

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Sandro Ilídio Coelho Oliveira

**Estudo sobre o impacto de dispositivos IoT em
ataques DDoS**

Uberlândia, Brasil

2018

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Sandro Ilídio Coelho Oliveira

**Estudo sobre o impacto de dispositivos IoT em ataques
DDoS**

Trabalho de conclusão de curso apresentado
à Faculdade de Computação da Universidade
Federal de Uberlândia, Minas Gerais, como
requisito exigido parcial à obtenção do grau
de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Rodrigo Sanches Miani

Universidade Federal de Uberlândia – UFU

Faculdade de Ciência da Computação

Bacharelado em Sistemas de Informação

Uberlândia, Brasil

2018

Sandro Ilídio Coelho Oliveira

Estudo sobre o impacto de dispositivos IoT em ataques DDoS

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, Minas Gerais, como requisito exigido parcial à obtenção do grau de Bacharel em Sistemas de Informação.

Prof. Dr. Rodrigo Sanches Miani
Universidade Federal de Uberlândia

Prof. Dr. Paulo Henrique R. Gabriel
Universidade Federal de Uberlândia

Me. Cláudio D. G. Linhares
Universidade Federal de Uberlândia

Uberlândia, Brasil
2018

*Dedico todo o sacrifício na confecção deste trabalho à Santa Mãe de Deus, Maria
Santíssima.*

Agradecimentos

Agradeço antes de tudo a Deus e em especial honra e louvor à Bem-Aventurada Sempre Virgem Maria pelo cuidado e intercessão para que eu conseguisse a oportunidade de trabalhar com um tema tão agradável. Já estendendo os agradecimentos ao meu orientador, que esteve de braços abertos para me ensinar com maestria, paciência e dedicação. Por fim, reconheço a especial oportunidade de ter atuado neste trabalho, por motivo de ter desenvolvido uma Iniciação Científica pelo Programa de Educação Tutorial Institucional – Sistemas de Informação (PET-SI), na tutoria do Prof. Dr. Paulo Henrique Ribeiro Gabriel. E não menos importante, a todos meus amigos e familiares que deram todo o suporte necessário para a conclusão deste projeto.

"Para um apóstolo moderno, uma hora de estudo é uma hora de oração"
São Josemaria Escrivá

Resumo

O intuito deste trabalho foi avaliar o potencial de dispositivos diretamente ligados ao paradigma de Internet das Coisas na realização de Ataques Distribuídos de Negação de Serviço. Para tal, o ambiente de simulações foi embasado a partir de uma das obras que compõe o referencial teórico. Após a compreensão e replicação dos experimentos, foram implementados novos cenários de testes baseados nos próprios parâmetros propostos pelos autores, isto é, o tamanho/quantidade dos pacotes enviados e a taxa de injeção do tráfego pelo atacante. Em razão da baixa capacidade de armazenamento, processamento e desempenho dos nós, a rede de sensores sem fio teve seus recursos rapidamente drenados durante as simulações de ataques DDoS, contudo, ao final da análise constatou-se que os ambientes constituídos de dispositivos IoT poderão se tornar potenciais ofensores deste tipo de ataque contanto que o atacante se atenha às características e tipo de rede utilizada no processo. Em alguns cenários, especialmente em casos onde foi requisitado maiores quantidades de dados, esta exaustão de processamento ocasionou a falha da própria rede, sendo ela própria vítima de um auto-ataque.

Palavras-chave: Rede de Sensores Sem Fio, Internet das Coisas, Segurança, Ataques de Negação de Serviço, Simulação.

Lista de ilustrações

Figura 1 – Exemplificação do funcionamento do paradigma IoT	17
Figura 2 – Taxonomia de ataques DDoS. Adaptada de Furfaro et al. (2016)	19
Figura 3 – Funcionamento simplificado de um ataque <i>Smurf</i> por reflexão/amplificação	21
Figura 4 – Pilha de protocolos IoT. Extraído de Pacheco et al. (2016)	23
Figura 5 – Abstração das camadas do CoAP. Extraído de Shelby, Hartke e Bormann (2014)	24
Figura 6 – Interface gráfica do NetAnim com 53 nós dispostos em formato malha se comunicando	26
Figura 7 – Comparação entre o impacto do ataque no protocolo DNS e NTP. Extraído de Furfaro et al. (2016)	28
Figura 8 – Taxa de crescimento do número de dispositivos conectados e ataques DDoS. Extraído de Peraković, Periša e Cvitić (2015)	29
Figura 9 – Funcionamento do ataque DDoS na rede WSN deste trabalho	31
Figura 10 – Quantidade de pacotes enviados por cada nó (1 Sensor)	34
Figura 11 – Amplificação média do número de pacotes enviado para a rede por cada sensor (1 Sensor)	35
Figura 12 – Tráfego gerado pelo atacante e tráfego amplificado pelos refletores (1 Sensor)	35
Figura 13 – Quantidade de pacotes enviados por cada nó (3 Sensores)	36
Figura 14 – Amplificação média do número de pacotes enviado para a rede por cada sensor (3 Sensores)	36
Figura 15 – Tráfego gerado pelo atacante e tráfego amplificado pelos refletores (3 Sensores)	37
Figura 16 – Quantidade de pacotes enviados por cada nó (5 Sensores)	38
Figura 17 – Amplificação média do número de pacotes enviado para a rede por cada sensor (5 Sensores)	38
Figura 18 – Tráfego gerado pelo atacante e tráfego amplificado pelos refletores (5 Sensores)	39
Figura 19 – Amplificação total das simulações com 50 sensores	39
Figura 20 – Tráfego gerado pelo atacante e tráfego amplificado pelos refletores (50 Sensores)	40
Figura 21 – Linha gráfica da simulação com 50 sensores, 16 Kbps e pacote de requisição 20 Bytes	41
Figura 22 – Fragmento da visualização completa da simulação com 100 sensores, 16 Kbps e pacote de requisição 20 Bytes	42

Figura 23 – Fragmento da visualização completa da simulação com 50 sensores, 64
Kbps e pacote de requisição 40 Bytes 43

Lista de tabelas

Tabela 1	– Principais características dos protocolos IoT	22
Tabela 2	– Diferenças e semelhanças entre as simulações elaboradas pelo Pacheco et al. (2016) e este trabalho	33
Tabela 3	– Legenda de cores para visualização MSV produzida pelo sistema <i>Dy-NetVis</i>	41

Lista de abreviaturas e siglas

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
ABNT	Associação Brasileira de Normas Técnicas
ACK	Acknowledgement
B	Byte
CoAP	Constrained Application Protocol
CON	Confirmable
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
DVR	Digital Video Recorder
DyNetVis	Dynamic Network Visualization System
ETSI	European Telecommunications Standards Institute
Fig.	Figura
GB	Gigabyte (s)
Gbps	Gigabits per second
GHz	Gigahertz
GNU	GNU's not Unix
GPL	General Public License
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
LoWPAN	Low-Power Wireless Personal Area Networks
M2M	Machine-to-Machine
MB	Megabyte
MQTT	Message Queuing Telemetry Transport
MSV	Massive Sequence View
MTU	Maximum Transmission Unit
NBR	Norma Brasileira
NIST	National Institute of Standards and Technology
NON	Non-confirmable
NTP	Network Time Protocol
OSI	Open Systems Interconnection
PPS	Pacotes Por Segundo
REST	Representational State Transfer
RFC	Request for Comments
RSSF	Rede de Sensores Sem Fio
RST	Reset
SSDP	Simple Service Discovery Protocol
Tbps	Terabits per second
TCP	Transmission Control Protocol

UDP	User Datagram Protocol
UPnP	Universal Plug and Play
W3C	World Wide Web Consortium
WSN	Wireless Sensor Network
XML	eXtensible Markup Language

Sumário

1	INTRODUÇÃO	14
2	REVISÃO BIBLIOGRÁFICA	16
2.1	Referencial teórico	16
2.1.1	Internet das Coisas	16
2.1.2	Segurança da Informação	17
2.1.3	Ataques de Negação de Serviço	18
2.1.3.1	Grau de automação	19
2.1.3.2	Fragilidade explorada	20
2.1.3.3	Dinâmica de variação da taxa de ataque	20
2.1.3.4	Impacto	21
2.1.4	Rede de Sensores Sem Fio	21
2.1.5	Pilha de protocolos para dispositivos IoT	22
2.1.5.1	CoAP	23
2.1.5.2	UDP	24
2.1.5.3	6LoWPAN e IEEE 802.15.4	24
2.1.6	Ferramentas	26
2.1.6.1	Simulador de redes ns-3	26
2.1.6.2	NetAnim	26
2.1.6.3	Wireshark	27
2.2	Trabalhos correlatos	27
3	DESENVOLVIMENTO	31
3.1	Metodologia	31
3.2	Resultados	34
3.2.1	1 Sensor	34
3.2.2	3 Sensores	36
3.2.3	5 Sensores	37
3.2.4	50 e 100 sensores	39
3.2.5	Discussão	43
4	CONCLUSÃO	45
	REFERÊNCIAS	48

1 Introdução

O termo Internet das Coisas (IoT, do inglês *Internet of Things*) está se tornando popular tanto no meio acadêmico quanto no ramo empresarial. O maior motivo de tamanha expressividade e interesse no assunto está basicamente no fato conceitual da IoT, isto é, o que ela pode oferecer para a sociedade contemporânea (RAYES; SALAM, 2016). Por exemplo, um dispositivo inteligente como um marca-passo que envia informações em tempo real diretamente para o médico particular do paciente pode aumentar significativamente a qualidade de vida da população.

Apesar do seu potencial na melhora da qualidade de vida das pessoas, a Internet das Coisas traz consigo uma crescente preocupação com a segurança e privacidade dos dados (RAYES; SALAM, 2016). Usando o exemplo anterior, suponha que o paciente tenha seu marca-passo inutilizado por um ataque de negação de serviço (DoS, do inglês *Denial of Service*), acarretando no óbito da vítima. Inúmeros são os exemplos que mostram os perigos desse aumento desenfreado de dispositivos sensoriais compartilhando informações entre si.

Em 2016 aconteceu o maior ataque de negação de serviço distribuído (DDoS, do inglês *Distributed Denial of Service*) registrado nos últimos anos, onde o *malware* Mirai infectou câmeras de segurança e dispositivos de gravação de vídeo (DVR, do inglês *Digital Video Recorder*). Tais dispositivos foram usados para disparar Ataques de Negação de Serviço contra servidores de nomes de domínio (DNS, do inglês *Domain Name System*) hospedados na empresa DYN que é responsável por fornecer serviços de infraestrutura de rede (CAO et al., 2017).

Para entender a capacidade de tais ataques, Hengst (2016) analisou os doze maiores ataques DDoS observados pela Akamai até março de 2015 e apurou que fatores como largura de banda, tipo de protocolo abordado pelo atacante e disponibilidade de serviço se mostraram influenciadores para determinar o potencial para dispositivos IoT serem utilizados como refletores em ataques DDoS. Afinal, perante a expectativa de aproximadamente 24 bilhões de elementos conectados em 2020, utilizando apenas 0.01% de 20 bilhões destes dispositivos os ataques lograram algo em torno de 36.28 Tbps, equivalente à 123.83% mais dados que o maior ataque conhecido até aquele período.

A pesquisa desenvolvida pelo Pacheco et al. (2016), implementou cenários para simular e avaliar os efeitos de um ataque DDoS de reflexão ampliada em uma rede de sensores sem fio (WSN, do inglês *Wireless Sensor Network*). Os cenários foram construídos de tal modo que esta rede possui um nó malicioso infiltrado que envia solicitações de descoberta de serviço para todos os sensores com o endereço de origem falsificado. Os

resultados obtidos evidenciam que ataques distribuídos de negação de serviço podem explorar ambientes IoT. Ademais, o próprio ambiente IoT se torna um alvo fácil, visto que sua largura de banda e recursos computacionais são aceleradamente consumidos.

Dado a vulnerabilidade dos dispositivos IoT e os recentes ataques visando tais elementos, este trabalho se encaixa na questão da avaliação do comportamento de uma rede composta por dispositivos IoT durante um Ataque de Negação de Serviço, em especial ataques por amplificação e replicação de pacotes. Ademais, possui o objetivo geral de avaliar o potencial de dispositivos diretamente ligados ao paradigma de IoT na realização de ataques DDoS. Para tal foi replicado o mesmo ambiente de simulações realizadas pelo Pacheco et al. (2016), sendo efetuada a alteração de alguns parâmetros com o intuito de recriar um novo ambiente de testes.

A partir desta introdução, este trabalho é organizado da seguinte forma: o capítulo 2 nomeado Revisão Bibliográfica possui a seção 2.1 do Referencial Teórico responsável por expor os conceitos relacionados à Internet das Coisas (2.1.1), Segurança da Informação (2.1.2), Ataques de Negação de Serviço (2.1.3), Rede de Sensores Sem Fio (2.1.4), a pilha de protocolos para dispositivos IoT (2.1.5) e por fim, as ferramentas (2.1.6) utilizadas na confecção deste trabalho. Ademais, a seção 2.2 apresenta o levantamento bibliográfico de alguns trabalhos relacionados ao tema desta pesquisa. O capítulo 3, traz os detalhes da metodologia (3.1) pelo qual foram desenvolvidos as simulações e conseqüentemente confeccionado os resultados, estes, descritos na seção 3.2 e discutidos na seção 3.2.5. O capítulo conclusivo 4, mostra as considerações finais e as perspectivas para trabalhos futuros.

2 Revisão Bibliográfica

Este capítulo contém a seção 2.1 relativa ao referencial teórico que possui o intuito de expor os principais conceitos abordados no trabalho e da mesma maneira, fundamentando o propósito desta pesquisa a seção 2.2 explicita sucintamente alguns trabalhos correlatos publicados por Furfaro et al. (2016), Hengst (2016) e Peraković, Periša e Cvitić (2015) que serviram de apoio na elaboração deste.

2.1 Referencial teórico

Esta seção elucida assuntos relativos à Internet das Coisas (2.1.1), Segurança da Informação (2.1.2), Ataques de Negação de Serviço e suas características (2.1.3), Rede de Sensores Sem Fio (2.1.4), a pilha de protocolos comumente usada em dispositivos IoT (2.1.5) e por fim, as ferramentas utilizadas, a saber: o simulador de redes ns-3 (2.1.6.1) e os *softwares* NetAnim (2.1.6.2) e Wireshark (2.1.6.3).

2.1.1 Internet das Coisas

Para Rayes e Salam (2016), a ideia principal do paradigma Internet das Coisas é atuar conectando fisicamente qualquer coisa à Internet com o objetivo de monitorar e controlar suas funcionalidades. Desta forma, a presença ubíqua destes dispositivos conectados entre si os torna capazes de interagirem e cooperarem mutuamente, a fim de chegar em um propósito comum (ATZORI; IERA; MORABITO, 2010). A exemplificação deste conceito pode ser visualizada na Figura 1, pelo qual podemos observar diversos tipos de elementos se conectando à Internet, como geladeiras, fogões e até mesmo coleiras de animais de estimação poderão ser monitoradas via Internet com o uso da IoT.

Conforme exposto por Rayes e Salam (2016), para se caracterizar um ambiente IoT é preciso que o meio possua:

- **Sensores:** dispositivos usados para captar os dados;
- **Identificadores:** utilizados na identificação da fonte onde o dado é coletado;
- **Software:** necessário para analisar os dados e transformá-los em informações;
- **Conectividade com a Internet:** princípio básico do paradigma, sendo responsável pela comunicação e notificação dos nós.

A união desses elementos com a infraestrutura de rede atual permite que dispositivos físicos tornem-se sensíveis à interações humanas, isto é, passam a produzir dados,

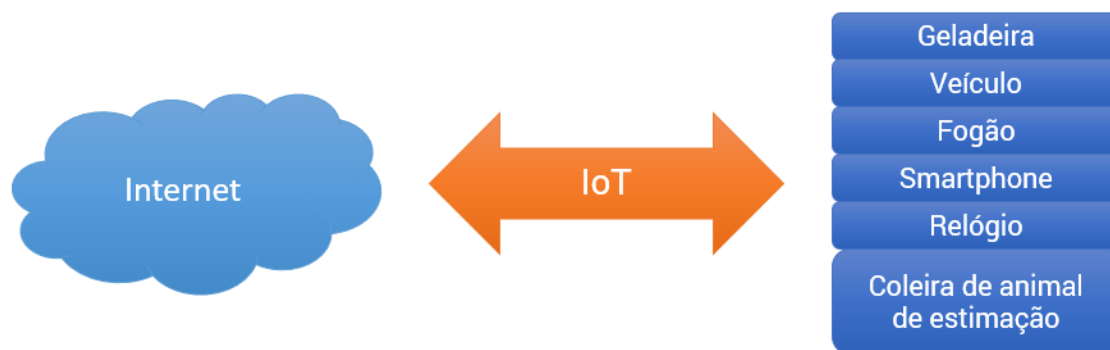


Figura 1 – Exemplificação do funcionamento do paradigma IoT

criando assim benefícios como melhoria na qualidade de vida, conforto, redução de gastos, dentre outros (RAYES; SALAM, 2016).

A fim de exemplificar os conceitos e benefícios supracitados, Kawano et al. (2015) mostra o uso do paradigma IoT em fazendas inteligentes, que a partir de uma Rede de Sensores Sem Fio (RSSF) instalada em toda plantação permite que gestores de propriedades acompanhem fatores como umidade e temperatura do ambiente por meio de um *software* que propicia a visualização dessas informações remotamente. Com esse auxílio, a tomada de decisão do momento ideal para aplicar defensivos agrícolas acaba sendo simplificada e mais assertiva, gerando então economia e melhores resultados no cultivo dos alimentos.

2.1.2 Segurança da Informação

De acordo com Suganthy e Maiti (2014) o fluxo de informações em qualquer organização tem aumentado ao longo das últimas décadas e conseqüentemente cresce também a necessidade de proteção de informações críticas de cada negócio. Para tal fim, Stallings (2015) aponta que a área de Segurança da Informação apoia-se em estratégias com o intuito de desviar, prevenir, detectar e corrigir violações de segurança relacionadas à transferência de informações.

A própria Segurança da Informação é definida pela norma ABNT NBR ISO/IEC 17799:2005 como sendo a "*preservação da confidencialidade, da integridade e da disponibilidade da informação*" (ABNT, 2005). Ainda de acordo com o Instituto Nacional de Padrões e Tecnologia (NIST, do inglês *National Institute of Standards and Technology*) o termo segurança da informação significa proteger a informação e sistemas de informação contra acesso, uso, divulgação, desmembramento, modificação ou destruição não autorizada (BARKER, 2003). A tríade CID (acrônimo para Confidencialidade, Integridade e

Disponibilidade) representa os objetivos da área e são definidas por [Stallings \(2015\)](#) e [Barker \(2003\)](#) como:

- **Confidencialidade:** preservar restrições autorizadas sobre acesso e divulgação de informação, incluindo meios para proteger a privacidade de indivíduos e informações privadas. Uma perda de confidencialidade seria a divulgação não autorizada de informação.
- **Integridade:** prevenir-se contra a modificação ou destruição imprópria de informação, incluindo a irretratabilidade e autenticidade dela. Uma perda de integridade seria a modificação ou destruição não autorizada da informação.
- **Disponibilidade:** assegurar acesso e uso rápido e confiável da informação. Uma perda de disponibilidade é a perda de acesso ou de uso da informação ou do sistema de informação.

2.1.3 Ataques de Negação de Serviço

Um ataque de negação de serviço (DoS, do inglês *Denial of Service*) possui o intuito de inviabilizar recursos disponibilizados por sistemas conectados à Internet simplesmente aumentando o tráfego de informações para o dispositivo alvo. Aderindo ao mesmo raciocínio, um Ataque Distribuído de Negação de Serviço (DDoS, do inglês *Distributed Denial of Service*) opera coordenadamente uma *botnet*, isto é, uma rede com vários sistemas previamente sequestrados (conhecidos como dispositivos zumbis ou *bots*) para enviar repetidas requisições ao alvo, a fim de exaurir recursos como os *buffers* de rede, ciclos de processamento do processador e largura de banda ([CARL et al., 2006](#)).

Por mais que o único objetivo de ataques DDoS seja incapacitar a vítima, existem várias maneiras pelo qual o atacante pode atingir essa meta. Em razão dessa expressividade, [Mirkovic e Reiher \(2004\)](#) examinaram a estrutura estratégica sob o qual os ataques são elaborados e propuseram uma taxonomia para classificação dos mesmos. Os autores expuseram as 4 principais fases que de maneira geral são observadas na execução dos ataques, são elas:

1. **Recrutar:** fase onde o atacante angaria agentes. Habitualmente, esta fase é desempenhada automaticamente através da busca por vulnerabilidades em sistemas;
2. **Explorar:** as vulnerabilidades encontradas são exploradas com o intuito de encontrar os pontos mais fracos;
3. **Infectar:** o código malicioso é inserido por meio da fragilidade localizada;
4. **Usar:** após infectado, o dispositivo é utilizado para enviar as requisições à vítima.

Em consonância com o trabalho de [Mirkovic e Reiher \(2004\)](#), [Furfaro et al. \(2016\)](#) sintetizou os resultados atingidos por eles e elaborou a Figura 2, na qual apresenta as principais propriedades arquiteturais de ataques DDoS, sendo os conceitos essenciais para a compreensão deste trabalho assinalados com uma cor mais forte na figura e logo em seguida explicados conforme as subseções: grau de automação (2.1.3.1), fragilidade explorada (2.1.3.2), dinâmica de ataque (2.1.3.3) e impacto à vítima (2.1.3.4)

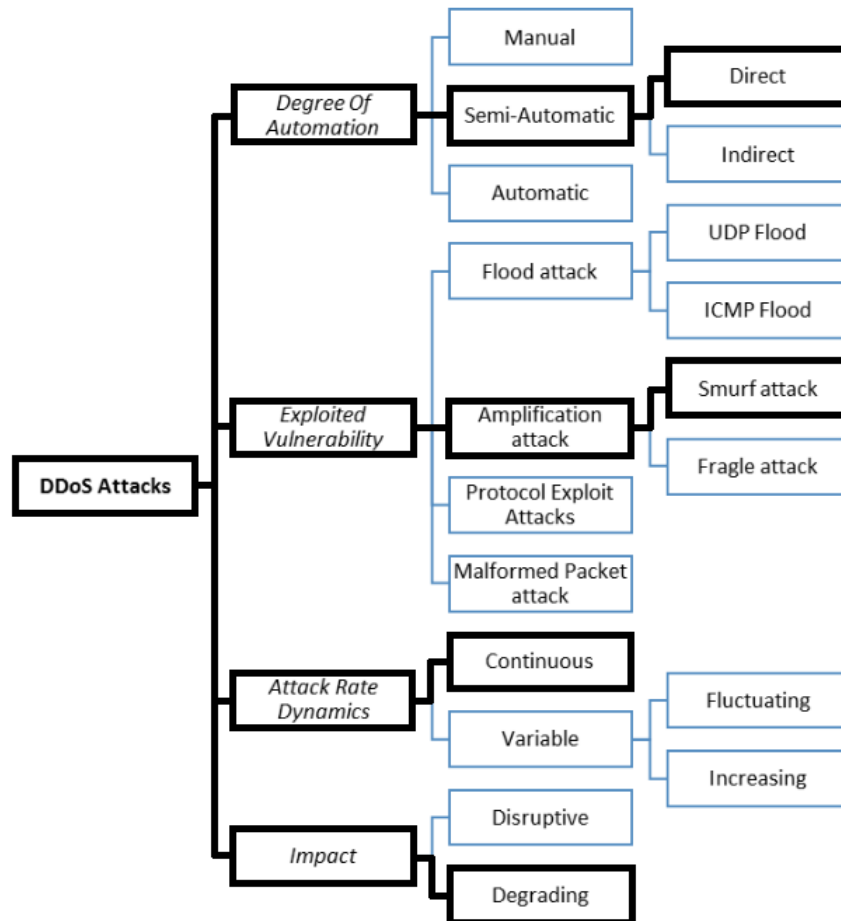


Figura 2 – Taxonomia de ataques DDoS. Adaptada de [Furfaro et al. \(2016\)](#)

2.1.3.1 Grau de automação

Singularmente, as quatro fases definidas anteriormente podem ser executadas de forma manual, semi-automática ou automaticamente. Caso o grau de automação seja definido como sendo semi-automático, a comunicação estabelecida entre os *hosts* pode ser direta ou indireta ([MIRKOVIC; REIHER, 2004](#)).

Os ataques semi-automáticos possuem um coordenador (*master*) e os agentes (*bots*). As fases de recrutamento, exploração e infecção são automatizadas, no entanto, a fase de uso é manual, visto que o dispositivo *master* especifica atributos como o tipo de ataque, duração e a vítima que será abordada pelos agentes. Em relação ao tipo de comu-

nicação, na [comunicação] direta se faz necessário conhecimento mútuo entre o atacante e os *bots*, já na comunicação indireta, são usados serviços legítimos como programas de *chat* para Internet (MIRKOVIC; REIHER, 2004).

2.1.3.2 Fragilidade explorada

Conforme Mirkovic e Reiher (2004), os ataques são classificados de duas formas: por semântica ou por força bruta, conhecidas na literatura por exploração de vulnerabilidade e inundação, respectivamente. Existe uma linha tênue entre as características das duas formas de ataque, em ambos os casos a vítima é sufocada com grandes quantidades de requisições. No entanto, os efeitos de ataques por semântica podem ser mitigados dada a implementação de filtros e/ou correções das falhas nos protocolos afetados. É oportuno ressaltar que ao ser contra-atacado por meio de modificações em protocolos ou aplicações, os ataques por exploração de vulnerabilidade são automaticamente categorizados como ataques por força bruta.

O ataque conhecido como *Smurf* é um dos exemplos que utilizam vulnerabilidades em protocolos para causar ataques por inundação (Division CERT, 2017). Basicamente, o atacante utiliza o conceito de *IP Spoofing* que consiste na falsificação do IP de origem pelo IP de destino e envia pacotes de requisição implementados no protocolo ICMP (*Internet Control Message Protocol*) para uma *botnet* usando o endereço *broadcast* e a partir disso todos os sensores são obrigados a responder as requisições para a vítima como se ela tivesse solicitado (FURFARO et al., 2016).

Além do *IP spoofing* dar a oportunidade de efetivar um ataque por reflexão, uma vez que cada *bot* ao receber os pacotes irão enviá-los para a vítima, o recurso de amplificação foi aplicado neste trabalho para aumentar a eficácia do ataque. A amplificação ocorre quando o tráfego gerado como resposta para a vítima é superior ao requisitado aos dispositivos refletores (FURFARO et al., 2016). De acordo com a Figura 3 que mostra de forma simplificada o funcionamento de um ataque *Smurf* com amplificação, o atacante envia um pacote com 10 bytes para a *botnet*, os refletores processam este pacote e cada um envia uma resposta para a vítima com o tamanho de 100 bytes. O tráfego inicial possui 30 bytes no total. No entanto, a resposta possui 300 bytes, configurando então uma taxa de amplificação que aumentou o impacto do ataque em 10 vezes.

2.1.3.3 Dinâmica de variação da taxa de ataque

Durante a realização do ataque, todos os dispositivos participantes da *botnet* são incitados pelo atacante a enviar uma sequência de pacotes para a vítima até que seus recursos sejam esgotados. Dito isso, a taxonomia proposta por Mirkovic e Reiher (2004) diferencia essa injeção do tráfego em uma dinâmica constante ou variável.

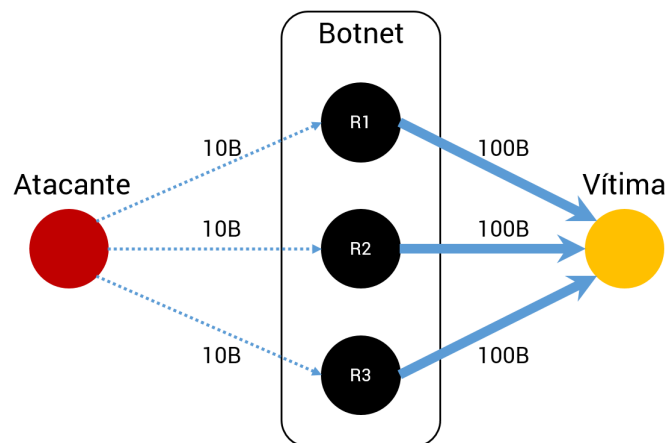


Figura 3 – Funcionamento simplificado de um ataque *Smurf* por reflexão/amplificação

Dentre as opções variáveis, a taxa pode crescer gradualmente ou flutuar conforme a necessidade. Ainda que essa dinâmica facilite o reconhecimento do tráfego anômalo pela vítima, a maioria dos ataques são implementados utilizando uma taxa constante de injeção do tráfego, (MIRKOVIC; REIHER, 2004).

2.1.3.4 Impacto

O impacto que um ataque DDoS causa à vítima foi classificado por Mirkovic e Reiher (2004) como sendo disruptivo ou degradante. O objetivo do ataque disruptivo é negar completamente os serviços da vítima por meio da transferência de grandes quantidades de dados. Já para o ataque com dinâmica degradante a meta é consumir determinada porção dos recursos disponíveis da vítima sem suspender os serviços completamente, pois desta forma, aumenta-se a complexidade na detecção do ataque por parte da vítima.

2.1.4 Rede de Sensores Sem Fio

Redes de Sensores Sem Fio (RSSF) ou WSN (do inglês, *Wireless Sensor Network*) são utilizadas para o monitoramento de variáveis de ambiente. Para isso são espalhados vários dispositivos, isto é, os nós da rede, que serão capazes de obter as informações ambientais, processar todos os dados e transmiti-los por uma rede sem fio a um ou mais pontos de saída, conhecidos como nós coordenadores da rede. Estes dispositivos possuem recursos de processamento, armazenamento e energia limitados. Em sua maioria, realizam apenas uma função específica de processamento e são alimentados por baterias não recarregáveis devendo ser independentes, ou seja, sem necessitarem de constantes atualizações e assistência humana no geral (DELICATO, 2005).

Os nós simulam sensores que possuem unicamente a função de coletar informações sobre a temperatura do ambiente e informar esses dados ao nó coordenador da rede

(PACHECO et al., 2016).

2.1.5 Pilha de protocolos para dispositivos IoT

Redes de computadores envolvem diferentes conceitos, protocolos e tecnologias. Portanto, com a intenção de esclarecer o intrincado escopo da área, a literatura tem organizado e explicado arquiteturas de redes a partir da ideia de camadas. Dessa forma, é possível perceber que cada uma dessas camadas possuem suas próprias características, objetivos e funções (KUROSE; ROSS, 2013).

De acordo com Zanella et al. (2014) e Palattella et al. (2012) a arquitetura dos protocolos elaborados para funcionar sob o conceito de Internet das Coisas é essencialmente diferente, pois, conforme já mencionado, os recursos destes equipamentos são limitados e necessitam de uma pilha de protocolos simplificados aos quais devem estar aptos para trabalhar com baixo processamento, consumo de energia reduzido e grande interoperabilidade. Alguns órgãos reguladores, tais como IETF (*Internet Engineering Task Force*), ETSI (*European Telecommunications Standards Institute*) e o W3C (*World Wide Web Consortium*) buscam definir protocolos e serviços que estejam alinhados ao paradigma REST (*Representational State Transfer*), uma vez que este ponto de referência atuará como interface entre a arquitetura tradicional e a IoT garantindo um design mais flexível, simples e escalável. Além dos protocolos 6LoWPAN [RFC 4919] que combina o IPv6 [RFC 2460] e o LoWPAN [IEEE 802.15.4] e o protocolo de troca de mensagens e descobrimento de rede chamado *Constrained Application Protocol* (CoAP) [RFC 7252], existe também o *MQ Telemetry Transport* (MQTT) [ISO/IEC PRF 20922] também operado em elementos IoT (BARRETO et al., 2017).

Protocolos	Principais características e funções	OSI simplificado
CoAP	Garante a formatação das mensagens enviadas/recebidas e também possui recursos de descoberta de serviços.	5 - Aplicação
UDP	Gerencia a comunicação ponto a ponto entre as aplicações. Apesar do TCP ser o protocolo dominante desta camada, o UDP se faz mais necessário visto sua simplicidade e tamanho reduzido do cabeçalho.	4 - Transporte
IPv6	Camada se encarrega de disponibilizar endereços e rotas aos dispositivos.	3 - Rede
6LoWPAN	Providencia a adaptação do IPv6 para IEEE 802.15.4, usando métodos de compressão de cabeçalhos.	2 - Enlace
IEEE 802.15.4 MAC	Disponibiliza um link confiável entre os nós, detectando erros que podem ocorrer durante a transmissão/recepção na camada física, além de usar recursos que diminuem a chance de colisão entre os pacotes.	2 - Enlace
IEEE 802.15.4	Responsável por converter os bits em sinais que serão transmitidos e recebidos através do ar.	1 - Física

Tabela 1 – Principais características dos protocolos IoT

No entanto, apesar de alguns protocolos simplificados estarem *de facto* sendo padronizados pelo uso, como é o caso do CoAP, 6LoWPAN e IEEE 802.15.4 ainda há algumas divergências entre autores (ZANELLA et al., 2014). A Figura 4 mostra a pilha de protocolos utilizada pelo Pacheco et al. (2016) na implementação dos sensores, na qual o protocolo 6LoWPAN é alocado na camada de rede, número 3 no modelo OSI (*Open Systems Interconnection*) simplificado. Contudo, para Olsson (2014), o referido protocolo

está na camada de enlace e atua como intermediário entre os protocolos IPv6 e o IEEE 802.15.4 conforme tabela 1. Os tópicos a seguir apresentarão os principais conceitos dos protocolos implementados na pilha da Figura 4.

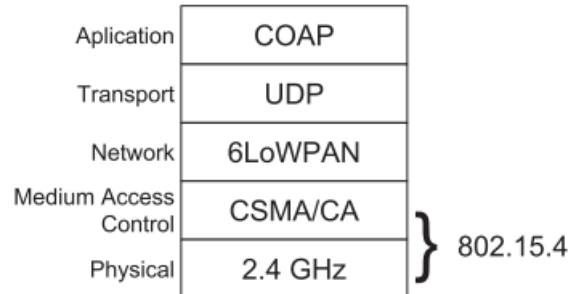


Figura 4 – Pilha de protocolos IoT. Extraído de Pacheco et al. (2016)

2.1.5.1 CoAP

De acordo com a RFC 7252 o protocolo CoAP pertencente à camada de aplicação (Tabela 1) é especializado na transferência de dados para uso em nós com recursos limitados, sendo desenvolvido para comunicação máquina a máquina (M2M, do inglês *Machine-to-Machine*) em aplicações inteligentes (SHELBY; HARTKE; BORMANN, 2014).

Com base nos conceitos do estilo de arquitetura REST, o CoAP é facilmente integrado com os protocolos existentes na Internet hoje, como por exemplo, o HTTP (*Hypertext Transfer Protocol*). Além dos recursos de integração, o protocolo ainda possui poucos *bytes* de cabeçalho, suporte à comunicação *unicast/multicast* e troca de mensagens ponto-a-ponto via UDP (SHELBY; HARTKE; BORMANN, 2014).

Sendo assim, a referida RFC ainda frisa que a comunicação estabelecida pelo protocolo está fundamentada em 4 tipos de mensagens: confirmável (CON, do inglês *Confirmable*), não-confirmável (NON, do inglês *Non-confirmable*), reconhecimento (ACK, do inglês *Acknowledgement*), *Reset* (RST) e também no modelo requisição/resposta; que pode ser visto na Figura 5. Mensagens do tipo CON são marcadas para obrigatoriamente receber uma mensagem do tipo ACK caso a comunicação tenha sido realizada com sucesso ou uma mensagem RST se houver alguma falha. O conceito de confiabilidade não é garantido nas mensagens NON, como nas do tipo CON, uma vez que o receptor não é obrigado a destinar uma mensagem ACK reconhecendo a conexão, se privando apenas a despachar uma mensagem RST quando sua condição não permitir estabelecer uma relação com o remetente.

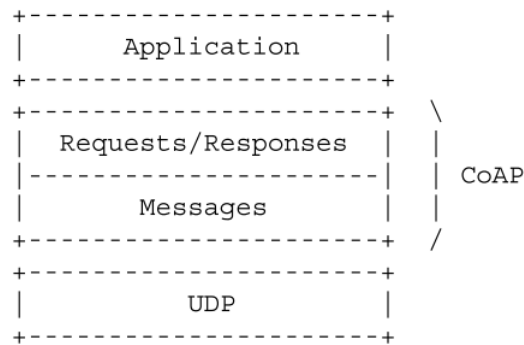


Figura 5 – Abstração das camadas do CoAP. Extraído de [Shelby, Hartke e Bormann \(2014\)](#)

2.1.5.2 UDP

A camada de transporte é responsável por fornecer a comunicação lógica entre processos de aplicações sendo executadas em hospedeiros distintos, ou seja, a aplicação ignora os detalhes da estrutura física que conecta os elementos. Neste caso, a título de exemplo, dispositivos conectados em países distintos enxergam-se como se estivessem diretamente conectados. Existem dois protocolos para esta camada: TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*) ([KUROSE; ROSS, 2013](#)).

Em conformidade com a RFC 768, o protocolo UDP não deve ser usado quando a comunicação necessita de confiabilidade na transmissão das mensagens, afinal, sua implementação não contempla o recurso de entrega confiável dos dados e não é orientado para conexão ([POSTEL, 1980](#)). Com o enfoque na simplicidade, o UDP tem o tamanho do cabeçalho reduzido e pelo fato de não ser orientado para conexão a quantidade de troca de pacotes de apresentação entre os dispositivos também é refreada, então por estes motivos, para [Olsson \(2014\)](#) o uso do UDP no paradigma IoT se torna mais viável que o TCP.

2.1.5.3 6LoWPAN e IEEE 802.15.4

O protocolo IPv4 [RFC 791] suporta cerca de 4 bilhões (2^{32}) de endereços válidos. Entretanto, devido ao fato de cada interface em cada elemento e roteador da Internet global possuir exclusivamente um endereço IP (salvo elementos que implementam o protocolo NAT [RFC 1631]), esta versão do protocolo se tornou defasada, pois a quantidade de equipamentos conectados à Internet é considerada maior que a quantidade de endereços IP possíveis. Considerando o problema de escassez de endereços válidos na arquitetura do protocolo IPv4, no início da década de 90, a IETF desenvolveu o sucessor do protocolo vigente na época, isto é, o IP versão 6 (IPv6). Esta nova versão do protocolo alterou o tamanho do endereço de IP de 32 bits para 128 bits, tornando real a possibilidade de

implantação da IoT, pois a partir desta alteração passa a ser viável a criação de 2^{128} endereços válidos (KUROSE; ROSS, 2013).

No entanto, apesar do problema de endereçamento estar resolvido, segundo Zanella et al. (2014) o novo protocolo IP não é compatível com as limitações computacionais, de memória e/ou disponibilidade dos dispositivos implantados em LoWPANs. Com o objetivo de resolver este impasse, os autores Kushalnagar, Montenegro e Schumacher (2007) publicaram a RFC 4919 onde são expostas de maneira geral as características de uma rede LoWPAN e sua relação com o IPv6.

Em primeiro lugar, Kushalnagar, Montenegro e Schumacher (2007) definem uma rede LoWPAN como sendo uma rede simples de baixo custo e largura de banda restrita que permite a conexão de dispositivos limitados computacionalmente. Em geral, estes elementos são caracterizados por seguirem o padrão IEEE 802.15.4, sendo que, os dispositivos possuem baixo custo, baixo alcance, baixa transmissão de bits e baixo desempenho, possuindo aspectos energéticos e computacionais limitados. Tais equipamentos normalmente trabalham em conjunto, com a finalidade de estabelecer uma interconexão entre o mundo real e as aplicações, como é o caso dos sensores de uma WSN; seu funcionamento está brevemente descrito na subseção 2.1.4.

Os autores precedentes citam algumas das principais características de redes LoWPANs:

- *Maximum Transmission Unit* (MTU) = 127 bytes ;
- Transferência de dados em enlaces de 250 kbps ou menos;
- Topologias padrões: estrela e malha;
- Funcionamento a partir de baterias;
- Baixo custo de produção;
- Habitualmente, são lançados inúmeros dispositivos no meio sem local pré-determinado;
- Uma quantidade considerável destes elementos são de difícil acesso e não devem requerer intervenção humana para atualizações ou manutenções.

A atuação do protocolo IPv6 paralelamente com a rede mencionada viabiliza a comunicação com outros dispositivos IP, pois, a rede terá acesso à infraestrutura web existente, na qual já existem ferramentas de diagnóstico, monitoramento e gerenciamento em funcionamento. Contudo, pelo fato da arquitetura IEEE 802.15.4 impor restrições à pilha de protocolos IoT, viu-se necessário o desenvolvimento do 6LoWPAN que atua como um compressor de cabeçalhos para os protocolos IPv6 e UDP (ZANELLA et al., 2014).

Deste modo, segundo a RFC 6282, em virtude da adaptação no formato dos protocolos citados anteriormente o 6LoWPAN propiciará que pacotes IPv6 sejam transferidos via redes que levam em consideração a limitação de banda, memória e/ou recursos energéticos (THUBERT, 2011).

2.1.6 Ferramentas

Nesta seção do trabalho serão expostos os materiais que foram utilizados ao decorrer do projeto. As subseções 2.1.6.1, 2.1.6.2 e 2.1.6.3 tratam das ferramentas utilizadas para criação/análise dos dados.

2.1.6.1 Simulador de redes ns-3

O ns-3 é um simulador de redes para pesquisas e de uso educacional, desenvolvido por pesquisadores. É um *software open source* que conta com contribuições da comunidade no desenvolvimento de novos modelos, correções de bugs e compartilhamento de resultados. O ambiente de desenvolvimento é feito em C++ ou Python, sendo os modelos e tutoriais previamente elaborados majoritariamente escritos em C++. Todos os códigos-fonte devem ser compilados utilizando o compilador próprio baseado em Python do ns-3, nomeado *waf*, que é responsável por gerar os binários dos documentos (ns-3 project, 2018b).

2.1.6.2 NetAnim

O NetAnim é um *software* usado para animar as simulações realizadas no ns-3 usando um arquivo de rastreamento XML coletado durante a simulação. Na Figura 6, segue a *Graphical User Interface* (GUI) do programa simulando 53 nós em processo de comunicação, onde o nó número 37 envia pacotes em *broadcast*, isto é, para todos os outros nós da rede (ns-3 project, 2018a).

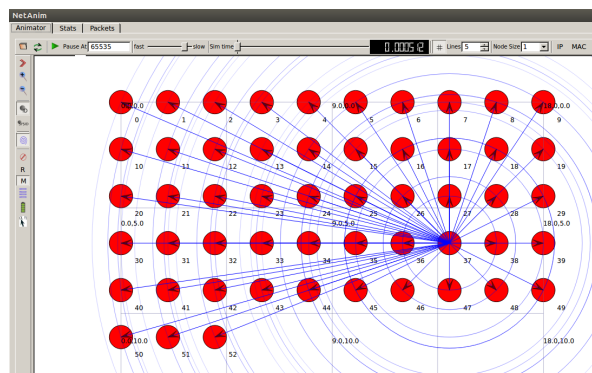


Figura 6 – Interface gráfica do NetAnim com 53 nós dispostos em formato malha se comunicando

2.1.6.3 Wireshark

O Wireshark é uma ferramenta para análise de pacotes inicialmente desenvolvida em meados de 1998. É um *software* livre multiplataforma divulgado sob a licença GNU GPL (do inglês, *General Public License*) que possui o intuito de auxiliar na análise e solução de problemas relacionados à comunicação entre dispositivos ([The Wireshark team, 2018](#)).

Mediante alterações nos parâmetros: quantidade de sensores e taxa de injeção do tráfego e tamanho/quantidade de pacotes enviados, foram executadas várias simulações do ambiente de testes proposto pelo [Pacheco et al. \(2016\)](#), sendo o algoritmo implementado para resultar um arquivo de extensão .pcap que possui os dados de todas as interações entre os elementos envolvidos. Consequentemente, o Wireshark permite analisar a comunicação do protocolo CoAP entre os nós e facilita a coleta das informações usadas na confecção de relatórios e arquivos resultantes da análise dos objetos ([The Wireshark team, 2018](#)).

2.2 Trabalhos correlatos

O objetivo principal do trabalho de [Furfaro et al. \(2016\)](#) foi avaliar os efeitos de ataques DDoS em protocolos da camada de aplicação funcionando sob o protocolo UDP. Para isso, os autores desenvolveram um script usando o simulador de redes *NeSSi* que foi capaz de testar a efetividade dos sistemas de defesa/reação diante de ataques DDoS por amplificação e reflexão nos protocolos DNS (do inglês, *Domain Name System*) [RFC 1034/1035] e NTP (do inglês, *Network Time Protocol*) [RFC 928]. Na constituição do ambiente de simulações, foi usada uma *botnet* com 150 dispositivos explorando a vulnerabilidade de 3 servidores com largura de banda disponível em 200 Mbit/s. Os experimentos foram executados por 20 segundos com intenção de monitorar a utilização da banda apoiada em três pontos de referência:

- Do ponto de vista de um dispositivo zumbi dentro da sub-rede;
- Monitoramento singular para cada servidor;
- Por fim, foi observado a reação total do ataque mediante uma conexão entre a vítima e os servidores.

A Figura 7 mostra a evolução do sobrecarregamento da banda disponível para os protocolos NTP e DNS, sendo representados pelas linhas, vermelha e preta, respectivamente. Conforme exposto pelos pesquisadores, em ambos os ataques, as taxas de crescimento foram idênticas. No entanto, o ataque sob o protocolo NTP mostrou-se 300%

maior. Este resultado foi observado devido o fato do NTP gerar a proporção de 23:1 pacotes em relação ao DNS.

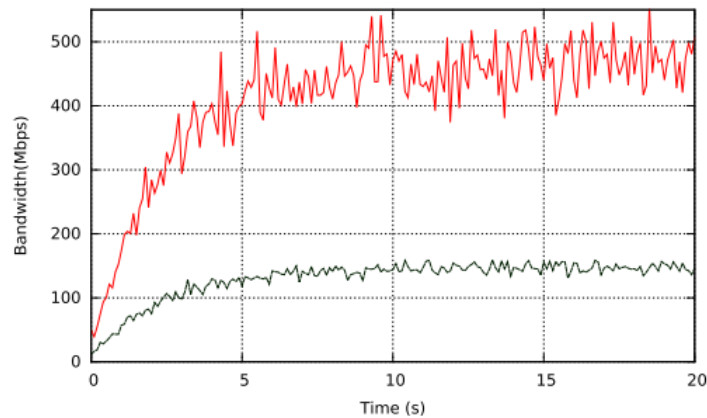


Figura 7 – Comparação entre o impacto do ataque no protocolo DNS e NTP. Extraído de [Furfaro et al. \(2016\)](#)

Já no trabalho desenvolvido por [Hengst \(2016\)](#), o intuito primário foi avaliar o potencial de dispositivos IoT como refletores em ataques DDoS por reflexão. Para este fim, o autor analisou os doze maiores ataques buscando saber quais dispositivos poderiam se tornar zumbis em um ambiente de rede e por fim observou a influência de fatores como disponibilidade do elemento e largura de banda do meio. Foram usados aplicativos como Nmap para escanear as portas abertas na rede, na qual foi possível definir quais serviços estavam ativos nesse dispositivo e uma vez encontrada essa informação, a partir do Scapy (ferramenta para manipulação de pacotes), essas portas receberam vários pacotes posteriormente analisados usando o Wireshark. Portanto, dispositivos ligados ao paradigma da Internet das Coisas podem se tornar refletores em ataques distribuídos de negação de serviço, desde que observados alguns fatores como disponibilidade, usabilidade e acessibilidade. Para o ano de 2020 espera-se que o número de dispositivos que poderão ser usados nesse tipo de ataque está próximo à 24 bilhões, sendo que apenas 0.1% do total de elementos disponíveis para o referido ano, gerou algo em torno de 36.28 Tbps de dados, equivalente à 123.83% mais dados que o maior ataque conhecido até aquele período.

A complexidade na implementação de métodos avançados de proteção para os elementos IoT, os torna vulneráveis à diversos tipos de ataques, tais como os Ataques Distribuídos de Negação de Serviço, pois, se apresentam mais simples de serem elaborados. O trabalho proposto por [Peraković, Periša e Cvitić \(2015\)](#) expõe a dificuldade em prover a disponibilidade, confidencialidade e integridade de informações e serviços em dispositivos IoT, ademais tendo como objetivo identificar os tipos de ataques DDoS com os maiores índices de ameaça, bem como os métodos de proteção para as amostras identificadas.

Estatisticamente foram analisados dados gerados em ataques DDoS durante o

período de 2 anos entre 2013 e 2015, onde foi possível identificar que dentre os vários tipos de ataques DDoS o mais comum foi explorando o protocolo SSDP (do inglês, *Simple Service Discovery Protocol*) responsável pela detecção de dispositivos UPnP (do inglês, *Universal Plug and Play*). De acordo com os autores, o motivo dessa larga proporção de ataques baseados nos protocolos referenciados anteriormente está no fato da crescente implementação da comunicação M2M empregada no conceito IoT.

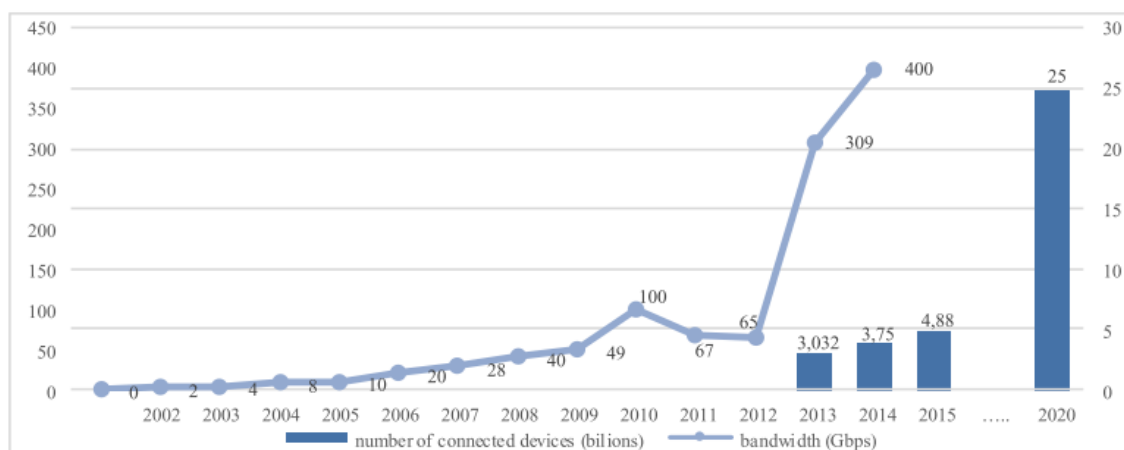


Figura 8 – Taxa de crescimento do número de dispositivos conectados e ataques DDoS. Extraído de [Peraković, Periša e Cvitić \(2015\)](#)

A Figura 8 indica o crescimento de dispositivos baseados em IoT conectados à Internet e sua relação com o tráfego gerado pelos ataques DDoS. Após 2013, o expressivo aumento na extensão dos ataques se dá pelo fato do número de dispositivos com recursos limitados e baixos níveis segurança implementados serem facilmente captados para atuarem em *botnets* capazes de gerar significantes quantidades de tráfego para uma determinada vítima.

Existe uma relação muito próxima entre os trabalhos citados na seção 2.2 e o artigo originador deste experimento. A pesquisa desenvolvida pelo [Furfaro et al. \(2016\)](#), mostrou que os dispositivos IoT ainda estão muito frágeis e não possuem sistemas de defesa/reação apropriados contra ataques DDoS. Paralelamente [Hengst \(2016\)](#) exprime uma preocupação com a quantidade de dispositivos que estarão interconectados e a capacidade de se tornarem refletores de dados no futuro. Outrossim, [Peraković, Periša e Cvitić \(2015\)](#) salienta um vultoso crescimento na extensão de ataques DDoS em decorrência do aumento considerável de dispositivos IoT conectados à Internet, sendo estes caracterizados por níveis de segurança não tão elevados e por possuírem recursos de processamento e armazenamento limitados.

Para consolidar essas ideias, o artigo desenvolvido pelo [Pacheco et al. \(2016\)](#) destaca a potencialidade desses dispositivos serem protagonistas em ataques DDoS por amplificação e reflexão, como provado no próprio ataque do *malware* Mirai. Portanto, em

consequência de todos esses dados e da incerteza diante de um futuro potencialmente arriscado para a Segurança da Informação, este trabalho se mostra necessário para verificar se existem restrições na própria arquitetura IoT que poderão ser abordadas por pessoas mal-intencionadas e que podem ser eventualmente preservadas com suporte de ferramentas desenvolvidas a partir da evolução de pesquisas na área. Ademais, também é importante discutir as diferentes métricas que servirão de apoio para analisar o impacto dos ataques. Fatores como largura de banda, quantidade/tamanho dos pacotes e a taxa de injeção do tráfego são apenas alguns dos atributos a serem explorados pelos atacantes.

3 Desenvolvimento

O capítulo a seguir expõe na seção 3.1 as características do ambiente de simulação e a metodologia pelo qual os experimentos foram elaborados. O produto das simulações, presente na seção 3.2, se divide em duas partes, a primeira delas apresenta as simulações com 1, 3 e 5 sensores, nessa ordem, as subseções 3.2.1, 3.2.2 e 3.2.3. A segunda parcela mostra os resultados alcançados com a contribuição da ferramenta *DyNetVis* em simulações com 50 e 100 sensores (3.2.4). Em seguida, na subseção 3.2.5 são apresentadas algumas discussões sobre os resultados obtidos com a alteração de parâmetros já mencionados.

3.1 Metodologia

Os cenários de testes estão baseados numa topologia estrela com 1, 3, 5, 50 e 100 nós, dispostos "fisicamente" em malha com 2 metros de espaçamento entre eles; visto na Figura 6. A topologia em estrela tornou-se mais adequada, pois a comunicação e gerenciamento da rede de sensores sem fio se dá a partir do nó coordenador. No presente ambiente de simulação, evidenciado na Figura 9, foi programado para que existam sempre um nó coordenador da RSSF, isto é, aquele que é responsável por gerenciar e estruturar a comunicação entre os demais nós; um atacante que enviará as solicitações com o IP de origem falsificado em *broadcast*; os outros sensores presentes no meio e por fim a própria vítima que está fora da WSN.

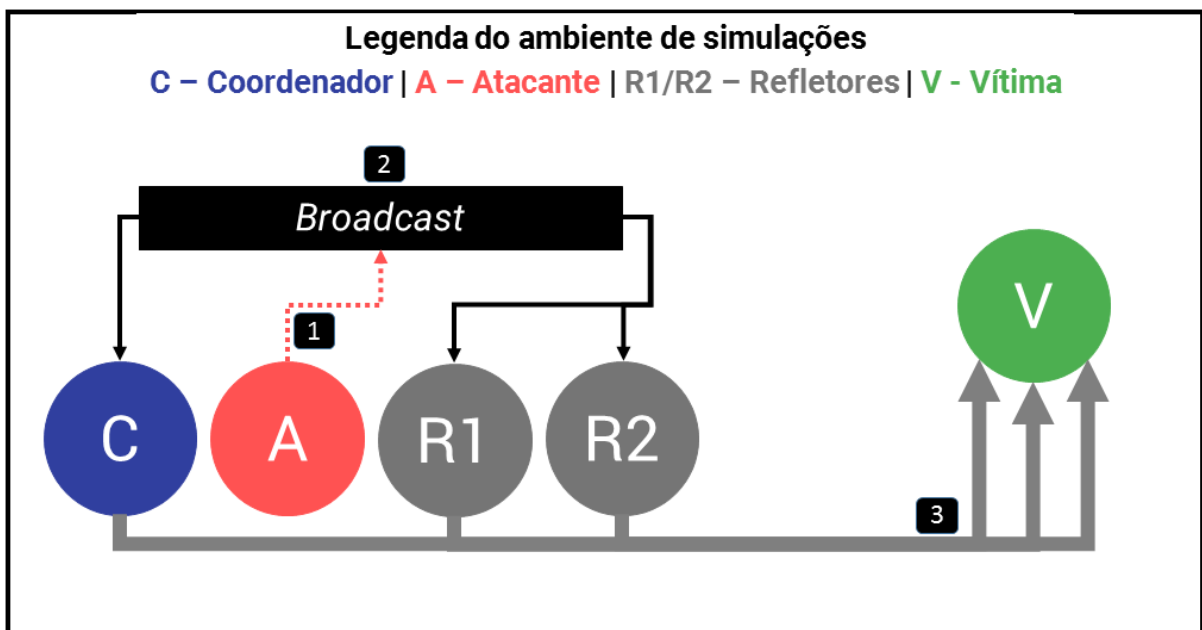


Figura 9 – Funcionamento do ataque DDoS na rede WSN deste trabalho

Diante da discussão exposta na seção 2.2, pode-se chegar a conclusão de que em virtude da grande quantidade de dispositivos interconectados no futuro existe uma preocupação quanto à segurança desse ambiente. Portanto, para avaliar o impacto de dispositivos IoT em ataques DDoS, os cenários foram desenvolvidos de tal modo a explorar a função de descobrimento de serviço do CoAP. A rede possui um nó malicioso infiltrado que envia solicitações de descoberta de serviço para todos os sensores (comunicação em *broadcast*), conforme pode ser visualizado no passo número 1 da Figura 9. Como característica fundamental do protocolo CoAP, assim que um sensor recebe uma requisição, ele deve imediatamente enviar uma resposta informando quais serviços ele suporta, segue-se assim o número 2 da Figura 9, na qual mostra os sensores recebendo os pacotes e consequentemente enviando a resposta para a vítima.

É válido ressaltar que o tamanho da resposta enviada pelos refletores é aumentado pela taxa de amplificação e perante o que foi descrito cada sensor adicionado e o coordenador da WSN, deverá ser considerado como refletores de pacotes, isto é, dentro do cenário elaborado para este trabalho apenas o atacante e a vítima não refletirão dados.

Semelhante ao ataque *Smurf* o atacante explora uma vulnerabilidade na função de descobrimento de serviço implementada pelo CoAP, em outras palavras, ele envia um pacote de requisição marcado com a *flag* CON (seção 2.1.5.1) de tamanho padrão 20 bytes para todos os sensores da rede que ao receberem este tipo de requisição são obrigados a enviar uma resposta ao remetente como mencionado anteriormente. No entanto, o pacote está com o IP falsificado, ou seja, o IP de origem foi alterado para o IP da vítima.

Dito isso, atribui-se aos ataques simulados por este trabalho, como sendo ofensores da disponibilidade do sistema, pois, o modo de organização do ambiente das simulações mostra que o objetivo do ataque é reduzir os recursos de processamento e de banda disponível da vítima. É pertinente salientar que o nível de criticidade do ataque dependerá de qual elemento é escolhido como vítima bem como os serviços por ela implementados. O grau de automação do ataque é definido como semi-automático com comunicação direta.

Como esperado de uma rede WSN (veja a seção 2.1.4), os sensores desta simulação executam apenas a função de coletar a temperatura do ambiente, logo, ao renderizar esta informação o pacote de resposta obtém o tamanho de 61 bytes, equivalente à 3.05 de taxa de amplificação para cada dispositivo.

As simulações foram executadas por 60 segundos, na qual a quantidade de pacotes por segundo (PPS) enviada pelo atacante define a taxa de injeção dos dados. Logo, uma taxa de 0.16 kbps equivale a 1 pacote de requisição por segundo transmitido para todos os sensores. Os experimentos foram divididos conforme a quantidade de sensores adicionados. É relevante dizer que o nó coordenador foi considerado apenas na elaboração dos cálculos, ou seja, o experimento que estiver descrevendo possuir x ($x > 0$) sensor (es), possuirá $(x + 1)$ sensores para efeito estatísticos/matemáticos. Por exemplo, a seção 3.2.3

trata dos resultados encontrados para a simulação usando 5 sensores, então, para efeitos estatísticos/matemáticos o coordenador foi considerado, logo, este experimento possui 6 sensores transmitindo informações e assim segue-se para todos os demais resultados deste trabalho.

Ante o exposto e com base no trabalho conduzido por Pacheco et al. (2016) foi construída a tabela 2 que representa as características do trabalho desenvolvido pelos autores mencionados e este trabalho. Os valores que estiverem marcados de negrito na coluna "Este trabalho" destaca os parâmetros dissemelhantes. A partir da linha "Tipo de ataque" os atributos são idênticos.

Características de cada trabalho		
Atributo	Trabalho do Pacheco et al. (2016)	Este trabalho
Tamanho do pacote de requisição	20 Bytes	20 / 40 Bytes
Taxa de injeção do tráfego	0.16 / 1.6 / 3.2 / 4 / 8 / 16 Kbps	0.16 / 1.6 / 1.92 / 2.8 / 3.2 / 4 / 8 / 16 / 24 / 32 / *64 Kbps
Quantidade de PPS enviados	1 / 10 / 20 / 25 / 50 / 100	1 / 10 / 12 / 13 / 20 / 25 / 50 / 100 / 150 / 200
Quantidade de sensores	5 / 25 / 50 / 75 / 100	1 / 3 / 5 / 50 / 100
Métrica	Taxa de amplificação dos dados	Taxa de amplificação dos dados
	Tráfego total gerado	Tráfego total gerado
	Média do tráfego gerado para cada nó	Amplificação média de pacotes
		Pacotes enviados
Tipo de ataque	DDoS por reflexão e amplificação	
Topologia	Estrela	
Duração da simulação	60 segundos	
Pilha de protocolos	CoAP / UDP / 6LowPAN / IEEE 802.15.4	
Tipo de sensores	Coordenador / atacante / vítima	
Serviço implementado	Temperatura	

Tabela 2 – Diferenças e semelhanças entre as simulações elaboradas pelo Pacheco et al. (2016) e este trabalho

Em relação às diferenças apresentadas na tabela 2, o tamanho do pacote de requisição teve seu valor dobrado para que fosse analisado o comportamento da rede frente à maiores quantidades de dados. A taxa de injeção foi alterada entre 1.92, 2.8, 24, 32 e 64 Kbps (12/13/150/200 PPS), tendo em conta os resultados obtidos pelos autores principais. O motivo da taxa de injeção do tráfego referente à 64 Kbps estar marcada com um asterisco é porque ela foi obtida por causa do aumento do tamanho do pacote de 20 bytes para 40 bytes, diferentemente das outras taxas que foi aumentando a quantidade de pacotes enviados por segundo.

Além da taxa de amplificação do tráfego, foi proposto considerar a amplificação da quantidade de PPS enviado pelos nós para a vítima, desta maneira, se tornou viável verificar se a rede conseguiu responder os pacotes de requisição recebidos proporcionalmente ou se houve alguma queda nesta taxa. Por fim, com o intuito de simular redes de menor porte, foram realizados os testes com 1 e 3 sensores apenas, visto que a quantidade mínima usada pelos autores foram 5 sensores.

3.2 Resultados

Os resultados foram divididos em duas partes: a primeira mostra as simulações realizadas com 1, 3 e 5 sensores (subseções: 3.2.1, 3.2.2 e 3.2.3, respectivamente), onde serão expostos: a quantidade absoluta de pacotes enviados pelos sensores para seus respectivos destinos, a métrica de amplificação média dos pacotes e a relação entre o tráfego do atacante e o tráfego refletido pelos sensores. A segunda parte dos resultados, na subseção 3.2.4 apresenta os resultados alcançados com o auxílio do *software DyNetVis* nas simulações com 50 e 100 sensores, pelo qual foram alteradas a quantidade de PPS, a taxa de injeção de dados e tamanho do pacote de requisição. A seção 3.2.5 destaca as discussões sobre os resultados atingidos.

3.2.1 1 Sensor

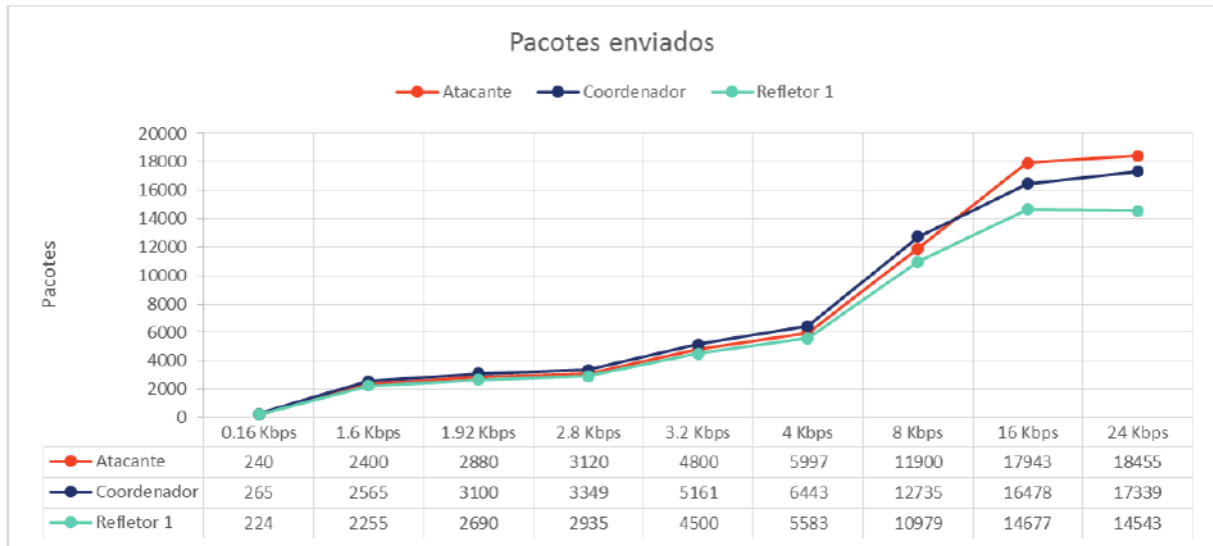


Figura 10 – Quantidade de pacotes enviados por cada nó (1 Sensor)

A Figura 10 representa a quantidade de pacotes que cada sensor presente na rede enviou para o meio, sendo o atacante responsável por enviar os pacotes de requisição em *broadcast* e os demais enviados para a vítima. Além de ser o único sensor adicionado no experimento, o coordenador também atua como refletor, isto é, recebe pacotes do nó malicioso, amplifica-os e os envia para a vítima. Observa-se na Figura 10 que o comportamento da rede mantém-se semelhante perante a taxa de injeção do atacante variando entre 0.16 Kbps e 8 Kbps, de tal forma que o coordenador diante desta situação conseguiu refletir mais de 100% dos pacotes recebidos e mesmo o sensor complementar ficando continuamente abaixo do seu vizinho, a com a taxa de reflexão mantendo-se sem muita discrepância. Entretanto, a partir de 16 Kbps, o desempenho do coordenador cai em relação ao atacante, mas sua diferença entre o sensor adicional acaba aumentando.

A Figura 11 representa, em média, o quanto a rede conseguiu refletir dos pacotes enviados pelo atacante. Como observado, executando a simulação com 1 sensor (além do coordenador e atacante), a rede se comporta bem até 4 Kbps, refletindo mais de 100% dos pacotes recebidos. Entretanto, a partir de 8 Kbps, os refletores começam a perder pacotes, pois o fluxo acaba sendo muito alto.

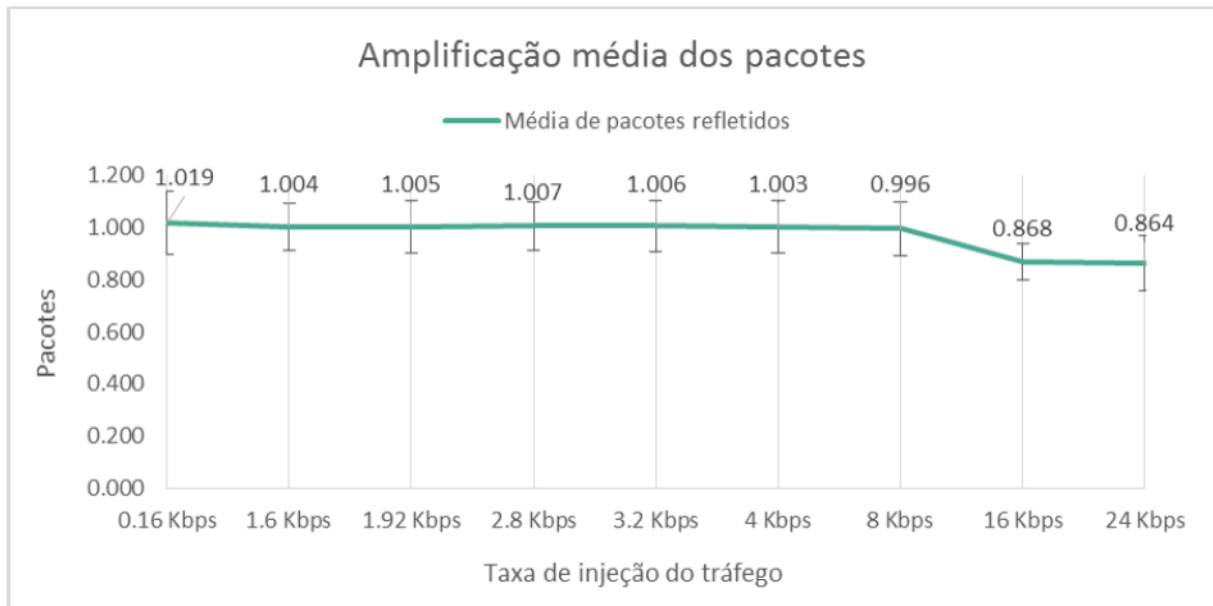


Figura 11 – Amplificação média do número de pacotes enviado para a rede por cada sensor (1 Sensor)

A Figura 12 foi gerada com o intuito de melhorar a visualização da quantidade de dados enviados para a rede pelo atacante e o quanto esses dados foram amplificados e enviados para a vítima. É possível observar que no último cenário do experimento (24 Kbps) o tráfego passa de 7.57 MB para 36.03 MB, mostrando assim uma amplificação de 4.75 vezes.

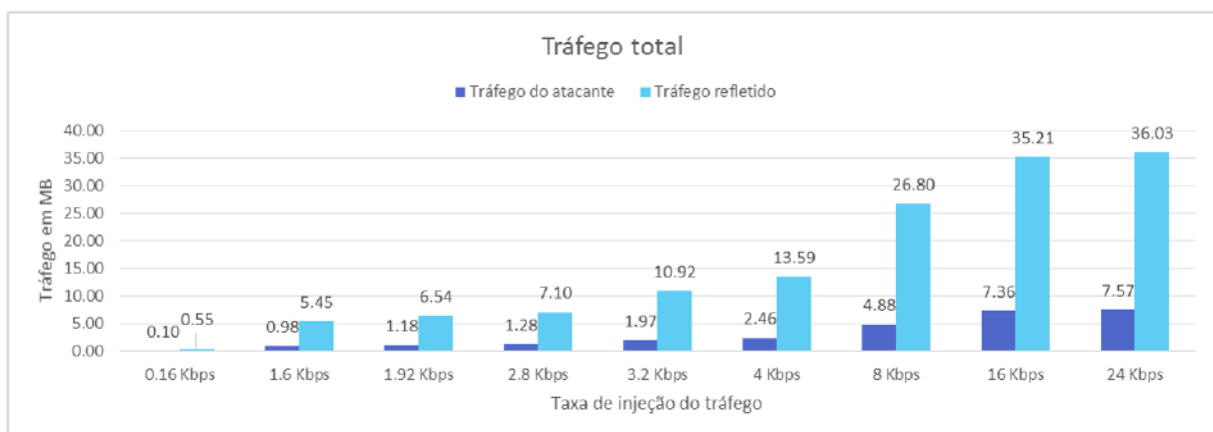


Figura 12 – Tráfego gerado pelo atacante e tráfego amplificado pelos refletores (1 Sensor)

3.2.2 3 Sensores



Figura 13 – Quantidade de pacotes enviados por cada nó (3 Sensores)

Observa-se na Figura 13 que o comportamento da rede mantém-se semelhante perante a vazão do atacante variando entre 0.16 Kbps e 4 Kbps, de tal forma que o coordenador diante desta situação conseguiu refletir boa parte dos pacotes recebidos e mesmo os sensores complementares ficando continuamente abaixo, a taxa de reflexão manteve-se relativamente invariável. Entretanto, a partir de 8 Kbps há uma degradação no desempenho dos demais sensores em relação ao atacante, chegando à uma diferença máxima de aproximadamente 7585 pacotes no último cenário da simulação.

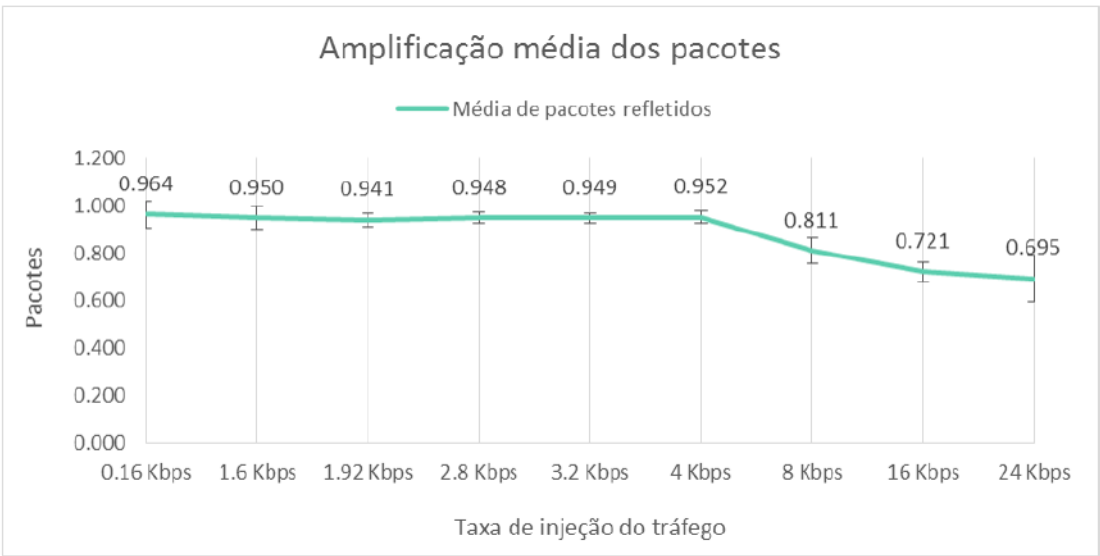


Figura 14 – Amplificação média do número de pacotes enviado para a rede por cada sensor (3 Sensores)

A Figura 14 mostra que a rede consegue refletir cerca de 95% dos pacotes que ela recebe até a taxa de vazão do atacante permear os 4 Kbps. A partir de 8 Kbps, os refletores não conseguem processar a quantidade de pacotes recebidos do atacante e a rede perde recursos de processamento progressivamente chegando à cerca de 30% dos pacotes no cenário com a taxa de injeção à 24 Kbps.

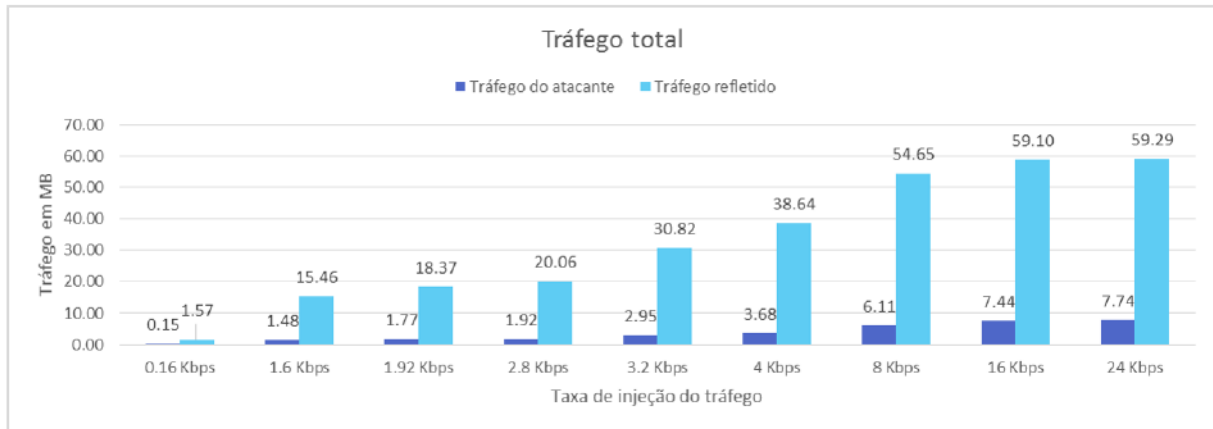


Figura 15 – Tráfego gerado pelo atacante e tráfego amplificado pelos refletores (3 Sensores)

Com a Figura 15 visualiza-se que no último cenário do experimento (24 Kbps) o tráfego evolui de 7.74 MB para 59.29 MB, mostrando assim uma amplificação de 7.66 vezes, isto é, um valor 2.89x maior que o experimento anterior usando apenas 1 sensor. É também perceptível que a quantidade de dados que o atacante enviou para a rede permanece quase sem nenhuma alteração nas taxas de injeção de 16/24 Kbps tanto dentro da própria simulação com 3 sensores, quanto em relação ao experimento anterior. Este comportamento onde os níveis indicam uma estagnação, evidencia o fato de que a rede começa a diminuir o desempenho, isto é, a quantidade de dados enviados pelo atacante se torna superior ao processamento dos sensores.

3.2.3 5 Sensores

A Figura 16 mostra que durante a simulação houve variações em todos os níveis de vazão da rede, podendo definir os refletores 2 e 5 como aqueles que tiveram mais dificuldade em refletir os pacotes do atacante, posto que no total de 19071 PPS enviados pelo atacante, eles conseguiram refletir apenas 10126 e 10653, respectivamente. O refletor 4 obteve níveis elevados chegando a ser o 2º nó que mais refletiu pacotes à 8 Kbps, perdendo apenas para o coordenador. Entretanto, após essa vazão sua performance caiu drasticamente até atingindo o antepenúltimo lugar na quantidade de pacotes refletidos. Por fim, pode-se observar que a diferença entre quantidade de pacotes enviados pelo atacante e a quantidade de pacotes refletidos pelos sensores é proporcionalmente definido pelo aumento da taxa de injeção do tráfego.

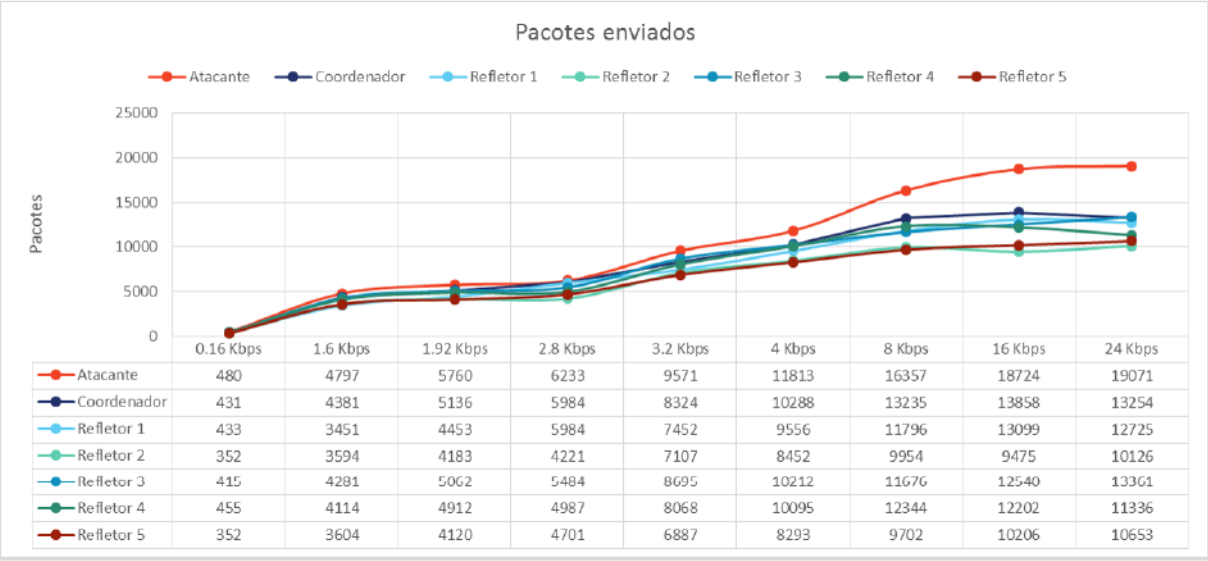


Figura 16 – Quantidade de pacotes enviados por cada nó (5 Sensores)

No cenário descrito pela Figura 17, percebe-se que a rede perde cerca de 15% a 20% dos pacotes que deveriam ser refletidos com as taxas de vazão entre 0.16 Kbps e 4 Kbps, sendo seu melhor nível à 2.8 Kbps, pois mesmo a média da vazão à 0.16 Kbps sendo maior, a quantidade de pacotes enviados é menor. A partir de 8 Kbps os níveis caem gradativamente, de forma que ao final da simulação apenas 62% dos pacotes recebidos estão sendo refletidos. Os resultados obtidos com 5 sensores demonstraram diferenças significativas perante os resultados alcançados com 1 e 3 sensores em todas as métricas apresentadas, especialmente na exposta pela Figura 17, onde são perceptíveis as alterações na taxa de amplificação desde os primeiros níveis de injeção de tráfego.

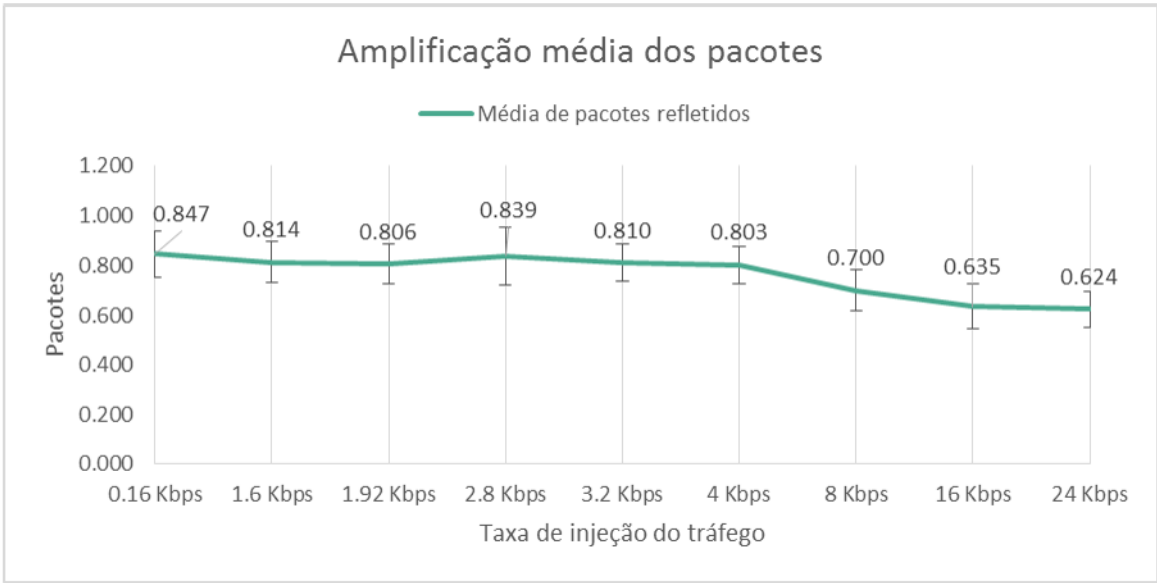


Figura 17 – Amplificação média do número de pacotes enviado para a rede por cada sensor (5 Sensores)

Uma característica que a Figura 18 mostra é que não houve diferença significativa entre os valores das taxas de vazão mais elevadas, pois a rede nesse ponto já se mostrava saturada com a quantidade de pacotes recebidos. O melhor resultado é encontrado com uma taxa de injeção de tráfego de 2.8 Kbps, chegando a amplificar 13.84 vezes a quantidade de dados recebidos.

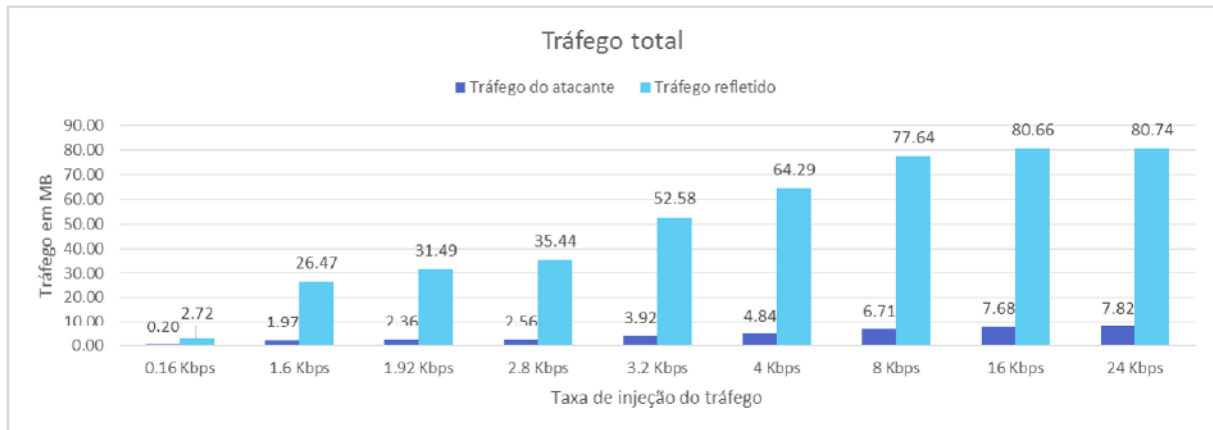


Figura 18 – Tráfego gerado pelo atacante e tráfego amplificado pelos refletores (5 Sensores)

3.2.4 50 e 100 sensores

A primeira parcela desta subseção apresenta as Figuras 19 e 20 que representam a taxa de amplificação total do tráfego e a relação entre o tráfego enviado pelo atacante e o tráfego refletido pelos demais sensores em simulações realizadas com 50 sensores. A segunda fração, apresenta os resultados obtidos com o auxílio da ferramenta de visualização de dados *DyNetVis* desenvolvida por Linhares et al. (2017). Em ambos os casos, no cenário representado pela taxa de injeção do tráfego sendo igual à *64 Kbps, o tamanho do pacote de requisição foi alterado de 20 para 40 bytes.

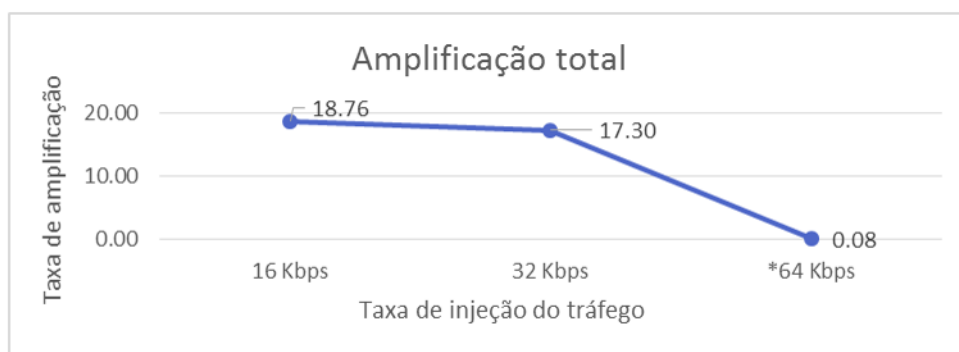


Figura 19 – Amplificação total das simulações com 50 sensores

Na Figura 19 constata-se que a taxa de amplificação do tráfego não obteve o resultado eficaz diante dos cenários, uma vez que o resultado máximo esperado seria o

total de 155.55, correspondente à 3.05 vezes o total de 51 sensores. Para o cenário com uma taxa de injeção do tráfego igual a 16 Kbps, o resultado se mostrou 88% inferior ao esperado e mesmo dobrando a taxa de vazão do atacante, a rede se mostrou ainda mais congestionada, apresentando um resultado aproximadamente 89 vezes menor que o total aguardado.

Para o último cenário simulado, apenas 0.05% dos pacotes recebido pela rede foi refletido para a vítima, mostrando a total exaustão dos protocolos responsáveis pela comunicação dos sensores. Em números absolutos, o tráfego total para os cenários com 16 e 32 Kbps deveria estar entre 311 e 622.2 MB, já para 64 Kbps a vítima estaria recebendo um ataque total de 1.24 GB, contudo, como visualizado na Figura 20 o tráfego obtido com as simulações não alcançaram números satisfatórios, sendo o tráfego total máximo refletido igual à 44.21 MB.

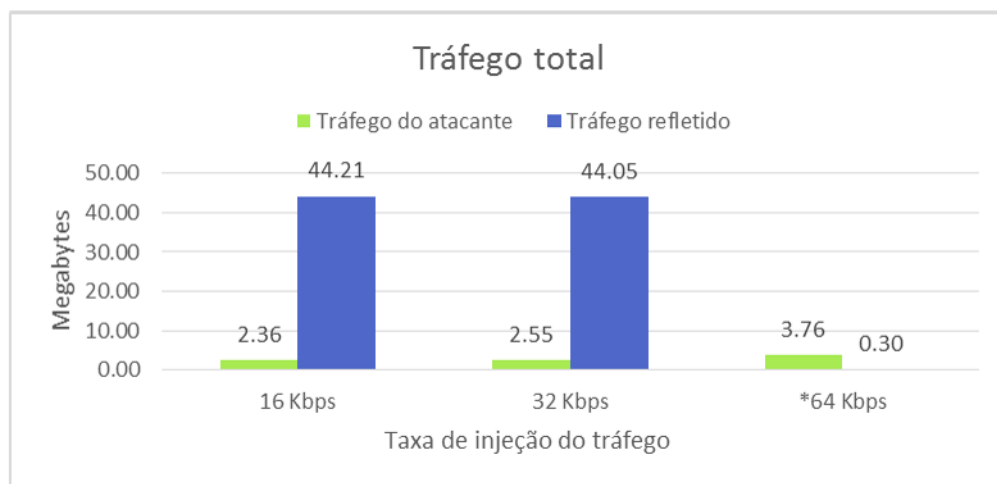


Figura 20 – Tráfego gerado pelo atacante e tráfego amplificado pelos refletores (50 Sensores)

Com o intuito de melhorar a percepção do comportamento da rede durante o ataque, decidiu-se usar uma abordagem visual nos dados. O Sistema de Visualização de Redes Dinâmicas (DyNetVis, do inglês *Dynamic Network Visualization System*), fornece diferentes tipos de análise das dimensões temporais e estruturais em redes complexas formadas por conexões entre nós. Com o auxílio da visualização temporal, que implementa recursos que expõem as atividades dos nós (MSV, do inglês *Massive Sequence View*) e uma técnica de ordenação lexicográfica que organiza os nós em ordem alfabética, tornou-se mais imediata a realização da análise da comunicação entre os sensores (LINHARES et al., 2017).

A linha gráfica é uma forma de representar dados e visualizar a evolução do número de conexões ao longo do tempo (LINHARES et al., 2017). É importante frisar que devido protocolo IEEE 802.15.4 implementar o conceito de CSMA/CA, durante a simulação não há 2 ou mais nós se comunicando com o mesmo destino simultaneamente, ou seja, isso só

acontece nas figuras produzidas pelo *DyNetVis* em razão da resolução que foi utilizada na elaboração das visualizações, para facilitar a compreensão.

Para a melhor compreensão das figuras a seguir, define-se:

- P - Pacote de requisição em bytes;
- S - Sensores;
- T - Taxa de injeção do tráfego em Kbps;
- Exemplo: *50S16T20P*, é o mesmo que a simulação de 50 Sensores com 16 Kbps de taxa de injeção do tráfego e 20 Bytes para o tamanho dos pacotes de requisição.

A fração da linha gráfica obtida na simulação *50S16T20P* exibida na Figura 21 mostra que a rede se mantém estável, visto que em vários períodos de tempo existe a mesma quantidade de sensores se comunicando. Dificilmente verifica-se a falta de progressão tanto na subida quanto na descida da linha, sendo contabilizada no máximo 7 sensores se comunicando com a vítima concomitantemente.

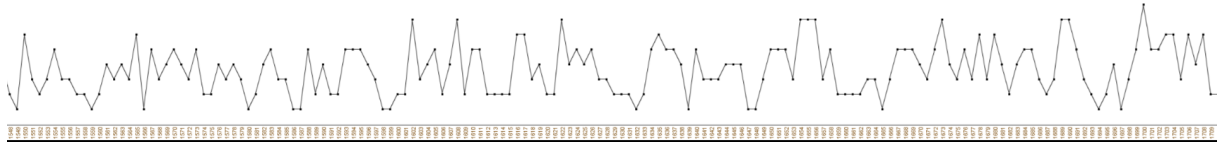


Figura 21 – Linha gráfica da simulação com 50 sensores, 16 Kbps e pacote de requisição 20 Bytes

Além da linha gráfica, a visualização MSV, que disponibiliza informações das atividades dos nós, auxilia na análise da comunicação entre os pares de sensores. Para isso, foram aplicados alguns recursos policromáticos. Cada sensor é representado por um círculo e, se há conexão entre os nós, a aresta que conecta os dois sensores também é evidenciada. A tabela 3 exibe a legenda para as cores utilizadas nas figuras elaboradas utilizando o *DyNetSis*:

Nós	Aresta	Cor
Coordenador	Cordenador ->Vítima	Vermelho
Sensores	Sensor ->Vítima	Azul
Vítima	Sensor ->Coordenador	Verde

Tabela 3 – Legenda de cores para visualização MSV produzida pelo sistema *DyNetVis*

A Figura 22 que representa a simulação *100S16T20P* mostra um comportamento estável da rede semelhante à Figura 21. Analisando a linha gráfica deste experimento, é possível identificar que há vários períodos de tempo em que a mesma quantidade de nós se

comunica com a vítima e existe a mesma progressão crescente e decrescente na quantidade de elementos conectados paralelamente. No entanto, o que difere os resultados entre ambos os experimentos, é que na simulação com 100 sensores há momentos que a comunicação entre os nós é cessada evidenciando certo desgaste de recursos da rede. Para este último caso, onde não há comunicação entre os nós, a visualização MSV facilita na análise, porque basta encontrar as lacunas em branco na parte superior da figura e perceber que a linha está alocada em 0 comunicações simultâneas. Os padrões mencionados são constatados tanto na visualização deste experimento quanto nas simulações de *50S16T20P* e *50S32T20P*.

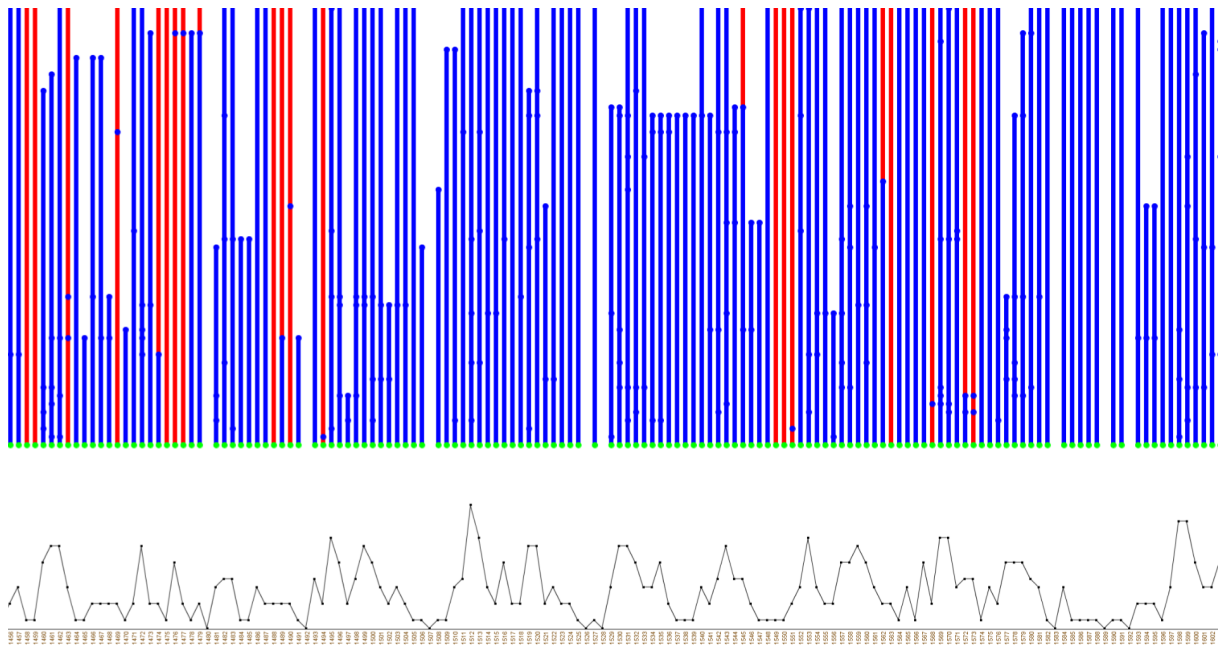


Figura 22 – Fragmento da visualização completa da simulação com 100 sensores, 16 Kbps e pacote de requisição 20 Bytes

Por fim, o resultado mais expressivo foi obtido quando o tamanho do pacote de requisição foi dobrado para 40 bytes. A figura 23 que representa a simulação *50S64T40P* apresenta características que a difere das Figuras 21 e 22, sendo elas:

- A presença de poucas conexões simultâneas entre os nós, simbolizadas por um padrão comum evidente na linha gráfica exibida na parte inferior da Figura 23;
- A ausência de picos elevados nesta mesma linha gráfica que destacaria mais quantidades de nós se comunicando entre si;
- A quantidade elevada de lacunas entre cada período de tempo, demonstrando a exaustão dos recursos da rede, visto a falta de comunicação entre os sensores.

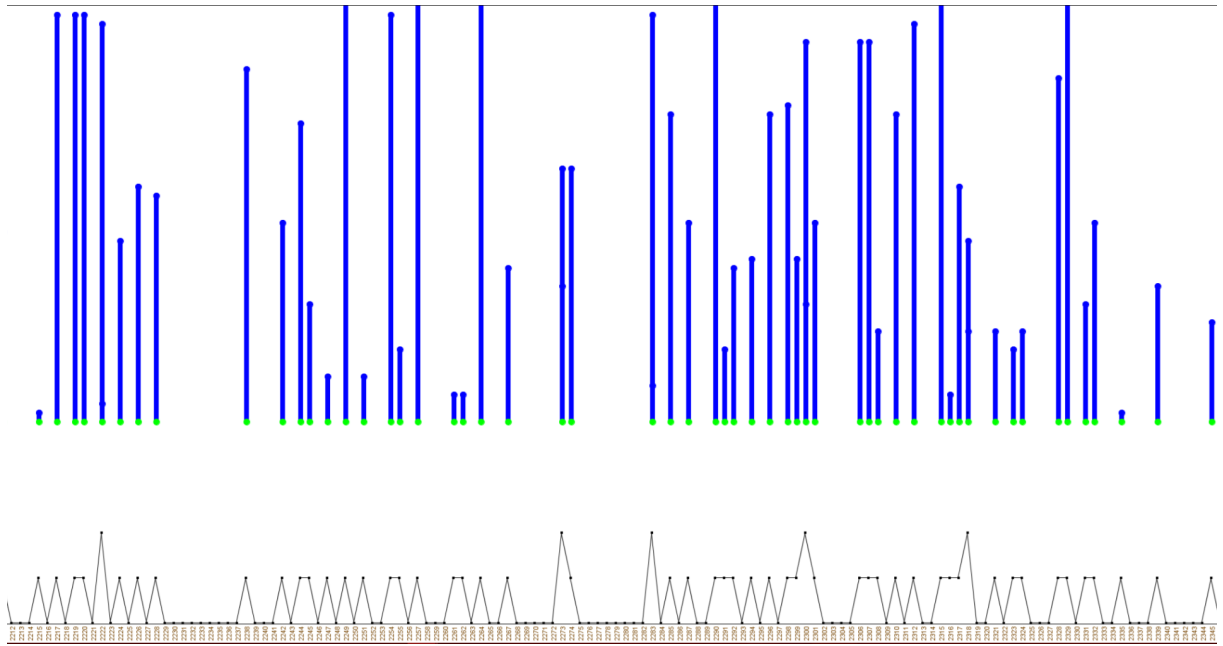


Figura 23 – Fragmento da visualização completa da simulação com 50 sensores, 64 Kbps e pacote de requisição 40 Bytes

3.2.5 Discussão

Os resultados encontrados podem ser analisados com base em dois pontos de vista, a visão do atacante e a da rede. Para os resultados obtidos em simulações com 1, 3 e 5 sensores, onde foram analisadas a quantidade absoluta de pacotes enviados pelos nós, a taxa de amplificação destes pacotes para cada injeção de tráfego e por fim a relação entre o tráfego enviado pelo atacante e o tráfego refletido, podemos constatar que a rede se manteve em bom desempenho por mais tempo com menos sensores.

Isto é observado pelas Figuras 10, 13 e 16 que mostram o comportamento dos sensores em relação à quantidade de pacotes enviados. Com 1 sensor, é possível observar que a diferença de pacotes enviados entre o atacante e os demais sensores aumenta a contar do cenário com 8 Kbps. Já para as simulações com 3 e 5 sensores, o mesmo efeito acontece em 4 e 3.2 Kbps, respectivamente.

Um outro detalhe importante é que nas métricas analisadas para os resultados com 1, 3 e 5 sensores, os cenários na qual a taxa de injeção do tráfego ultrapassou 16 Kbps expôs que os níveis de amplificação e reflexão daquele ponto em diante já se tornara estáveis e para o atacante continuar aumentando a taxa de injeção do tráfego não surtiria o efeito desejado, pois o processamento dos pacotes/dados requisitados já não seriam correspondidos. Podemos considerar este impacto na rede como um princípio de auto-ataque DDoS, pois a RSSF teve seus recursos drenados ao invés de mostrar elevação nos índices de amplificação/reflexão.

Os resultados obtidos com as simulações contendo 50 e 100 sensores mostraram

uma estagnação no processamento da rede diante da quantidade de informações que ela recebeu e deveria processar. Para o atacante, não se tornou vantajoso aumentar a quantidade de nós, em virtude da queda na quantidade de dados refletidos pelos sensores. Por exemplo, no cenário com a taxa de injeção do tráfego permeando 16 Kbps, o tráfego refletido caiu de 80.66 MB com 5 sensores para 44.21 MB com 50 sensores.

Utilizando a ferramenta *DyNetVis*, foi averiguado que a simulação com 100 sensores apresentou maiores quantidades de lacunas indicativas da falta de comunicação entre as pontas em comparação com as simulações com 50 sensores, mas nada que pudesse comprometer drasticamente os serviços apresentados pela rede.

O indício de um auto-ataque DDoS se torna muito mais evidente no cenário onde o pacote de requisição teve seu tamanho dobrado. A rede entrou em colapso e não conseguiu processar boa parte das requisições oriundas do atacante, fato que coloca uma ressalva na RFC 4919 publicada por [Kushalnagar, Montenegro e Schumacher \(2007\)](#), onde os autores mencionam não haver restrições para transferências de grande quantidade de dados utilizando sistemas que usam o protocolo 6LoWPAN.

4 Conclusão

O paradigma de Internet das Coisas mostra-se muito amplo e com inúmeras possibilidades para melhorar o cotidiano da população. Contudo, a grande quantidade de dispositivos conectados simultaneamente à Internet traz consigo preocupações plausíveis quanto à Segurança da Informação. Assim, o presente trabalho foi desenvolvido com o intuito de auxiliar na identificação da potencialidade de dispositivos ligados ao paradigma na efetivação de ataques DDoS.

Para tanto, o primeiro passo deste trabalho foi compreender e replicar o mesmo ambiente de simulações desenvolvido pelo [Pacheco et al. \(2016\)](#). Após esta etapa, foi necessário desenvolver novos experimentos alterando atributos como quantidade de sensores, tamanho/quantidade de pacotes enviados e a taxa de injeção do tráfego pelo atacante, a fim de analisar o comportamento da RSSF diante da simulação de um ataque DDoS.

Os resultados mostraram que existe um grande potencial em ambientes IoT serem maliciosamente capturados para a execução de ataques DDoS, mas o atacante deve buscar entender o ambiente IoT que será usado como *botnet*, isto é, saber qual a capacidade dos dispositivos, serviços, protocolos implementados, dentre outras características que poderão ajudar na efetivação do ato.

Em virtude da baixa capacidade de processamento, armazenamento e desempenho em RSSF, na visão do atacante, alguns pontos devem ser considerados na elaboração do ataque:

- **Quantidade de sensores:** a quantidade de sensores pode definir o quão eficaz será o ataque, dados os resultados obtidos, nem sempre maiores quantidades de sensores capturados numa mesma rede gerarão mais tráfego para a vítima;
- **Tamanho dos pacotes:** este atributo se mostrou um dos mais importantes a ser considerado durante a execução do ataque, pois, a rede simulada apresentou sinais de total ou quase total exaustão de recursos quando quantidades elevadas de dados foram requisitadas;
- **Taxa de injeção do tráfego:** representa em quanto tempo o atacante vai enviar determinada quantidade de dados e como averiguado nos resultados, não necessariamente um ataque cuja característica é aumentar tráfego malicioso subitamente para a vítima pode vir a indicar eficácia, visto que nos índices a partir de 8 Kbps, mais especificamente acima de 16 Kbps, a WSN se mostrou com os recursos bastante drenados e praticamente não houveram alterações nas taxas de amplificação tanto de dados quanto de pacotes;

- **Quantidade de *botnets*:** o atacante deve suprir a falta de recursos disponíveis em redes elaboradas em ambientes IoT angariando mais *botnets*, para que seja realizado ataques coordenados entre todos os dispositivos zumbis para uma mesma vítima.

O ataque DDoS desenvolvido neste trabalho teve o objetivo de exaurir os recursos computacionais da vítima. Para tanto, o Ataque de Negação de Serviço foi configurado à uma taxa contínua de solicitações com impacto degradante, ou seja, o intuito não foi inutilizar totalmente a vítima, mas reduzir suas capacidades de processamento paulatinamente. Em razão destas propriedades se mostrarem agravantes na complexidade de detecção do ofensor pela vítima, os administradores de rede devem estar atentos à lentidões inesperadas nos serviços implementados pelos dispositivos, perda de pacotes, frequência no envio/recebimento de pacotes e, se possível, buscar soluções para mitigar vulnerabilidades nos protocolos em execução.

Por fim, o resultado mais significativo foi obtido quando o pacote de requisição teve seu tamanho padrão dobrado para 40 bytes através do ambiente configurado com 50 sensores à uma taxa de injeção de dados de 64 Kbps. Para auxiliar na análise desta simulação, foi utilizado o *software DyNetVis* desenvolvido por [Linhares et al. \(2017\)](#). Neste ambiente, observou-se que a rede não conseguiu processar a alta quantidade de dados requisitada pelo atacante, ou seja, os recursos da RSSF entraram em colapso. Tal fato, coloca uma ressalva na RFC 4919, onde os autores [Kushalnagar, Montenegro e Schumacher \(2007\)](#) afirmam não haver restrições para transferências de grande quantidade de dados utilizando dispositivos LoWPAN.

A interpretação do termo "restrições" utilizado pelos autores possui dois aspectos que podem ser abordados, o primeiro deles (e neste caso, este trabalho apenas reforça este conceito) é que, de fato, os protocolos não impedem a transferência de grandes quantidades de dados; e o segundo aspecto pelo qual este trabalho coloca uma condicionante é usar o termo no sentido de permitir a transferências desses dados com eficácia.

Os resultados obtidos mostraram-se satisfatórios para realizarmos as conclusões deste trabalho, visto que alcançamos o objetivo proposto, com alguns atributos podendo ser alterados para melhor avaliar as simulações desenvolvidas, como é o caso, de reduzir o tamanho do pacote de requisição, alterar a dinâmica da taxa de ataque, fazendo com que esta seja variável ao invés de contínua e configurar o impacto para descontinuar totalmente a vítima ao invés de apenas degradar os recursos da mesma.

Como trabalhos futuros, propõe-se um estudo aprofundado sobre a influência da distância no desempenho dos elementos, posto que os sensores que permaneciam mais próximos ao atacante mantiveram o desempenho melhor que seus vizinhos e, por outro lado, os sensores que estiveram localizados distantes "fisicamente" do atacante tiveram seus rendimentos reduzidos. Um outro experimento seria utilizar várias redes de sensores

sem fio conectadas e coordenadas atacando apenas uma vítima.

Referências

- ABNT. Abnt Nbr Iso/Iec 17799. *Tecnologia da informação - Técnicas de segurança - código de prática para a gestão da segurança da informação*, p. 120, 2005. Citado na página 17.
- ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A survey. *Proceedings of the 1st International Conference on E-Business Intelligence (ICEBI2010)*, Elsevier B.V., v. 54, n. 15, p. 358–366, 2010. ISSN 1389-1286. Citado na página 16.
- BARKER, W. C. NIST - Special Publication. n. August, p. 21, 2003. Citado 2 vezes nas páginas 17 e 18.
- BARRETO, F. et al. CoAP-CTX: Extensão Sensível ao Contexto para Descoberta de Objetos Inteligentes em Internet das Coisas. *Proceedings of the XXXV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, n. May, 2017. Citado na página 22.
- CAO, C. et al. Hey, you, keep away from my device: remotely implanting a virus expeller to defeat Mirai on IoT devices. p. 1–15, 2017. Citado na página 14.
- CARL, G. et al. Denial-of-service attack-detection techniques. *IEEE Internet Computing*, v. 10, n. 1, p. 82–89, 2006. ISSN 10897801. Citado na página 18.
- DELICATO, F. Middleware Baseado em Serviços para Redes de Sensores Sem Fio. p. 196, 2005. Citado na página 21.
- Division CERT. 1998 CERT Advisories. p. 78, 2017. Disponível em: <<http://www.cert.org/advisories/CA-1998-01.html>>. Citado na página 20.
- FURFARO, A. et al. A Simulation Model for the Analysis of DDoS Amplification Attacks. *Proceedings - UKSim-AMSS 17th International Conference on Computer Modelling and Simulation, UKSim 2015*, p. 267–272, 2016. Citado 7 vezes nas páginas 7, 16, 19, 20, 27, 28 e 29.
- HENGST, K. DDoS through the Internet of Things. *25th twente student conference on IT*, 2016. Citado 4 vezes nas páginas 14, 16, 28 e 29.
- KAWANO, B. R. et al. Agricultura Inteligente No Contexto Da Computação Ubíqua: Estado Da Arte E Uma Proposta De Um Modelo Aplicado. *Proceedings of the 12th CONTECSI International Conference on Information Systems and Technology Management*, n. May 2016, 2015. Citado na página 17.
- KUROSE, J. F.; ROSS, K. W. *Redes de computadores e a Internet: uma abordagem top-down*. 6ª edição. ed. São Paulo: Pearson Education do Brasil, 2013, 2013. 634 p. ISBN 9788543014432. Citado 3 vezes nas páginas 22, 24 e 25.
- KUSHALNAGAR, N.; MONTENEGRO, G.; SCHUMACHER, C. *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*. [S.l.], 2007. v. 111, n. 2, 154–162 p. Disponível em: <<https://www.rfc-editor.org/info/rfc4919>>. Citado 3 vezes nas páginas 25, 44 e 46.

- LINHARES, C. D. G. et al. DyNetVis: A System for Visualization of Dynamic Networks. *Proceedings of the Symposium on Applied Computing*, p. 187–194, 2017. Citado 3 vezes nas páginas 39, 40 e 46.
- MIRKOVIC, J.; REIHER, P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, v. 34, n. 2, p. 39, 2004. ISSN 01464833. Citado 4 vezes nas páginas 18, 19, 20 e 21.
- ns-3 project. *NetAnim*. 2018. Disponível em: <<https://www.nsnam.org/wiki/NetAnim>>. Citado na página 26.
- ns-3 project. *ns-3 Network Simulator*. 2018. Disponível em: <<https://www.nsnam.org/>>. Citado na página 26.
- OLSSON, J. 6LoWPAN demystified. *Texas Instruments*, p. 13, 2014. Citado 2 vezes nas páginas 22 e 24.
- PACHECO, L. A. B. et al. Evaluation of Distributed Denial of Service Threat in the Internet of Things. p. 89–92, 2016. Citado 10 vezes nas páginas 7, 9, 14, 15, 22, 23, 27, 29, 33 e 45.
- PALATTELLA, M. R. et al. Standardized Protocol Stack For The Internet Of (Important) Things. *IEEE Commun. Surveys Tuts.*, v. 15, n. 3, p. 1389–1406, 2012. Citado na página 22.
- PERAKOVIĆ, D.; PERIŠA, M.; CVITIĆ, I. Analysis of the IoT impact on volume of DDoS attacks. *33rd Symposium on New Technologies in Postal and Telecommunication Traffic (PosTel 2015)*, n. December, p. 295–304, 2015. Citado 4 vezes nas páginas 7, 16, 28 e 29.
- POSTEL, J. *User Datagram Protocol*. [S.l.], 1980. v. 34, n. 2, 259–278 p. Disponível em: <<https://www.rfc-editor.org/info/rfc0768>>. Citado na página 24.
- RAYES, A.; SALAM, S. Internet of things-from hype to reality: The road to digitization. *Internet of Things From Hype to Reality: The Road to Digitization*, Springer International Publishing, Cham, v. 32, n. 8, p. 1–328, 2016. ISSN 0970034X. Citado 3 vezes nas páginas 14, 16 e 17.
- SHELBY, Z.; HARTKE, K.; BORMANN, C. *The Constrained Application Protocol (CoAP)*. [S.l.], 2014. 1–112 p. Disponível em: <<https://www.rfc-editor.org/info/rfc7252>>. Citado 3 vezes nas páginas 7, 23 e 24.
- STALLINGS, W. *Criptografia e segurança de redes: princípios e práticas*. [S.l.]: Pearson Education, Inc., 2015. 572 p. ISBN 9788543014500. Citado 2 vezes nas páginas 17 e 18.
- SUGANTHY, A.; MAITI, M. Information Security – Evolution , Impact and Design Factors. v. 100, n. 2, p. 14–19, 2014. Citado na página 17.
- The Wireshark team. *Wireshark*. 2018. Disponível em: <<https://www.wireshark.org/>>. Citado na página 27.
- THUBERT, P. *Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks*. [S.l.], 2011. 1–24 p. Disponível em: <<https://www.rfc-editor.org/info/rfc6282>>. Citado na página 26.

ZANELLA, A. et al. Internet of things for smart cities. *IEEE Internet of Things Journal*, v. 1, n. 1, p. 22–32, 2014. ISSN 23274662. Citado 2 vezes nas páginas [22](#) e [25](#).