a respeito da saúde e da forma como seus clientes dirigem para então decidir como proceder em caso de reivindicação de pagamento de seguros;
4) Falta de um padrão comum: Como existem vários padrões para dispositivos IoT e para a fabricação dos mesmos, torna-se difícil distinguir entre aqueles que são permitidos e os que não são permitidos na rede;
5) Preocupações técnicas: Devido ao aumento do uso de dispositivos IoT, conseqüentemente houve o aumento do trafego gerado por tais aparelhos. Portanto é necessário elevar não só a capacidade da rede, mas também a capacidade de armazenamento de dados para que os mesmos possam ser analisados;
6) Ataques de segurança e vulnerabilidades do sistema: Muitas coisas já foram feitas até o momento no cenário do IoT no quesito segurança. Esses trabalhos podem se subdividir em três principais pontos:
    a) Sistema de segurança: Este tipo de sistema foca principalmente em identificar problemas de segurança em cenários IoT, em desenvolver *frameworks* específicos para garantir segurança, proporcionar linhas gerais para manter a segurança da rede.
    b) Aplicações de segurança: Essas aplicações trabalham para lidar com questões de segurança de acordo com os requisitos do cenário.
    c) Segurança de rede: Segurança de rede lida com assegurar a comunicação entre dispositivos IoT de forma segura na rede.

4.4. VULNERABILIDADES DO PROTOCOLO RPL

O protocolo RPL possui características que o tornam suscetíveis a ameaças próprias como aquelas que exploram seu sistema de *rank* e outras já conhecidas em outros protocolos de roteamento como ataques de *blackhole*, *wormhole* e etc. (PONGLE,. 2015).

Segundo Pongle (2015) a exploração dessas vulnerabilidades pode levar desde a interceptação de pacotes a indisponibilidade do serviço por meio de DoS (*Denial of Service*). A introdução de nós maliciosos na rede pode acarretar diferentes tipos de ataques às mesmas, quer elas apresentem mobilidade ou não. Os ataques podem afetar não apenas a distribuição dos pacotes, diminuindo sua taxa de entrega, mas também aumentar as mensagens de controle e consumo de energia.

Os ataques mais comuns em redes RPL segundo Pongle (2015) são:

- *Wormhole*: neste tipo de ataque uma grande quantidade de mensagens segue apenas pelas rotas estabelecidas pelos nós maliciosos;

- *Blackholes*: neste ataque as mensagens são enviadas a um ou a um grupo de nós maliciosos e então são descartadas. Este tipo de ataque pode ser combinado com ataques de “rankeamento”;

- *Sybil*: neste ataque um nó invade a rede com uma identidade falsa e pode ser utilizado para realizar outros tipos de ataques como os descritos acima.

- Ataques de *rank*: os ataques de *rank* podem levar a duas conseqüências. Ou a elevação de *rank* dos nós maliciosos afetando assim o desempenho da rede principalmente nos pontos afetados, outro ataque de *rank* é a diminuição do *rank* dos nós afetados o que acarreta na escolha destes nós como “pais preferidos” dos demais, isto feito os nós maliciosos tem livre acesso as mensagens interceptadas como em ataques *blackhole*.

4.5. DIFERENTES NÍVEIS DE ATAQUE

Segundo Razzaq et al (2017) o IoT enfrenta vários tipos de ataques que podem ser divididos em ataques passivos e ataques ativos, que podem perturbar o funcionamento

dos serviços. Em ataques passivos, intrusos apenas detectam os nós da rede ou interceptam informações, porém sem atacar fisicamente. Já os ataques ativos perturbam fisicamente as atividades da rede e podem ser subdivididos em duas categorias: ataques externos e internos. Em comum esses ataques tem por objetivo impedir que os dispositivos se comuniquem de maneira inteligente, conseqüentemente medidas de segurança devem ser aplicadas para impedir tais ameaças.

De acordo com o comportamento e a natureza das ameaças é possível categorizá-las em quatro níveis (RAZZAQ et al,. 2017):

- Ataques de baixo nível: Quando um invasor tenta atacar uma rede e seu ataque não é bem sucedido;

- Ataques de nível médio: Quando um invasor ou espião consegue capturar informações sem alterar a integridade dos dados;

- Ataques de alto nível: Quando um invasor não só tem acesso a rede, mas também corrompe a integridade dos dados alterando-os;

- Ataques de altíssimo nível: Quando um invasor faz ataques a uma rede obtendo acesso não autorizado, executando operações ilegais, tornando a rede indisponível, enviando mensagens em massa ou bloqueando a rede.

5. EXPERIMENTOS

Com o intuito de buscar novas vulnerabilidades em redes IoT foram realizadas simulações no simulador Cooja. Os cenários de busca partiram de vulnerabilidades já conhecidas como o ataque de negação de serviço (DoS – *Denial of Service*) para explorar possíveis falhas não encontradas ou pouco conhecidas no protocolo RPL.

Os cenários investigados utilizam dois tipos de nós: o nó RPL-*collect sink* e o nó RPL-*collect sender*. O nó *sender* pode ser tanto o nó malicioso quanto os nós comuns da rede enquanto o nó *sink* é o alvo dos ataques. Neste tipo de ataque os atacantes enviam excessiva quantia de pacotes HELLO com o objetivo de comprometer a coleta de informações por parte do alvo.

Para as simulações de DoS à taxa de transmissão dos pacotes HELLO foi alterada de um pacote por minuto para um pacote por segundo assim que o usuário dispara um evento ao clicar com o botão direito do mouse.

No primeiro cenário de teste montou-se uma rede com doze nós, um nó *sink* (número 1), cinco nós *sender* maliciosos (números 2, 3, 4, 5 e 6) e seis nós *sender* (números 7, 8, 9, 10, 11 e 12) comuns. No segundo cenário o número de nós da rede foi mantido, porém o número de nós maliciosos e a topologia da rede foram modificados. Um nó *sink* (número 1), três são nós *sender* maliciosos (números 6, 11 e 12) e o restante são nós *senders* comuns (números 2, 3, 4, 5, 7, 8, 9 e 10). Ao terceiro cenário de simulações foi aplicado aos nós maliciosos o *plugin* de mobilidade do Cooja, chamado *Mobility*, para torná-los móveis. São doze nós dispostos em grade, um nó *sink* (número 1), nove nós comuns (4, 5, 6, 7, 8, 9, 10, 11 e 12) e dois nós maliciosos móveis (2 e 3). As topologias das redes estão ilustradas pelas figuras 3, 4 e 5.

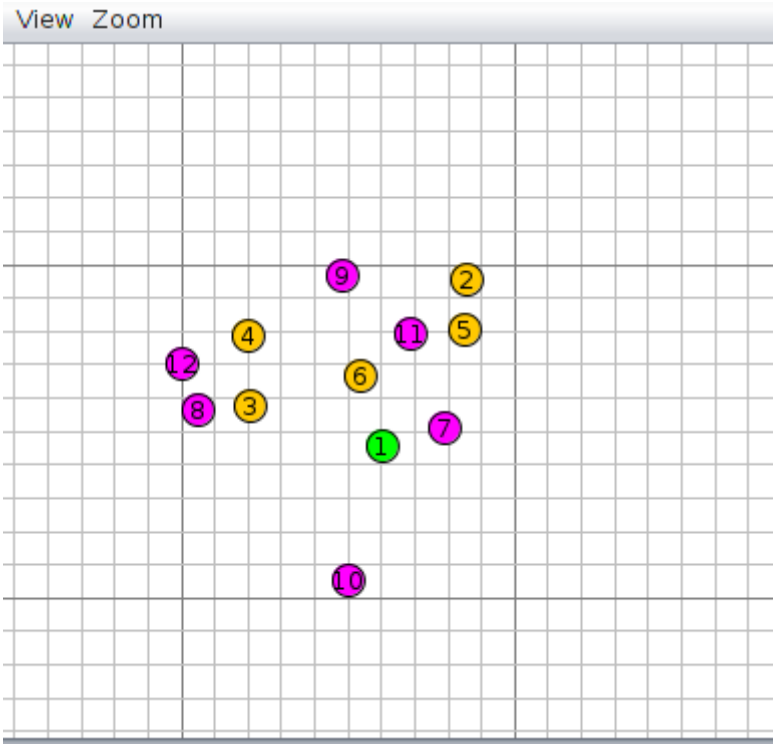

Figura 3: Topologia do cenário 1

Fonte: do Autor

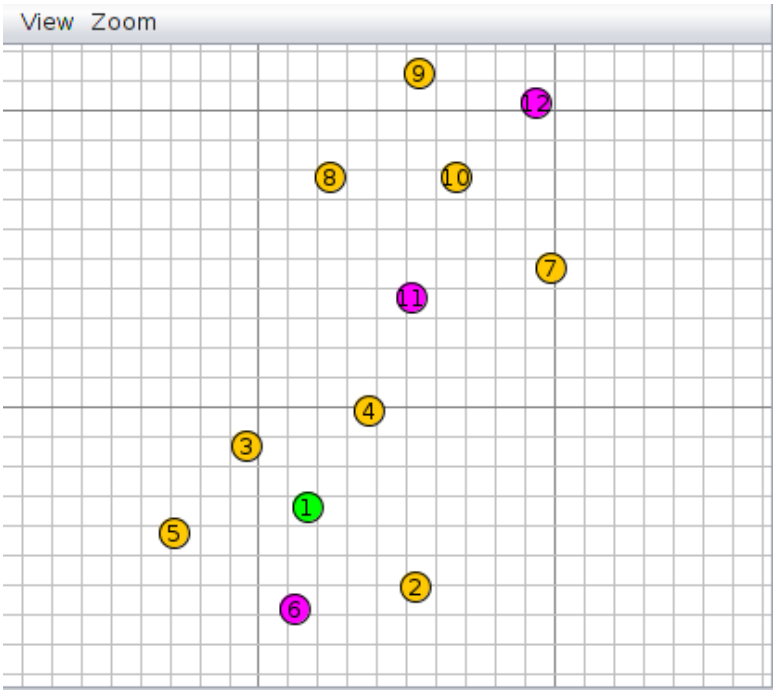

Figura 4: Topologia do cenário 2

Fonte: do Autor

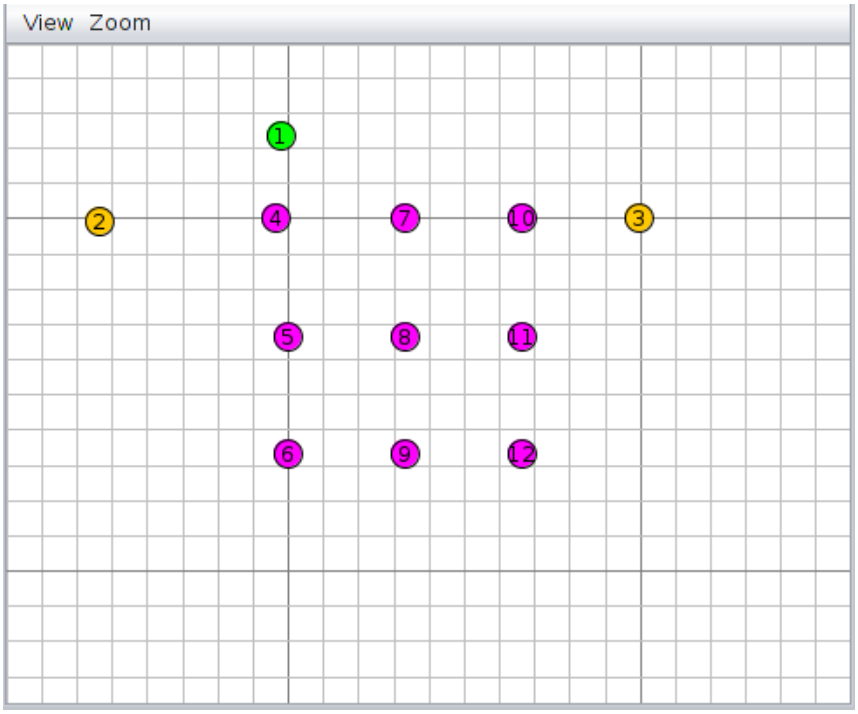

Figura 5: Topologia do cenário 3

Fonte: do Autor

O tempo das simulações foi calculado de acordo com o número de nós contido em cada uma. Para cada nó contou-se cinco minutos do tempo da rede operando normalmente, e o restante da simulação ocorre com a rede sob ataque até que ela pare ou até que um tempo igual ao de operação normal seja atingido. Desta maneira um cenário com doze nós é dividido em dois períodos, um com duração de sessenta minutos (uma hora) de operação normal e mais um de sessenta minutos sob ataque ou até que o serviço fique indisponível.

Para avaliação dos cenários propostos foram analisados os seguintes critérios: as métricas de roteamento, histórico de consumo médio de energia da rede, consumo médio de energia por nó, ciclo de rádio de cada nó, número estimado de pacotes recebidos e perdidos na rede e o número de pacotes recebidos por nó.

Em todas as simulações emulou-se o *tmote Sky* um sensor de potência ultra-baixa baseado no microcontrolador MSP430 (CONTIKI-OS, 2008). Devido ao objetivo de descobrir novas falhas a variação de topologias e posicionamento de nós maliciosos foi proposital para os experimentos.

5.1. RESULTADOS

Na avaliação dos impactos dos ataques a rede foram coletados dados de todos os nós sob dois contextos, fora de ataque e sob ataque, de tal maneira a avaliar os impactos sob cada ponto. O primeiro cenário contou com um período de uma hora de pré-ataque e trinta e dois minutos de ataque até ficar indisponível. Nos gráficos das figuras 6 e 7 pode-se observar o contraste do consumo de energia na rede entre os dois períodos. O maior consumo de energia se dá devido à elevação da taxa de envio de pacotes HELLO a ser processados e respondidos.

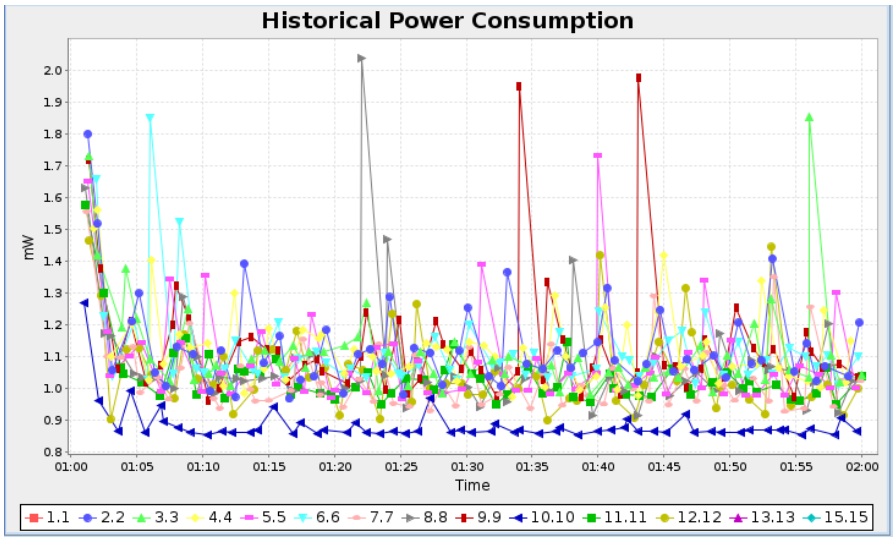

Figura 6: Histórico de consumo de energia pré-ataque, cenário 1

Fonte: do Autor

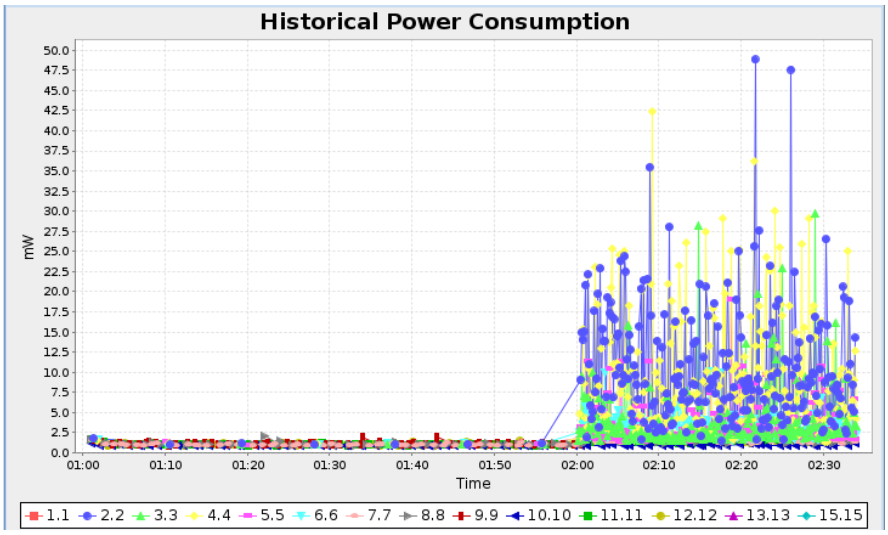

Figura 7: Histórico de consumo de energia durante ataque, cenário 1

Fonte: do Autor

Pode-se deduzir que os principais responsáveis pela alta no consumo são justamente os nós maliciosos, em especial aqueles que se encontram a uma maior distancia do nó raiz (*sink*), provavelmente em decorrência do maior número de saltos, como exemplificado pela comparação das figuras 8 e 9.

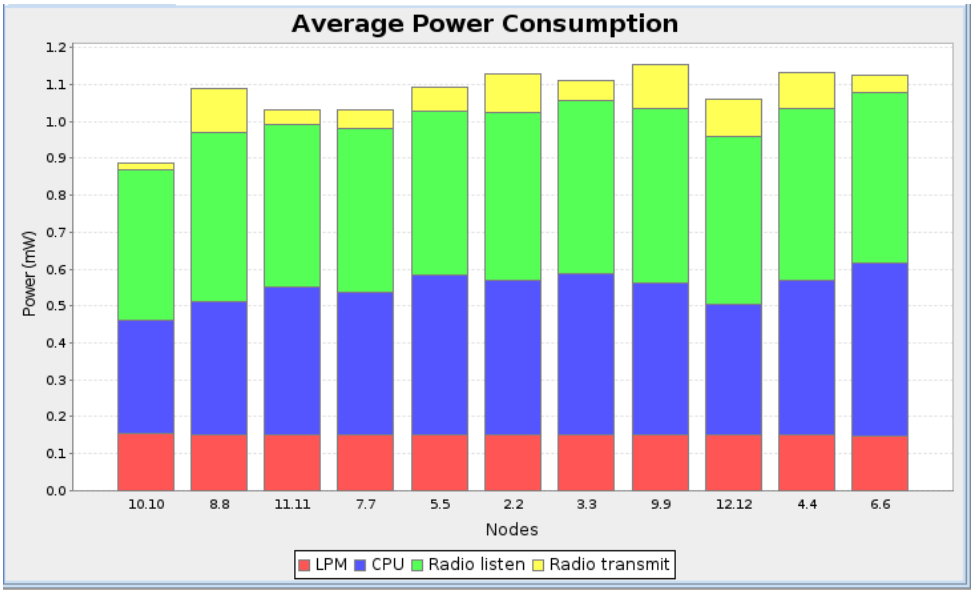

Figura 8: Consumo médio de energia pré-ataque, cenário 1

Fonte: do Autor

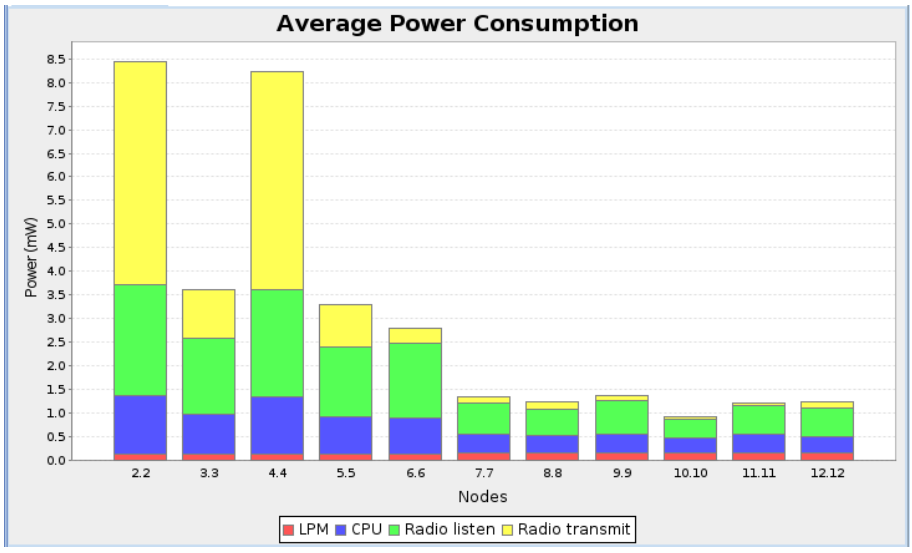

Figura 9: Consumo médio de energia durante ataque, cenário 1

Fonte: do Autor

Na figura 10 pode-se observar que a maior parte da energia gasta pelos nós antes do ataque esta na espera dos pacotes, com os nós mais distantes da raiz gastando mais energia na transmissão de rádio. Durante o período de ataque os nós maliciosos aumentam os gastos com transmissões enquanto os demais nós baixam as transmissões ao mínimo, como ilustrado pela figura 11.

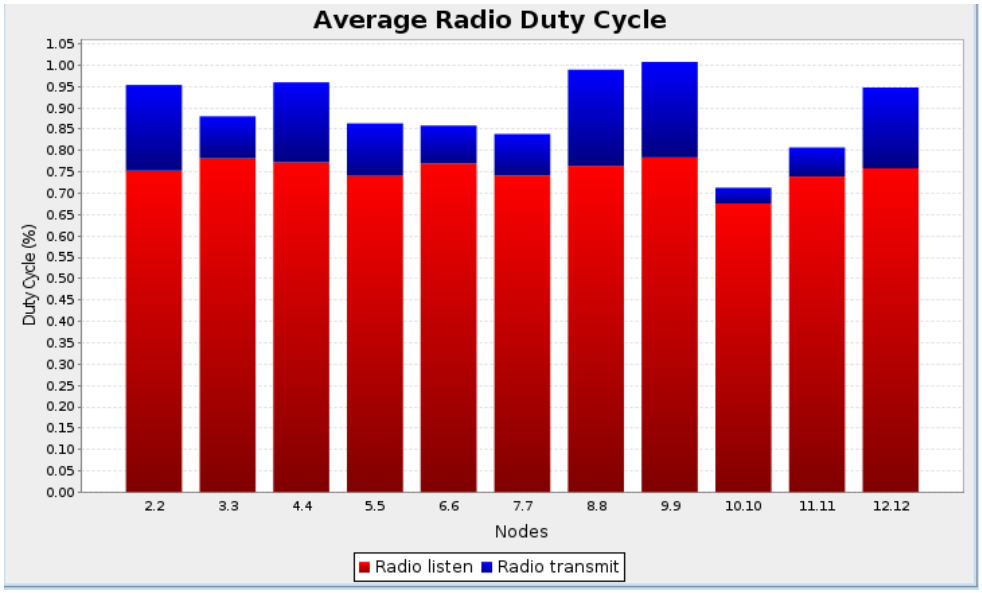

Figura 10: Média de ciclo de rádio pré-ataque, cenário 1

Fonte: do Autor

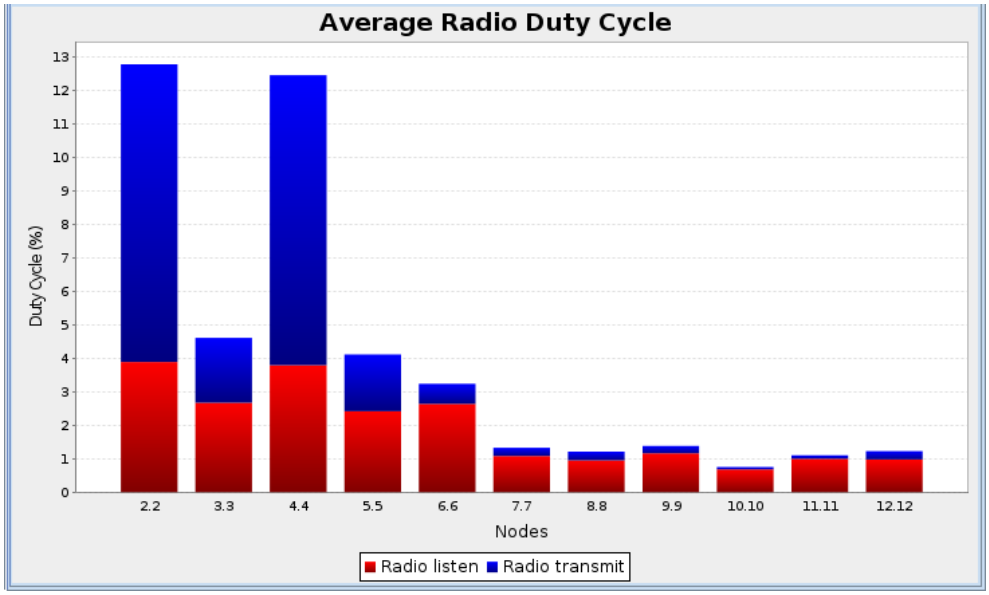

Figura 11: Média de ciclo de rádio durante ataque, cenário 1

Fonte: do Autor

Também devido à inundação de pacotes na rede as métricas de roteamento são alteradas constantemente durante o ataque, provavelmente isso se dá pelo fato dos nós comuns diminuírem a freqüência da transmissão de pacotes ao nó raiz que consequentemente atualiza a tabela de roteamento ao enviar mensagens DIO buscando otimizar as rotas de entrega. As figuras 12 e 13 ilustram as comparações entre as métricas de roteamento.

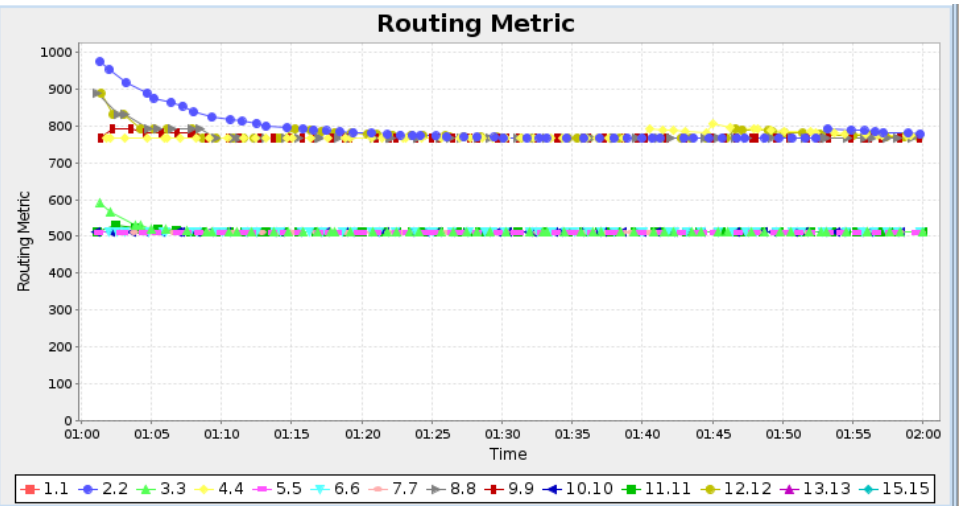

Figura 12: Métricas de roteamento pré-ataque, cenário 1

Fonte: do Autor

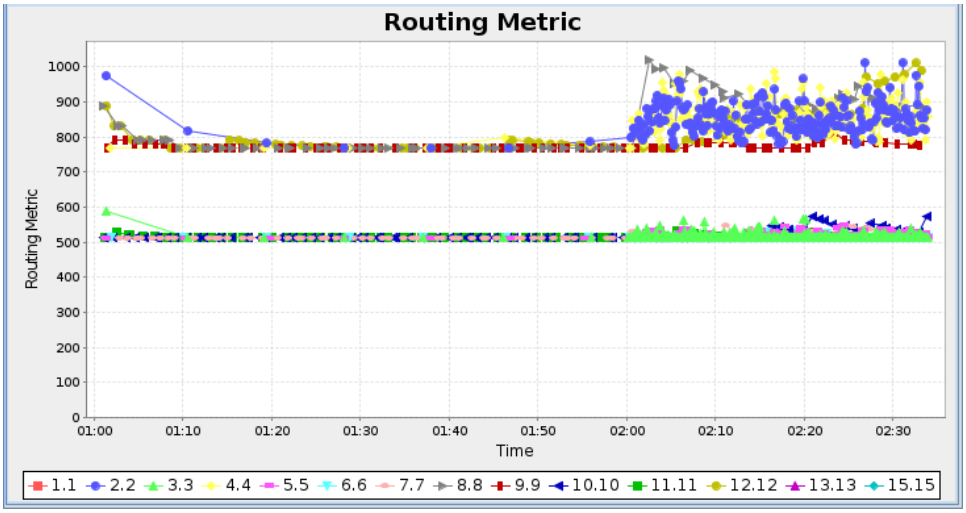

Figura 13: Métricas de roteamento durante ataque, cenário 1

Fonte: do Autor

Durante o período pré-ataque observou-se o recebimento estimado de seiscentos e quarenta e nove pacotes com nenhuma perda, como demonstra a figura 14. Depois do ataque, como ilustra a figura 15, o número estimado de pacotes subiu para cerca de dez

mil trezentos e setenta e oito pacotes com a estimativa de cento e sessenta e nove perdidos, uma taxa de perda de 1,62%.

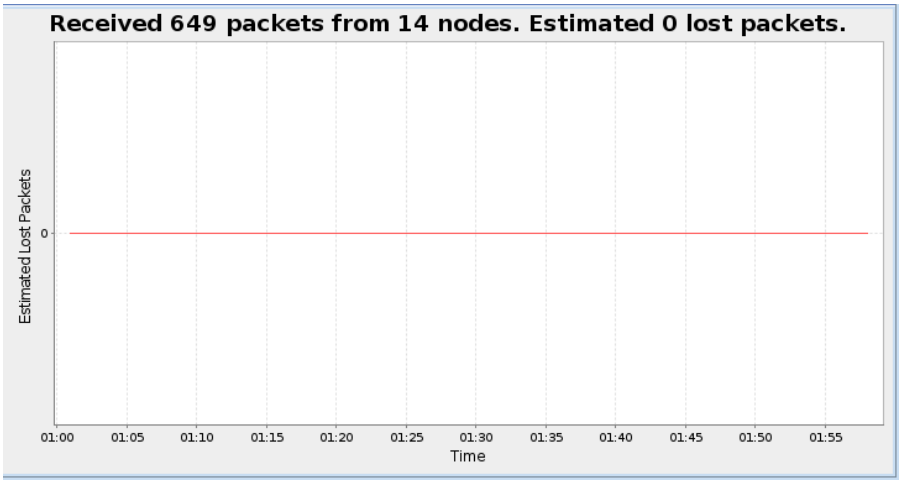

Figura 14: Estimativa de pacotes enviados e perdidos pré-ataque, cenário 1

Fonte: do Autor

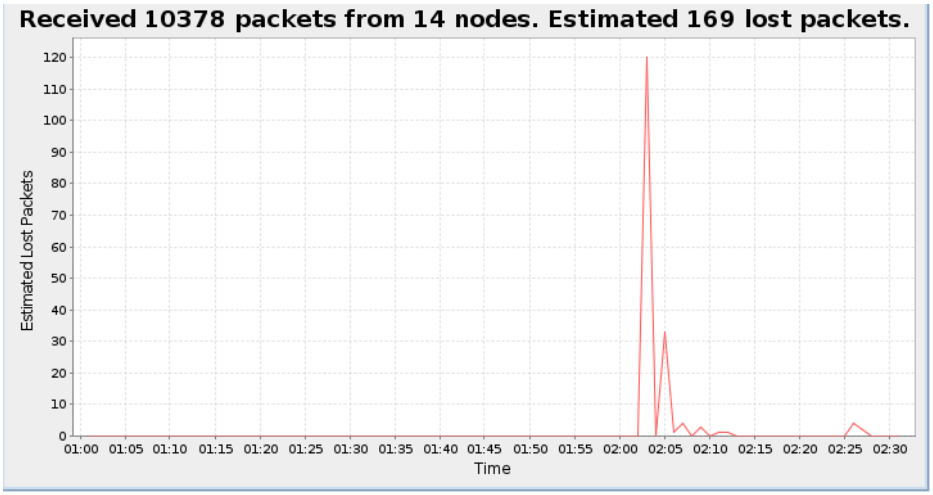

Figura 15: Estimativa de pacotes enviados e perdidos durante ataque, cenário 1

Fonte: do Autor

Ao avaliar a distribuição da carga entre os nós da rede em ambos cenários, constatou-se que antes do ataque a distribuição era homogênea por todos os pontos, em contrapartida, após o ataque os nós atacantes concentram maior parte da atividade, destacando-se em muito sobre os demais. Estes dados são ilustrados pelas figuras 16 e 17.

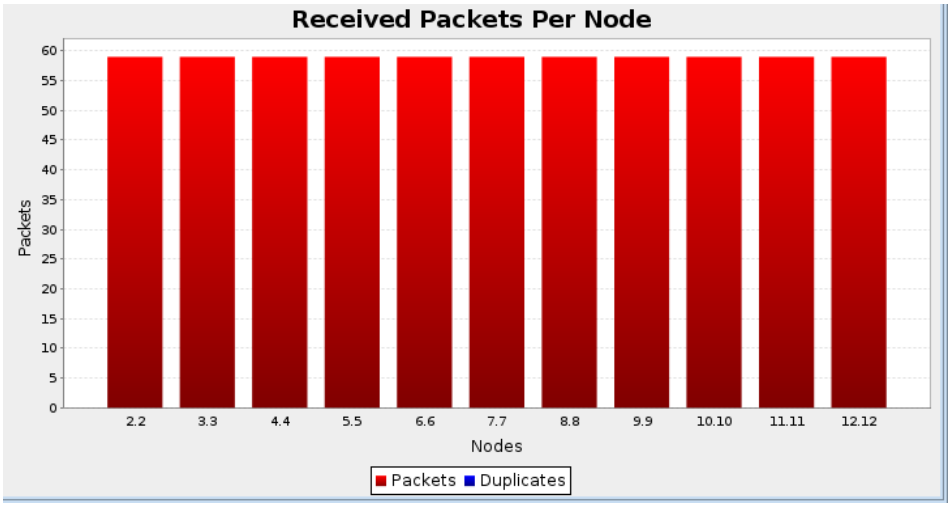

Figura 16: Pacotes recebidos por nó pré-ataque, cenário 1

Fonte: do Autor

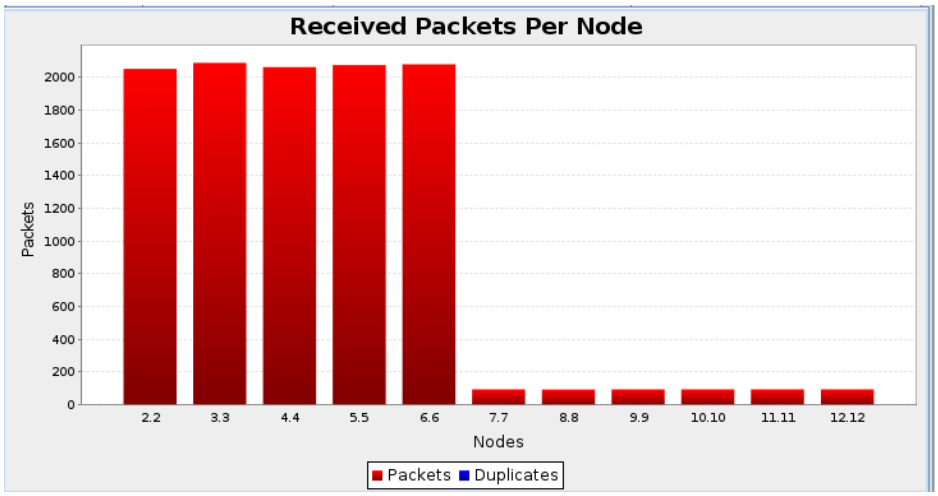

Figura 17: Pacotes recebidos por nó durante ataque, cenário 1

Fonte: do Autor

No segundo cenário é possível verificar tendência similar no quesito consumo energético com os nós maliciosos gastando mais recursos durante o ataque que os nós comuns, com o valor de consumo variando de acordo com a quantidade de pacotes transmitidos tanto que, devido à topologia formou-se uma rota passando pelos nós 12, 10, 11, e 4 até o nó raiz que elevou o consumo energético dos nós 10 e 4 que não são maliciosos, como ilustrado pelas figuras 18 e 19.

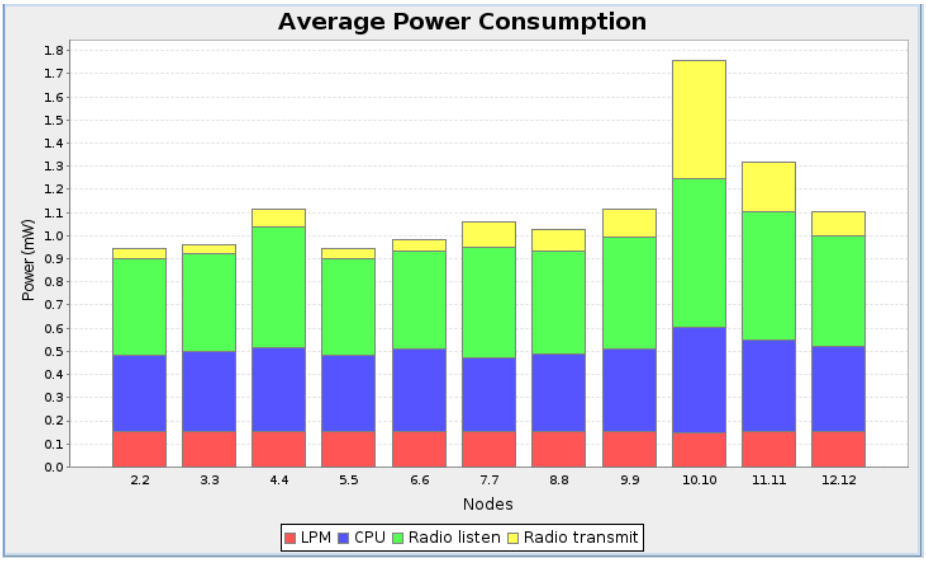

Figura 18: Consumo médio de energia pré-ataque, cenário 2

Fonte: do Autor

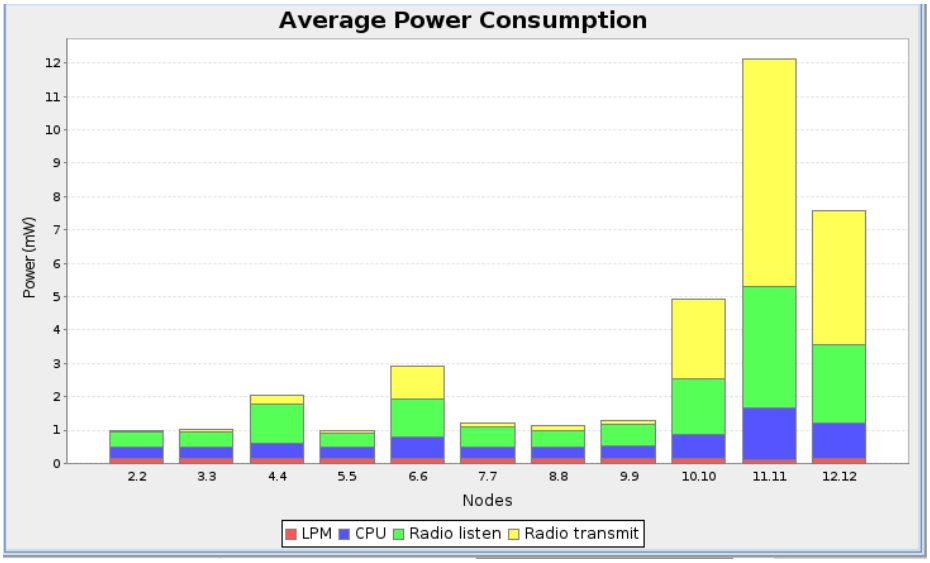

Figura 19: Consumo médio de energia durante ataque, cenário 2

Fonte: do Autor

Assim como no cenário anterior a média do ciclo de rádio aumenta de um período para o outro e os nós que mais consomem com transmissões são os nós maliciosos, embora a tendência observada na figura 15 de elevação dos gastos dos nós 4 e 10 que fazem parte do melhor caminho para o nó raiz, assim como consta nas figuras 20 e 21.

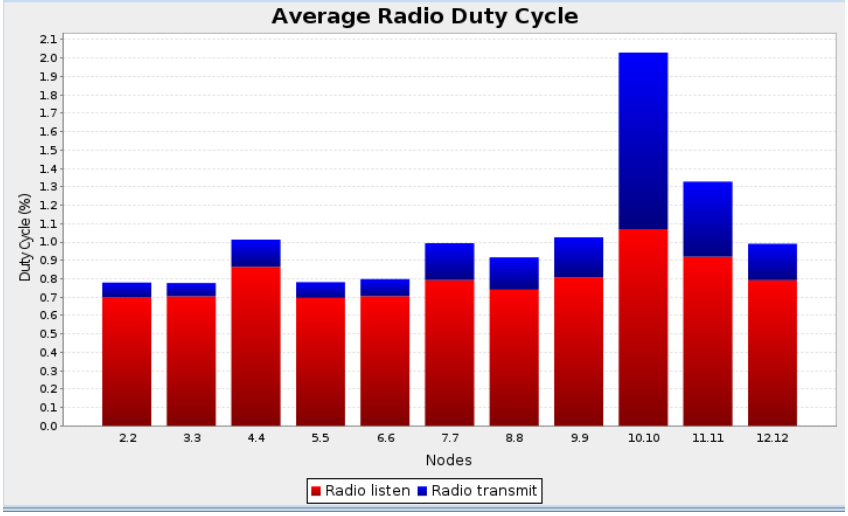

Figura 20: Média de ciclo de rádio pré-ataque, cenário 2

Fonte: do Autor

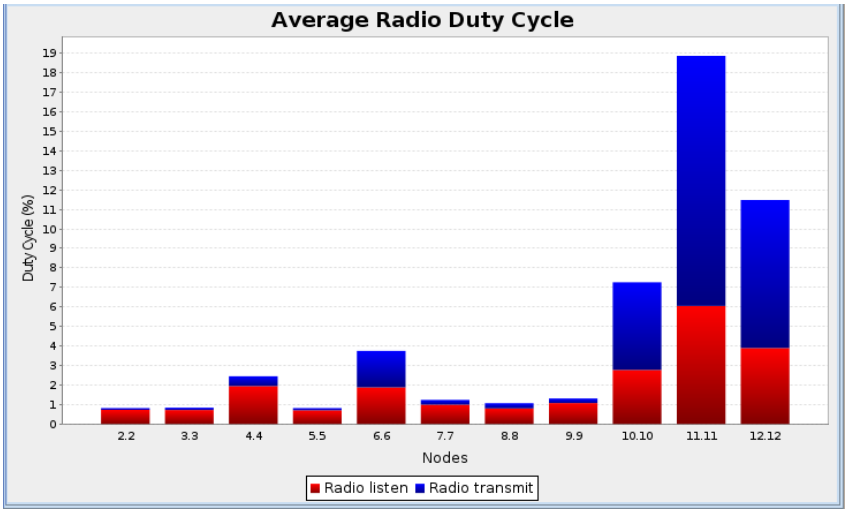

Figura 21: Média de ciclo de rádio durante ataque, cenário 2

Fonte: do Autor

Como as figuras 22 e 23 demonstram o consumo de energia na rede como um todo subiu quase em cento e dezesseis vezes do período pré-ataque para o período durante o ataque. Este cenário sob ataque levou cerca de quarenta minutos até ficar indisponível.

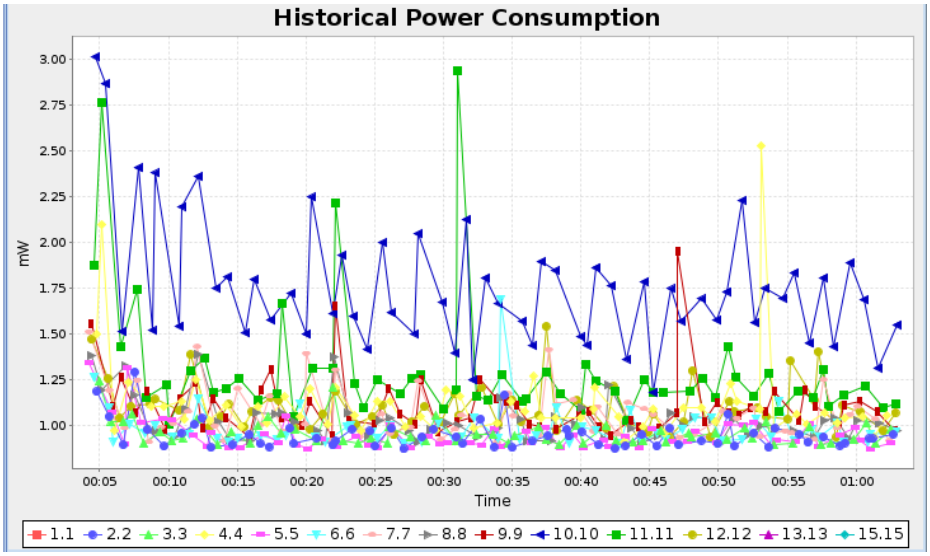

Figura 22: Histórico de consumo de energia pré-ataque, cenário 2

Fonte: do Autor

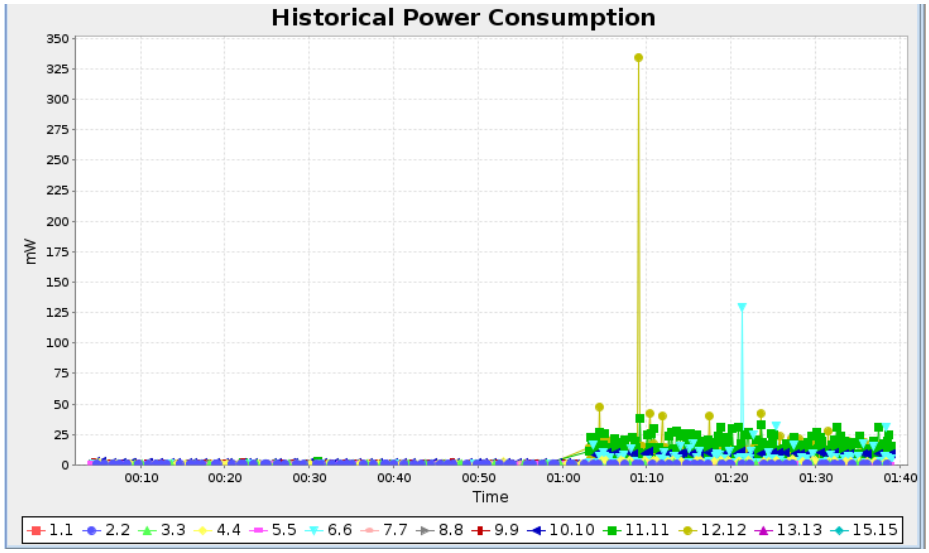

Figura 23: Histórico de consumo de energia durante ataque, cenário 2

Fonte: do Autor

Assim como no primeiro cenário, as métricas de roteamento configuradas durante a fase pré-ataque sofreram rearranjos devido ao volume adicional de pacotes, porém, diferente do exemplo anterior a variação nas métricas demonstrou-se maior tanto durante o período pré-ataque quanto no período de ataque, como descrito pelas figuras 24 e 25, provavelmente devido à topologia, já que o numero de atacantes neste cenário era menor.

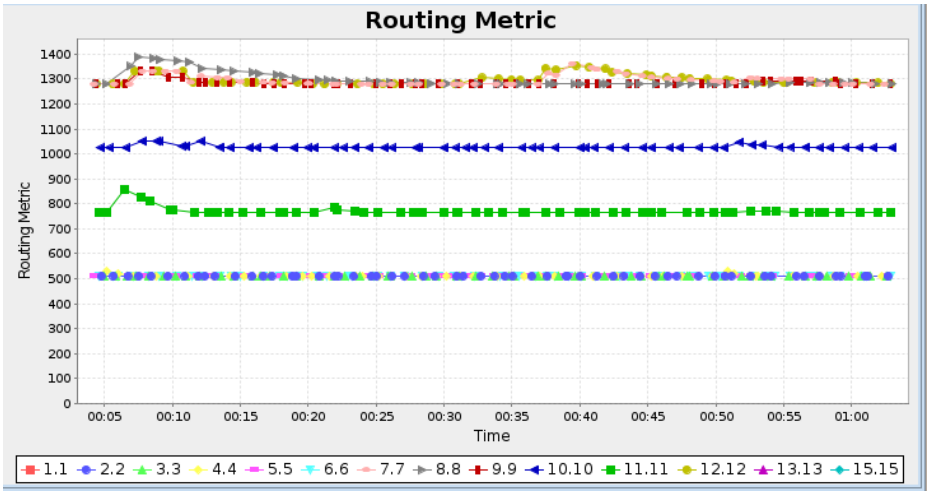

Figura 24: Métricas de roteamento pré-ataque, cenário 2

Fonte: do Autor

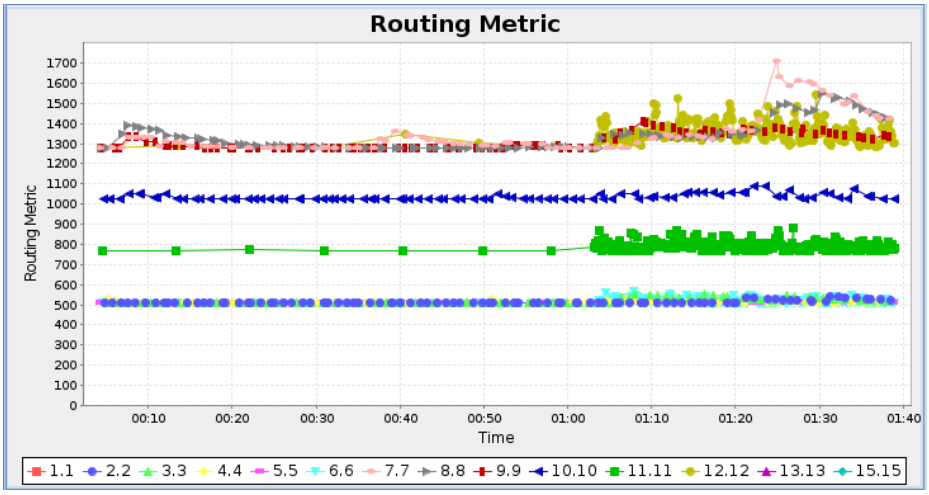

Figura 25: Métricas de roteamento durante ataque, cenário 2

Fonte: do Autor

Durante o período pré-ataque foram recebidos pelos nós da rede seiscentos e quarenta e nove pacotes e nenhum foi perdido. Depois que o ataque foi concluído, o nó raiz havia recebido cerca de sete mil trezentos e quarenta pacotes e perdido uma estimativa de vinte e cinco, ou seja, cerca de 0,34%. Esses valores são apresentados nas figuras 26 e 27.

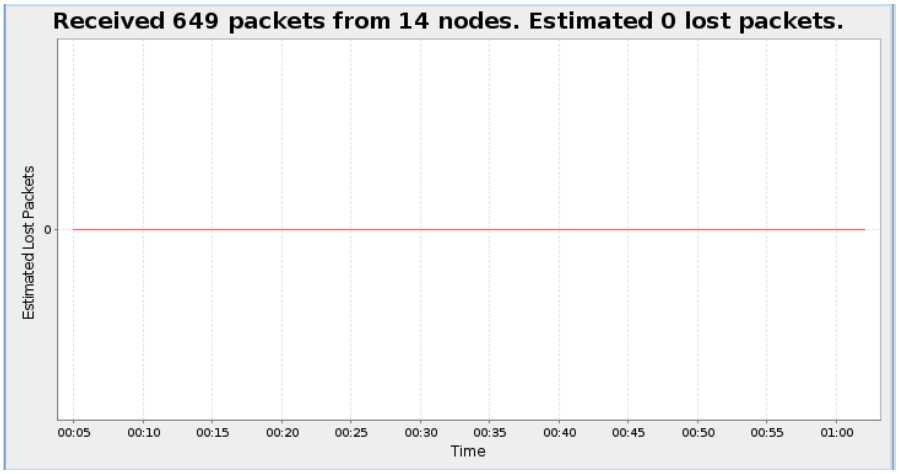

Figura 26: Estimativa de pacotes enviados e perdidos pré-ataque, cenário 2

Fonte: do Autor

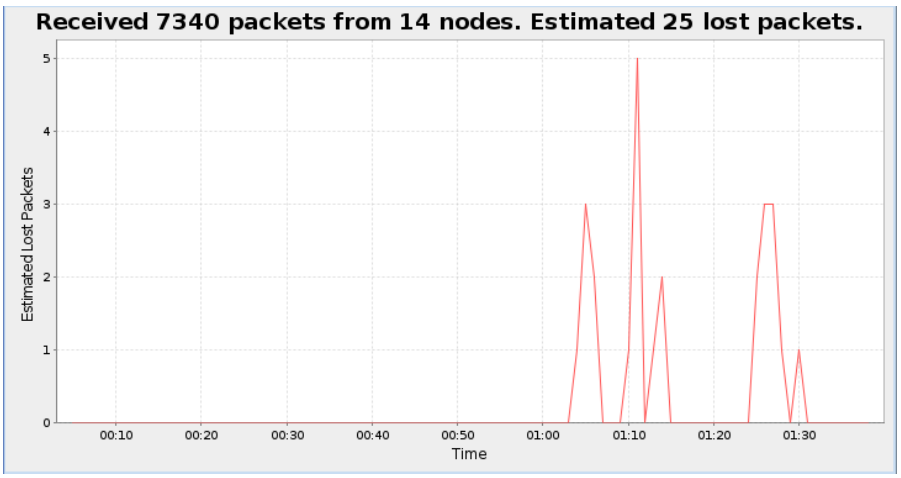

Figura 27: Estimativa de pacotes enviados e perdidos durante ataque, cenário 2

Fonte: do Autor

Por fim, as figuras 28 e 29 demonstram gráficos com a quantidade de pacotes recebidos por cada nó antes e depois do ataque. Antes do ataque pode-se notar que a carga era distribuída igualmente entre os pontos da rede, no entanto, durante o ataque a carga se concentrou principalmente nos nós maliciosos em respostas aos seus sucessivos HELLO.

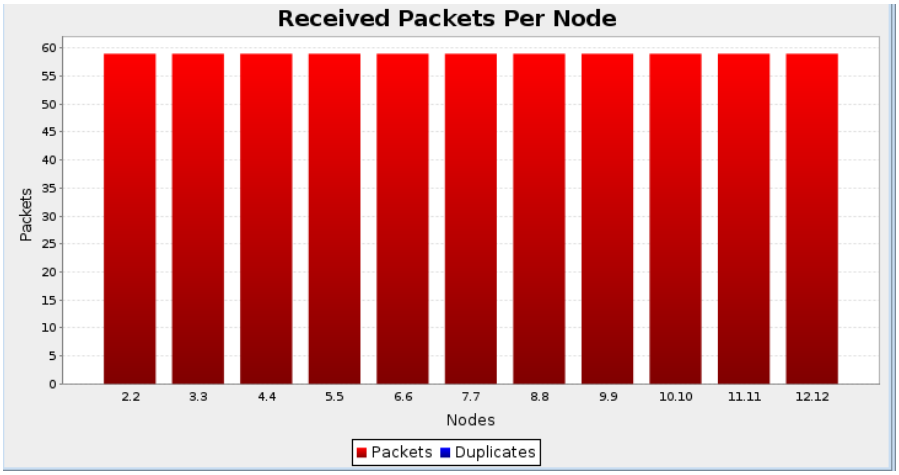

Figura 28: Pacotes recebidos por nó pré-ataque, cenário 2

Fonte: do Autor

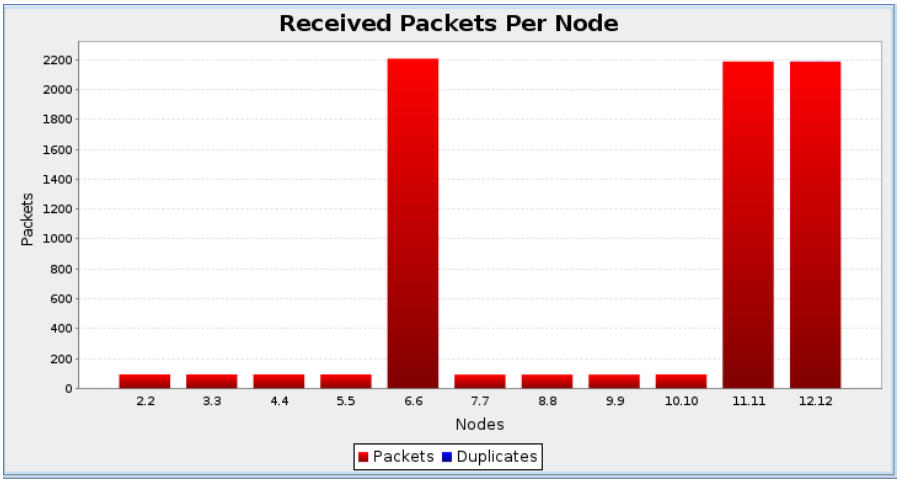

Figura 29: Pacotes recebidos por nó durante ataque, cenário 2

Fonte: do Autor

No terceiro cenário foi adicionada mobilidade aos nós atacantes o que por um breve momento os coloca fora do alcance de qualquer nó da rede, desta maneira sempre que eles ficam ao alcance enviam uma mensagem DIO para atualização das rotas na rede e por este fato há uma variação nas métricas de roteamento, garantindo a rede certo dinamismo, como ilustra a figura 30. Na figura 31 observou-se que as alterações nas métricas de roteamento que subiram em grande proporção, principalmente no que tange aos nós maliciosos.

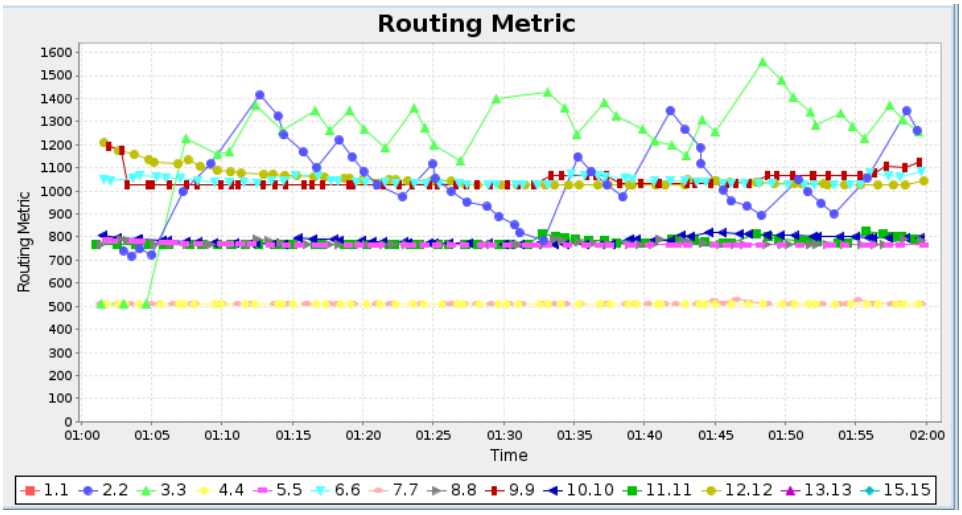

Figura 30: Métricas de roteamento pré-ataque, cenário 3

Fonte: do Autor

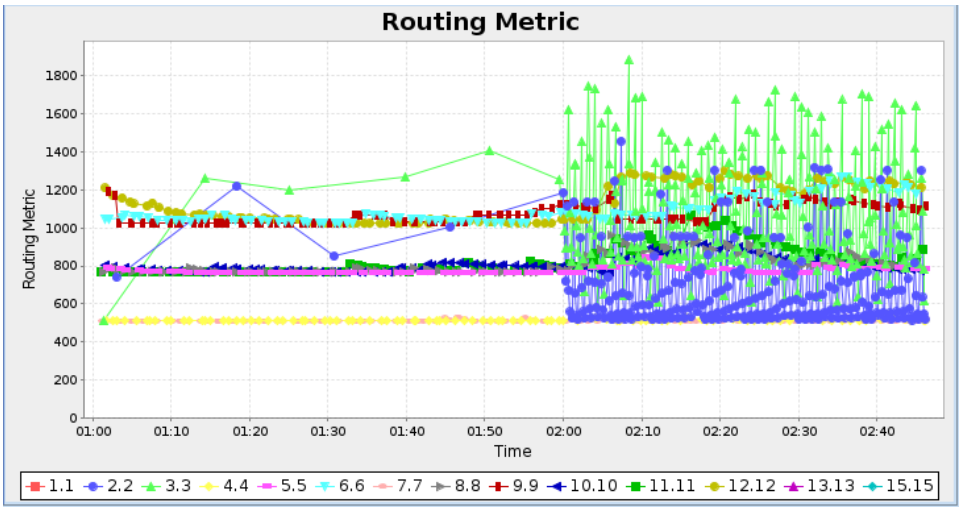

Figura 31: Métricas de roteamento durante ataque, cenário 3

Fonte: do Autor

A movimentação dos nós impacta a rede não apenas na alteração das tabelas de roteamento, mas também afeta a taxa de pacotes perdidos. Se no segundo cenário, estimou-se que nenhum pacote havia sido perdido no período pré-ataque, neste, de seiscentos e dezesseis pacotes recebidos, uma redução de 5,08% em relação ao cenário anterior, trinta e dois foram perdidos. No período de ataque houve grande aumento no número de pacotes perdidos com a estimativa da porcentagem de pacotes perdidos chegando a 75,77%. As informações a respeito dos pacotes recebidos e perdidos encontram-se nas figuras 32 e 33.

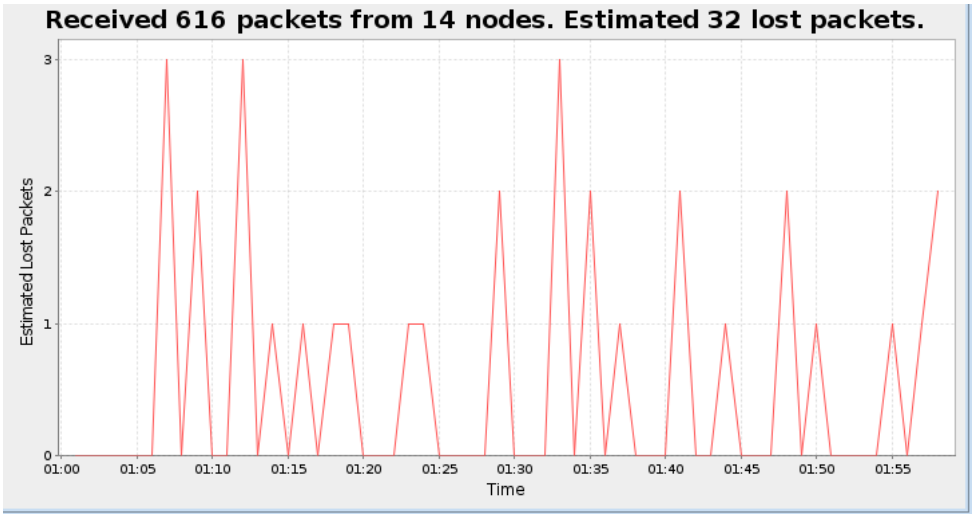

Figura 32: Estimativa de pacotes enviados e perdidos pré-ataque, cenário 3

Fonte: do Autor

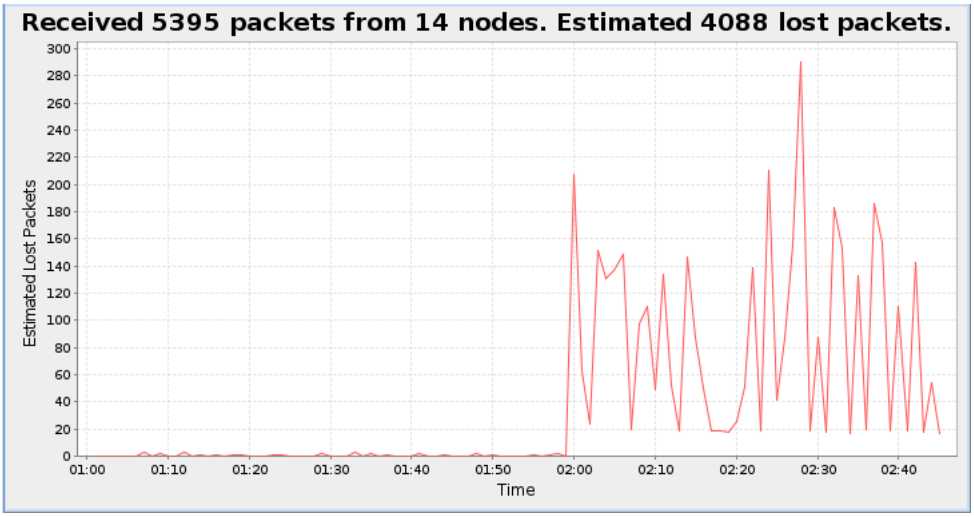

Figura 33: Estimativa de pacotes enviados e perdidos durante ataque, cenário 3

Fonte: do Autor

Como já constatou-se a influência da mobilidade dos nós na distribuição e no recebimento dos pacotes, pode-se verificar pela figura 30 que no período pré-ataque a distribuição dos pacotes é heterogênea, muito provavelmente pelas fatias de tempo em que os nós 2 e 3 ficam fora de alcance dos demais. Já no período de ataque, mesmo estando fora de alcance em alguns momentos, os nós maliciosos ainda recebem mais pacotes que os outros, como demonstram a figura 34 e 35.

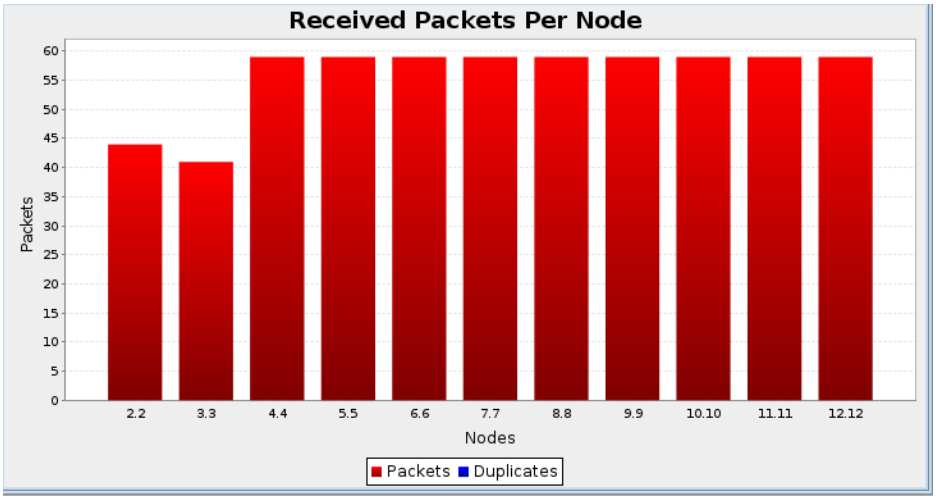

Figura 34: Pacotes recebidos por nó pré-ataque, cenário 3

Fonte: do Autor

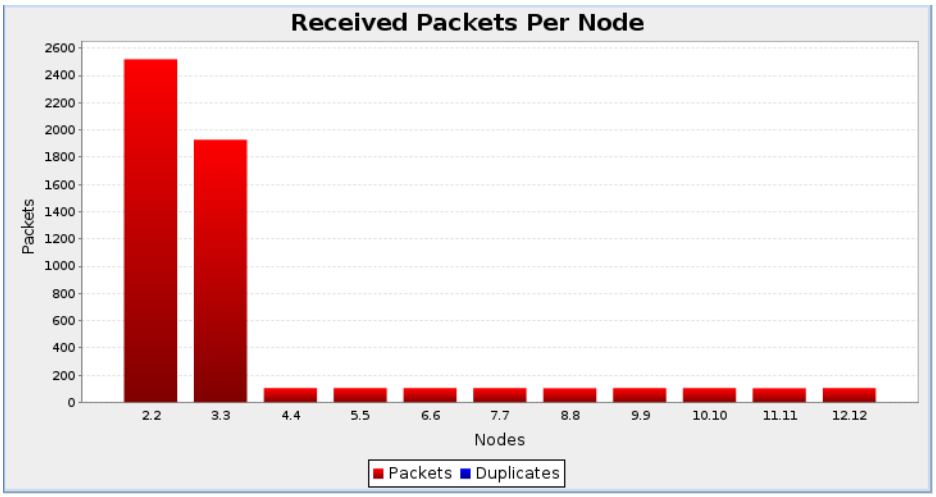

Figura 35: Pacotes recebidos por nó durante ataque, cenário 3

Fonte: do Autor

Em relação ao consumo de energia, no período pré-ataque, observou-se grande consumo por parte do nó número quatro, o dispositivo mais próximo a raiz, principalmente em gastos condizentes com espera por transmissões de rádio. Os nós móveis também apresentaram maior consumo, mas nada muito acima dos demais, com exceção do já citado número 4. Durante o ataque, como observado anteriormente o consumo dos nós maliciosos se eleva bem além dos outros nós, entretanto, no cenário 3 os atacantes não foram os maiores consumidores, ambos ficaram atrás do nó 4. Os gráficos com os dados de consumo de cada nó da rede encontram-se nas figuras 36 e 37.

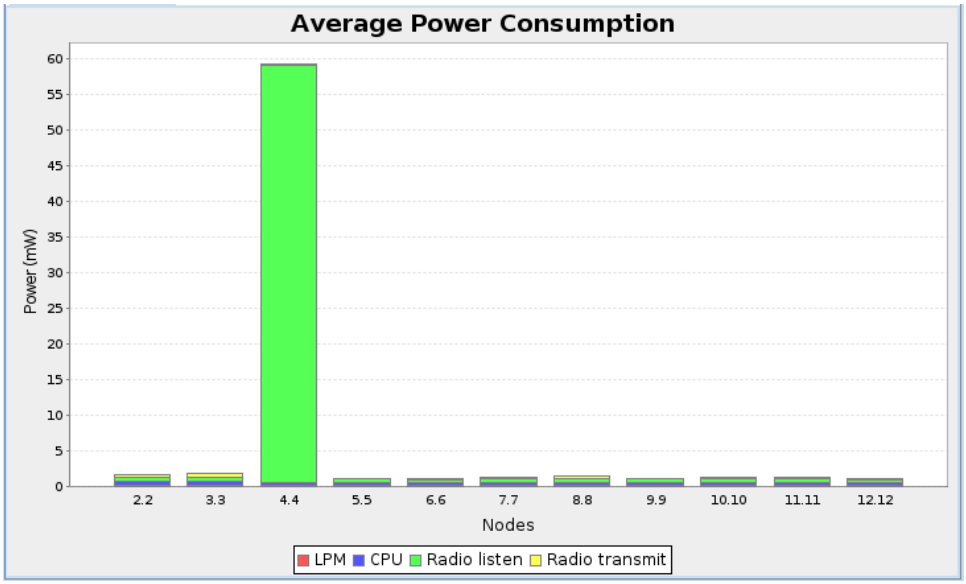

Figura 36: Consumo médio de energia pré-ataque, cenário 3

Fonte: do Autor

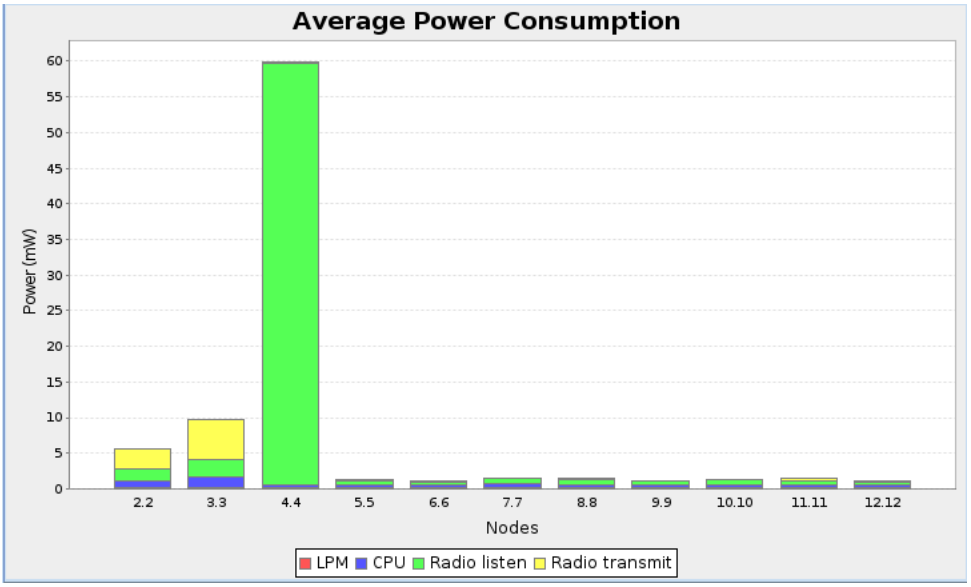

Figura 37: Consumo médio de energia durante ataque, cenário 3

Fonte: do Autor

Seguindo a tendência do consumo de energia a figura 38 demonstra que o nó número quatro é o que mais consome recursos de rádio ao esperar transmissões, nenhum ponto da rede chega perto de competir com ele neste quesito no período pré-ataque. Os nós maliciosos são os que mais gastam em realizar transmissões, no entanto, no total chegam a uma porcentagem ínfima do consumido pelo nó 4. Em comparação com o período de pré-ataque, notou-se que, assim como descreve a figura 39, durante o ataque ocorreu

aumento, como era de se esperar, no gasto com transmissão principalmente dos nós maliciosos, mas ainda assim seu consumo não chega nem a metade do número 4.

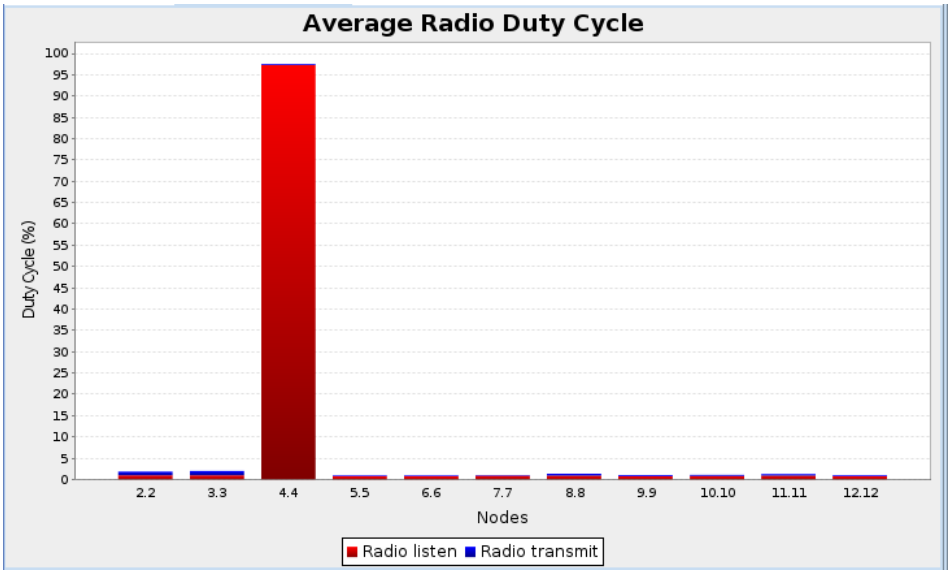

Figura 38: Média de ciclo de rádio pré-ataque, cenário 3

Fonte: do Autor

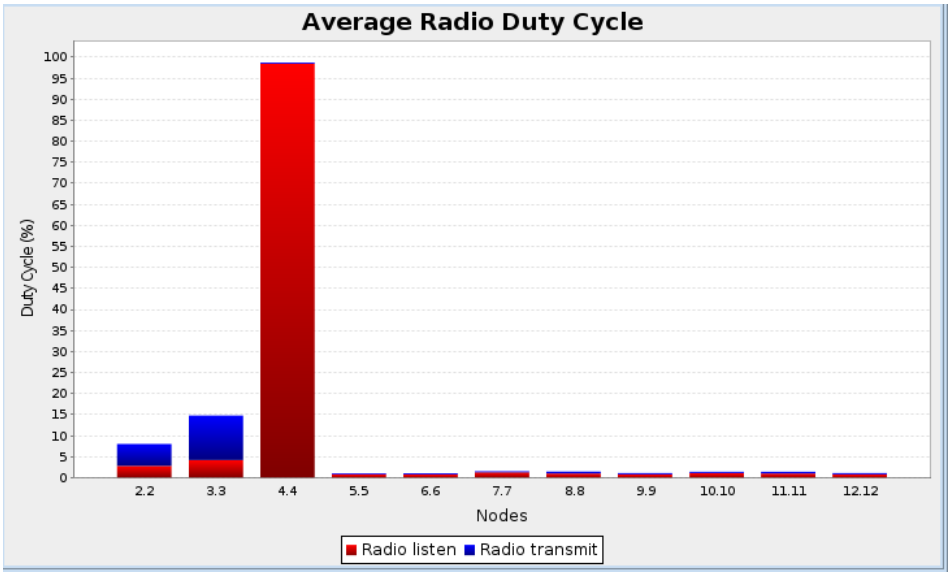

Figura 39: Média de ciclo de rádio durante ataque, cenário 3

Fonte: do Autor

As figuras 40 e 41 estabelecem uma comparação do consumo de energia durante toda a simulação. Por meio destes gráficos observou-se que, como esperada os nós móveis consumiram mais energia do que os fixos durante o período pré-ataque e apesar de o ataque ter elevado o consumo de energia da rede por meio do aumento de gasto

energético dos nós maliciosos, o nó de número 4 manteve um gasto alto constantemente durante a simulação.

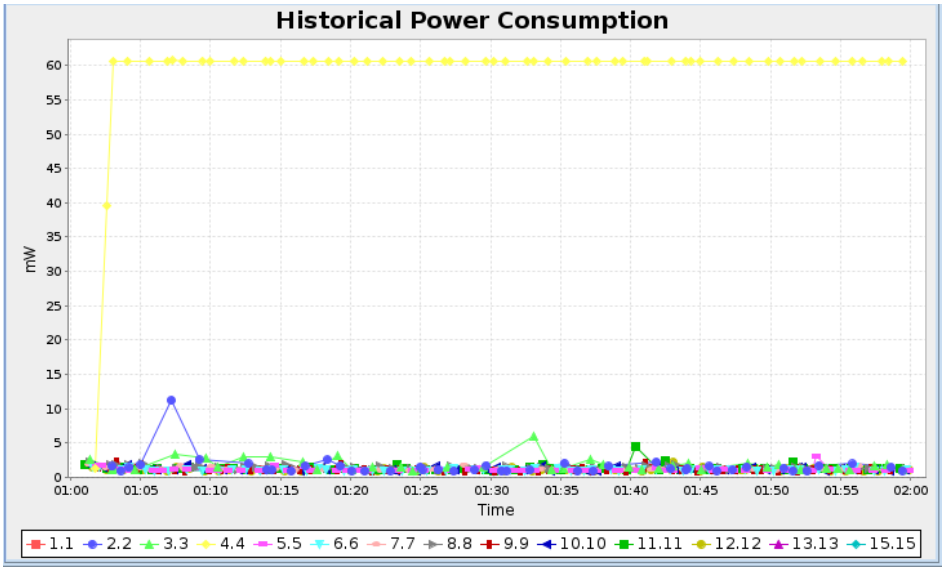

Figura 40: Histórico de consumo de energia pré-ataque, cenário 3

Fonte: do Autor

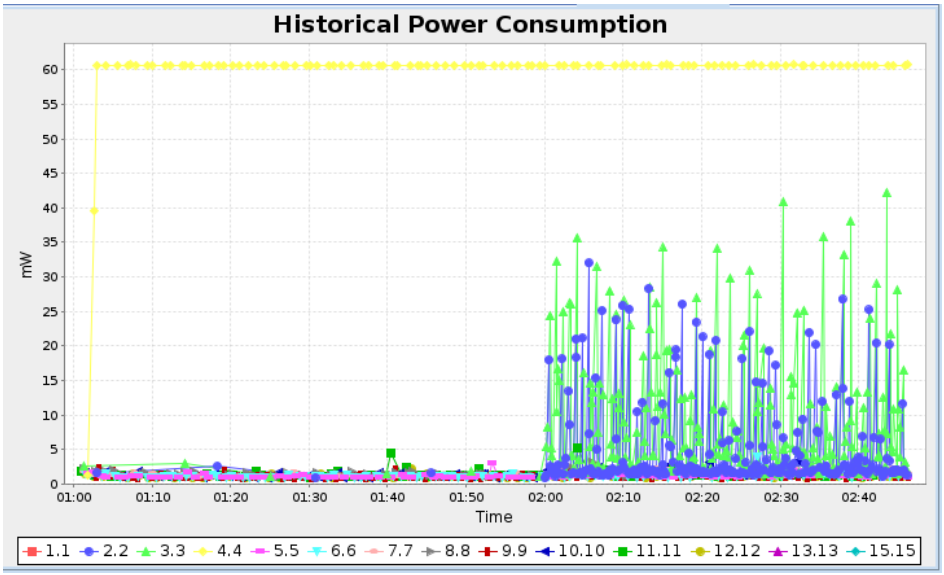

Figura 41: Histórico de consumo de energia durante ataque, cenário 3

Fonte: do Autor

Na comparação entre os três cenários observou-se que não apenas a topologia influência no consumo energético da rede, mas também que o número de nós maliciosos o faz. Afinal embora o primeiro cenário possua cinco nós atacantes o que apresentou maior consumo foi o cenário 2 que possui três nós maliciosos. Isso provavelmente ocorre porque da forma como os dispositivos atacantes estão posicionados neste cenário

formam uma espécie de “ponte” que é a melhor rota até o nó raiz da qual fazem parte outros dispositivos o que também eleva o consumo dos mesmos.

Com exceção do cenário 3, a distribuição dos pacotes recebidos entre os dispositivos foi homogênea antes dos ataques terem inicio, porém o padrão é o mesmo depois dos ataques nos três cenários: os nós maliciosos são os que mais recebem pacotes. Isso ocorre mesmo no caso do terceiro cenário em que os atacantes ficam fora de alcance por alguns segundos.

A adição de mobilidade à rede causou influência direta no número de pacotes recebidos e perdidos pelo nó raiz em relação aos cenários 1 e 2. Enquanto nos dois primeiros houve o mesmo número de pacotes recebidos, seiscentos e quarenta e nove, nenhum foi perdido antes dos ataques. No terceiro cenário o número de pacotes foi menor, seiscentos e dezesseis, com trinta e duas perdas. Depois dos ataques os cenários um e dois mantiveram em comum o maior número de pacotes recebidos e a menor quantidade de pacotes perdidos em relação ao terceiro cenário. Entretanto, devido ao maior número de atacantes no primeiro cenário a perda estimada é cerca de 6,5 vezes maior e o número de pacotes recebidos é superior ao segundo em quase três mil pacotes.

Nos dois primeiros cenários as métricas de roteamento mostraram uma tendência a se homogeneizar com o desenrolar da simulação. O terceiro cenário apresentou maior dinamismo nos critérios de roteamento devido à inclusão dos nós móveis e conseqüentes pedidos de atualização de rota por meio de mensagens de controle.

Com exceção apenas do cenário três, durante os ataques os nós que mais consumiram energia na rede foram os nós maliciosos, principalmente com transmissões de rádio. No cenário dois além de aumentarem o consumo com transmissões o ataque destes dispositivos aumentou também os gastos de outros nós com a espera por transmissões. Demonstrou-se como caso excepcional, no cenário 3, o nó número quatro que em ambos os períodos, o de pré-ataque e o de ataque, foi o que mais consumiu energia.

6.CONCLUSÃO

Por meio das simulações realizadas nos foi possível não apenas mensurar os impactos de ataques do tipo DoS sobre diferentes cenários em redes IoT, mas também avaliar a importância do uso de simuladores como o Cooja no desenvolvimento e implementação de dispositivos sob este paradigma. Tais simulações podem ser úteis não apenas para emular o funcionamento desejado dos serviços, mas também para averiguar o comportamento da rede sob os ataques descritos por Razzaq et al (2017) e a partir dos resultados das simulações elaborar soluções ainda na fase de projeto da rede para as possíveis falhas ou pontos vulneráveis.

Embora os testes tenham obtido sucesso em derrubar as redes nos cenários propostos, não o tiveram na descoberta de novas vulnerabilidades. Partiram de pontos já conhecidos do protocolo RPL (PONGLE,. 2015) como a redução da taxa de entrega de pacotes dos nós moveis, o aumento das mensagens de controle e de consumo. Sendo assim há a necessidade em trabalhos futuros de estudos mais aprofundados do protocolo RPL e de como ele se comporta sob outros tipos de ataques.

Apesar do escopo limitado dos cenários realizados demonstrou-se que a heterogeneidade entre os dispositivos (ATZORI ET AL,. 2010), neste caso apenas o fato de alguns nós apresentarem mobilidade, afeta o comportamento da rede. Pode-se extrapolar este conceito, esta heterogeneidade para outros cenários, contextos em que a diferença entre os dispositivos não está apenas no quesito movimentação, mas hardware, protocolos de rede, e etc., para inferir uma maior dificuldade na manutenção da segurança da rede.

REFERENCIAS

ALLEN, Mary. **Distributed intelligence and IoT fog.** InsightaaS. 06 ago. 2014. Disponível em <http://insightaas.com/distributed-intelligence-and-iot-fog-2/>. Acesso em: 03 mar. 2018.

ATZORI, L., IERA, A., and MORABITO, G. (2010). **The Internet of Things: A survey**. Computer Networks, v.54, n.15, Outubro, 2010, p. 2787–2805.

BABAR, S., STANGO, A., PRASAD, N., SEN, J., PRASAD, R. **Proposed embedded security framework for internet of things (iot)**, in: 2011 2nd INTERNETIONAL CONFERENCE ON WIRELESS COMMUNICATION, VEHICULAR TECHNOLOGY, INFORMATION THEORY AND AEROSPACE AND ELETRONIC SYSTEMS TECNOLOGY, Wireless VITAE 2011, Chennai, India, 2011, pp. 1 – 5.

BANAFA, A. **Internet of Things (IoT): Security, Privacy and Safety**. **New Trends in Hi Tech by Ahmed Banafa**: Internet of Things (IoT) , Big Data , Cloud Computing and Mobility. 09 mar. 2015. Disponível em: <http://ahmedbanafa.blogspot.com.br/2015/03/internet-of-things-iotsecurity- privacy.html>. Acesso em: 25 fev. 2018.

BURT, Jeff. **Internet of things presents host of security challenges**. Disponível em: <http://www.eweek.com/security/internet-of-things-presents-host-of-security-challenges> acessado em: 15 mar. 2018.

COMSOC. **Infographic: Internet of Things (IoT).** 2015. Disponível em: <http://www.comsoc.org/blog/infographic-internet-things-iot>. Acesso em: 26 jan. 2018.

CONTIKI-OS. Contiki. **The Open Source OS for the Internet of Things**. Disponível em: < http://www.contiki-os.org.> Acesso em: 16 mar. 2018.

FACCIONI FILHO, Mauro. BMS 2.0 - Nova geração de sistemas de automação e estão predial. **Congresso Netcom,** São Paulo, Aranda Eventos, 2015.

FACCIONI FILHO, Mauro. **Internet das coisas** : livro digital / Mauro Faccioni Filho ; designinstrucional Marina Cabeda Egger Moellwald. – Palhoça : UnisulVirtual,2016.

FACCIONI FILHO, Mauro. Complex Systems: Risk Model Based on Social Network Analysis. In: **INTERNATIONAL SYMPOSIUM ON INDUSTRIAL ELECTRONICS** (ISIE), 25th, 2016, Santa Clara, CA, USA. 2016a. p. 22-27.

FACCIONI FILHO, Mauro. Designing “things” for the Internet of Things. In: **I CONGRESSO INTERNACIONAL, I; WORKSHOP DESIGN & MATERIAIS**, VII, 2016, São Paulo: Universidade Anhembi Morumbi, 2016b.

FRANCIS, R. **How to conduct an IoT Pentest** . 2017. <https://www.networkworld.

com/article/3198495/internet-of-things/how-to-conduct-an-iot-pen-test.html> Acesso em : 16 mar 2018

GADDOUR, Olfa; KOUBÂA, Anis. RPL in a nutshell: A survey. **Computer Networks**, v. 56, n. 14, p. 3163-3178, 2012.

GRIECO, L.A; ALAYA, M.B; MONTEIL, T.; DRIRA, K.K. **Architecting information centric ETSI-M2M systems**, in: IEEE PerCom, 2014.

MALLERY, J. **Building a secure organization. Computer and Information Security Handbook**, p. 527–540, 2009.

MATTERN, Friedemann; FLOERKEMEIER, Christian. **From de Internet of Computers to the Internet of Things**. In: SACHS, Kai; PETROV, Ilia; GUERRERO, Pablo (Eds.). **From active data management to event-based systems and more**: papers in honor of

Alejandro Buchmann on the occasion of his 60th birthday. pp. 242-259, Berlin: Springer, 2010.

MENEZES, P. M.; ROCHA, F. G.; CARDOSO, L. M. **Segurança Em Redes De Computadores Uma Visão Sobre O Processo De Pentest**. Interfaces Científicas - Exatas e Tecnológicas, v. 1, n. 2, p. 85–96, 2015. ISSN 2359-4942.

MINERVA, Roberto; BIRU, Abyi; ROTONDI, Domenico. **Towards a Definition of the Internet of Things (IoT)**. IEEE Internet Initiative - Telecom Italia. 27 maio 2015. Disponível em: <https://pt.scribd.com/doc/306069323/IEEE-IoT-Towards-Definition-Internet-of-Things-Revision1-27MAY15>. Acesso em: 10 dez. 2017.

MIORANDI, D., SICARI, S., De PELLEGRINI, F., CHLAMTAC, I. **Survey internet of things: vision, applications and research challenges,** Ad Hoc Netw, v. 10, n. 7, Setembro, 2012, p. 1497–1516

PONGLE, Pavan; CHAVAN, Gurunath. A survey: Attacks on RPL and 6LoWPAN in IoT. In: **Pervasive Computing (ICPC), 2015 International Conference on**. IEEE, 2015. p. 1-6.

RANGER, Steve. **Welcome to the dystopian Internet of Things, powered by and starring you.** Disponível em: <http://www.zdnet.com/article/welcome-to-the-dystopian-internet-of-things-powered-by-and-starring-you/>. Acessado em: 10 mar. 2018.

RAZZAQ, M. A, GILL, S. H, QURESHI, M. A, ULLAH, Saleem. **"Security Issues in the Internet of Things (IoT): A Comprehensive Study"**, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

RECOMMENDATION ITU-T Y.2060. **Overview of the Internet of things**. ITU-T – International Telecommunication Union, 2012.

RICHMOND, Shane. **Wearable computing is here already: How hi-tech got under our skin.** Disponível em: <https://www.independent.co.uk/life-style/gadgets-and-tech/features/wearable-computing-is-here-already-how-hi-tech-got-under-our-skin-8721263.html> acessado em: 13 jan. 2018.

SKARPNESS, Mark. **Preparing the Data Center for the Internet of Things**. Intel Software and Services Group. 13 nov. 2014. Disponível em: <http://pt.slideshare.net/Inteliot/slideshelf>. Acesso em: 23 nov. 2016.

SMITH, Dave**. Google Cheirman: "The internet will disappear".** Disponível em: <http://www.businessinsider.com/google-chief-eric-schmidt-the-internet-will-disappear-2015-1> acessado em: 15 mar. 2018.

WANGHAM, M. S., DOMENECH, M. C., and de MELLO, E. R. (2013). **Infraestrutura de autenticação e de autorização para internet das coisas.** In Minicursos, volume 1 of 13th Brazilian Symposium on Information and Computer System Security (SBSeg'13). SBC.

WEBER, Rolf H. **Internet of Things–New security and privacy challenges**. Computer law & security review, v. 26, n. 1, p. 23-30, 2010.