Uma Proposta para Mitigação de IP *Spoofing* na Origem em Homenet Utilizando SDN

Manoel F. Ramos[1] **e Jéferson C. Nobre**[1]

[1]Escola Politécnica – Universidade Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos, 950 – Bairro Cristo Rei – 93.022-000 – São Leopoldo – RS – Brasil

manoel@dropreal.com, jcnobre@unisinos.br

Resumo. *A técnica de IP Spoofing é empregada em diversos tipos de ataques cibernéticos, tanto para amplificar ou redirecionar respostas de comunicação a um determinado alvo, quanto para alterar o real endereço de rede do atacante. Projeta-se que a utilização desta técnica seja intensificada com o surgimento de novas redes, como a do grupo de trabalho da IETF Home Networking (Homenet). Homenet utiliza o IPv6 e isto afirma que a mesma é vulnerável ao uso da técnica de IP Spoofing, isto porque o protocolo NDP – parte do IPv6 responsável pela descoberta de vizinhança – não possui mecanismos de validação dos endereços de rede e de enlace inseridos em seu cabeçalho. Este estudo apresenta um método simples para mitigar, identificar e impedir que o uso da técnica de IP Spoofing seja originado através de uma Homenet utilizando Redes Definidas por Software (Software-Defined Networking – SDN).*

Abstract. *IP Spoofing is used in various types of cyber attacks, either to amplify or redirect communications responses to a given target, how to change the actual address of the attacker network. It is projected that the use of this technique is intensified with the emergence of new networks, such as the working group of the IETF Home Networking (Homenet). Homenet uses IPv6, vulnerable to the use of IP Spoofing technique, that because the NDP protocol — part of IPv6 responsible for neighborhood discovery — does not have mechanisms of validation of address network and link embedded in its header. This study presents a simple method to mitigate, identify and prevent the use of IP Spoofing technique originated through a Homenet using Software-Defined Networking - SDN.*

1. Introdução

Home Networking (Homenet) [Haddad et al. 2015] utiliza o IPv6 como protocolo de endereçamento nativo. Isto destaca que a mesma é vulnerável ao uso da técnica de falsificação do endereços de origem contidos nos pacotes de rede (IP *Spoofing*), na qual é aplicada em diversos tipos de ataques cibernéticos.

Redes Definidas por Software (*Software-Defined Networking* – SDN) permitem como objetivo principal, dividir a função de encaminhamento da rede, realizado através do plano de dados, a partir da função de controle de rede, realizado pelo plano de gerenciamento. Isto permite uma gestão simplificada da rede. SDN tornou-se uma alternativa significante para elevar a segurança de redes de computadores, proporcionando a escalabilidade nos recursos dos equipamentos físicos, centralizando a tomada de decisão sobre o tráfego de rede através de seu controlador por meio de software [Hu 2014].

Este artigo apresenta um método simples para a mitigação do IP *Spoofing* em sua origem em uma Homenet utilizando SDN. A Seção 2 apresenta o referencial teórico, seguida da Seção 3 que descreve a solução proposta. A Seção 4 detalha a avaliação e os experimentos realizados, seguida dos trabalhos relacionados descritos na Seção 5. Por fim, a Seção 6 apresenta a conclusão sobre este estudo e os trabalhos futuros.

2. Referencial Teórico

Esta seção apresenta o referencial teórico sobre as principais tecnologias relacionadas a este estudo. Tais tecnologias são, o IP *Soofing*, Homenet e SDN.

2.1. IP *Spoofing*

A maioria dos ataques cibernéticos utilizam técnicas de falsificação (*Spoofing*) do endereço de origem contido nos cabeçalhos dos pacotes de rede, tanto para amplificar ou redirecionar respostas de comunicação a um determinado alvo, quanto para garantir o anonimato do atacante. Esta técnica é conhecida como IP *Spoofing* [Tanase 2003].

2.2. Homenet

Homenet é um grupo de trabalho da IETF que possui o objetivo de concentrar-se na evolução de redes residenciais, desenvolvendo e disponibilizando uma arquitetura simples e autoconfigurável para abordar os requisitos de configuração de prefixos IPv6 para roteadores, gestão de rede, resolução de nomes (*Domain Name System* - DNS) e serviços de descoberta de redes [Haddad et al. 2015].

Homenet utiliza o protocolo DNCP (*Distributed Node Consensus Protocol*) para receber informações de roteadores através de serviços de descoberta, de negociações e/ou de serviços de *autonomous bootstrapping*. DNCP troca pequenos conjuntos de TLV (*Type-Length-Value*) com o tamanho máximo de 64 Kb para cada nó participante da Homenet. Com isto, o DNCP descobre a topologia de cada nó da rede de forma bidirecional, permitindo que, quando há alguma mudança em um determinado nó, toda a informações é transmitida para os nós vizinhos através da troca de TLVs. Isto garante que toda informação recebida é válida e que todos os nós estão acessíveis. DNCP é um protocolo abstrato e para a sua implementação, deve ser combinado com um perfil DNCP específico e suas informações são divulgadas através de outro protocolo de comunicação para a divulgação das informações, como por exemplo, protocolos de autoconfiguração *Stateful* como o HNCP e o DHCPv6 [Haddad et al. 2015]. O HNCP inclui o perfil DNCP para o compartilhamento de informações entre o estado de roteadores e satisfaz as necessidades de funcionamento da arquitetura IPv6 da Homenet. Este compartilhamento é feito entre roteadores e *hosts* via TLVs, que permite a descoberta automática de *gateways* com base na topologia DNCP, assim como recebe e efetua a delegação de prefixos para os *hosts* e demais roteadores que possuem ou não suporte à HNCP.

Para a atribuição de prefixos IPv6, Homenet utiliza o *Distributed Prefix Assignment Algorithm* que faz uso do mecanismo de inundação (*flooding*), permitindo que nós anunciem seus prefixos aos *links* que estão diretamente conectados. Os prefixos já atribuídos não serão sobrepostos por outros ou seja, cada novo prefixo a ser atribuído, o endereço referente a este prefixo é acrescentado nas interfaces dos *hosts*. Além disto, o algoritmo cria um prefixo IPv6 /64 aleatoriamente e atribui os endereços para os *hosts*

com o intuito de garantir a comunicação, mesmo que o ISP esteja indisponível. Os dispositivos conectados à Homenet receberão os endereços atribuídos através do protocolo HNCP. Para dispositivos que não possuem suporte ao protocolo HNCP (*non*-HNCP), a atribuição é feita através de DHCPv6-PD ou por SLAAC [Haddad et al. 2015].

2.3. Redes Definidas por Software

SDN (*Software-Defined Networking*) está mudando a maneira de como as redes são concebidas e vem atraindo a atenção de diversos pesquisadores e empresas. SDN possui duas características definidas, a primeira é a separação do plano de controle do plano de dados. O plano de controle decide como lidar com o tráfego da rede, já o plano de dados encaminha o tráfego conforme decisão do plano de controle. A segunda característica é que SDN consolida o plano de controle de modo que o software exerça o controle direto sobre o estado dos elementos contidos no plano de dados como, por exemplo, *switches* e roteadores. Este software de controle, também denominado "controlador SDN" é uma interface de programação de aplicativos (*Application Programming Interface* - API) definida como, por exemplo, o protocolo OpenFlow [McKeown et al. 2008].

SDN integra todos os elementos físicos e virtuais, permitindo que o controlador gerencie a rede de forma automatizada e centralizada. Todo o tráfego é analisado pelo controlador no qual decide qual ação a ser tomada. O *switch*, quando recebe um determinado pacote de rede, analisará a sua tabela de fluxo e, caso desconheça a origem e o destino do mesmo, encaminhará as informações para o controlador no qual decidirá se o mesmo será descartado ou liberado [Kreutz et al. 2015].

3. Proposta para Mitigação de IP *Spoofing* na Origem em Homenet

A solução proposta é composta pelo uso de SDN que, além de permitir que se tenha uma visão global de todo o tráfego da rede através de uma análise de fluxos, permite que seja desenvolvida uma aplicação com base na API do controlador. Esta aplicação, denominada SPOOFING_SRC_CONTROL, é a responsável por analisar e tratar os endereços IPv6 de cada pacote que estão saindo da Homenet antes que o tráfego com o endereço de origem forjado seja liberado e que a tabela de fluxo do *switch* seja atualizada pelo controlador. Esta verificação é feita através da consulta sobre os endereços fornecidos pelo protocolo HNCP aos *hosts* internos da Homenet.

Esta seção descreve detalhadamente a solução proposta, contendo sua arquitetura, componentes e topologia de implementação em uma Homenet com suporte à SDN. A seguir são descritos os componentes e os algoritmos da solução proposta.

3.1. Arquitetura

Todo o processo é executado internamente no roteador Homenet e pode se estender por toda a topologia da rede residencial dependendo de sua extensão. A tecnologia SDN poderá estar localizada no próprio roteador de borda, no qual também pode fazer a função de *switch* para conectar fisicamente os *hosts* internos ou em *switches* localizados internamente na Homenet. O controlador SDN encontra-se configurado para acesso por este(s) *switch(es)* para efetuar o processo de gerenciamento do tráfego. Todo o tráfego de rede é analisado pelo controlador no qual decide se tráfego poderá ou não ser adicionado na tabela de fluxos do *switch*. A tomada de decisão é efetuada através da comparação dos

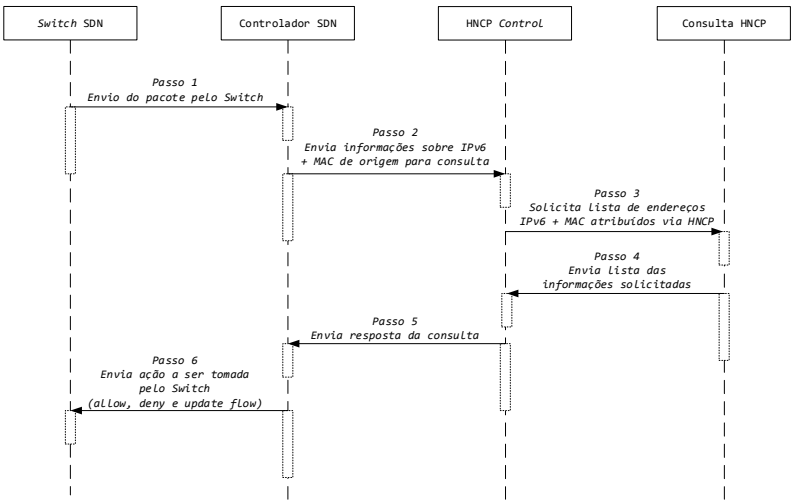

Figura 1. Diagrama de Troca de Mensagens da Solução.

endereços MAC e IPv6 inseridos na tabela de fluxo do *switch*. Caso os endereços de um respectivo pacote não estejam inseridos nesta tabela, ou o endereço IPv6 já esteja atribuído para outro endereço MAC (ou vice-versa), o *switch* encaminha o pacote para o controlador SDN que, consequentemente, decide qual a ação a ser tomada.

A Figura 1 apresenta o diagrama de troca de mensagens efetuado entre o *switch* SDN, o controlador e a base de armazenamento dos endereços IPv6 e MAC gerados pelo protocolo HNCP para os *hosts* internos da Homenet. O processo é iniciado quando o *switch* desconhece o endereço IPv6 de origem e de destino do pacote que chega para ser reencaminhado para um determinado destino. Este pacote é enviado para o controlador (passo 1) que, consequentemente, varificará se os endereços de destino e origem forem diferentes de algum endereço interno da Homenet. Com isto, o controlador efetuará uma consulta na base de dados que contém os endereços IPv6 e MAC dos respectivos *hosts* da Homenet gerados pelo protocolo HNCP (passo 2 e passo 5). Este procedimento é feito pelo submódulo da solução denominado MOD_IP-MAC_SEARCH() (Seção 3.2.2) no qual busca as informações sobre os endereços IPv6 e MAC atribuídos via HNCP (passo 3 e passo 4). Após isto, o controlador processa a verificação dos endereços enviando a ação necessária a ser tomada pelo *switch* sobre o respectivo pacote (passo 6). O *switch* atualiza a sua tabela de fluxo com a ação definida pelo controlador. Portanto, caso haja fragmentação de pacotes, os próximos fragmentos não serão analisados pela SPOOFING_SRC_CONTROL, pois o *switch* já compreendeu a ação a ser tomada.

3.2. Algoritmos de Verificação

SPOOFING_SRC_CONTROL é composto pelo módulo de controle, denominado MOD_CONTROL() e por seus submódulos MOD_VERIFY_IP-MAC() e MOD_IP-MAC_SEARCH(). Suas funções e algoritmos são descritos a seguir.

O módulo MOD_CONTROL() é o responsável pela tomada de decisão sobre a ação correta a ser tomada pelo pacote de rede analisado. Ele necessita dos seus submódulos MOD_VERIFY_IP-MAC() (Seção 3.2.1) e MOD_IP-MAC_SEARCH() (Seção 3.2.2) para o seu funcionamento. O Algoritmo 1 descreve que o MOD_CONTROL() primeiramente armazena as informações do endereço IP de origem

Algoritmo 1: MOD_CONTROL()

```
Entrada: IP_SRC, MAC_SRC, IP_DST, LOCAL_NETWORK_ADDRESS.
Saída: SDN_STATUS.
início
    se IP_DST == LOCAL_NETWORK_ADDRESS então
        se IP_SRC != LOCAL_NETWORK_ADDRESS então
            SDN_STATUS = ALLOWED
        fim
    fim
    senão
        SDN_STATUS = VERIFICATION
        ANL_IP_SRC = IP_SRC
        ANL_MAC_SRC = MAC_SRC
        MOD_VERIFY_IP-MAC()
        se SPOOFING_STATUS == NO então
            SDN_STATUS = ALLOWED
        fim
        senão se SPOOFING_STATUS == YES então
            SDN_STATUS = BLOCKED
        fim
        senão se SPOOFING_STATUS == FAIL então
            SDN_STATUS = BLOCKED
        fim
    fim
fim
```

do pacote na variável IP_SRC, o endereço MAC de origem na variável MAC_SRC e o endereço IP de destino do pacote na variável IP_DST. Além disto, o MOD_CONTROL() possui a variável LOCAL_NETWORK_ADDRESS, que possui o valor correspondente ao endereço IPv6 da rede local da Homenet. LOCAL_NETWORK_ADDRESS é extraído da base de dados dos endereços atribuídos pelo protocolo HNCP para a Homenet. A primeira ação do MOD_CONTROL() é analisar se o valor contido na variável IP_DST corresponde ao mesmo prefixo do valor da variável LOCAL_NETWORK_ADDRESS e se o endereço de origem (IP_SRC) é diferente da rede local. Este processo é feito para verificar se o destino do pacote é para a rede local ou para uma rede externa (internet), além de verificar se é um tráfego interno da Homenet. Caso o pacote esteja destinado para algum *host* interno da Homenet, o mesmo é liberado pelo sistema através da função SDN_STATUS e nenhuma verificação adicional será realizada, encerrando o módulo.

A função SDN_STATUS é a responsável por executar as ações do sistema internamente e perante o controlador SND, seus valores são **VERIFICATION** que possui a ação interna do sistema proposto para iniciar o processo de verificação do endereço IPv6 de origem analisado, **ALLOWED** que possui a ação a ser tomada pelo controlador SDN no qual liberará o fluxo no *switch* e **BLOCKED** que possui ação a ser tomada pelo controlador SDN no qual bloqueará o fluxo no *switch*.

O primeiro valor a ser gerado pela função SDN_STATUS é VERIFICATION,

no qual o sistema inicia o processo de verificação armazenando os valores de IP_SRC na variável ANL_IP_SRC e de MAC_SRC na variável ANL_MAC_SRC. Após isto, o submódulo MOD_VERIFY_IP-MAC() é executado alimentando o valor da variável SPOOFING_STATUS no MOD_CONTROL(). SPOOFING_STATUS possui três tipos de valores, sendo eles **FAIL** que é gerado quando o submódulo MOD_VERIFY_IP-MAC() não obteve resultados íntegros que comprovem a existência do IP *Spoofing*, **NO** que é gerado quando o submódulo MOD_VERIFY_IP-MAC() validou os endereços MAC e IPv6 e não identificou o uso da técnica de IP *Spoofing* no pacote e **YES** que é gerado quando o submódulo MOD_VERIFY_IP-MAC() validou os endereços MAC e IPv6 e identificou o uso da técnica de IP *Spoofing* no pacote.

Caso o valor de SPOOFING_STATUS for igual a FAIL, o sistema proposto não conseguiu analisar os endereços e comprovar a existência do uso da técnica de IP *Spoofing*. Este incidente poderá ocorrer em casos de indisponibilidade no processo de consulta ou até mesmo em um ataque na base de dados dos endereços atribuídos à Homenet. Neste caso, o sistema poderá inserir dois tipos de valores distintos na variável SDN_STATUS conforme a política de segurança estabelecida pelo administrador do ambiente Homenet no momento da configuração da solução, sendo eles ALLOWED para liberar o fluxo do pacote ou BLOCKED para bloquear o fluxo do pacote. Caso o valor de SPOOFING_STATUS for igual a NO, a variável SDN_STATUS recebe o valor ALLOWED, o que indica ao sistema que o pacote deve ser liberado através do controlador SDN pois conseguiu verificar os endereços e não identificou a existência do uso da técnica de IP *Spoofing*. Por fim, quando o valor de SPOOFING_STATUS for igual a YES, a variável SDN_STATUS recebe o valor BLOCKED, o que indica ao sistema que o controlador SDN deve descartar o pacote pois identificou o uso da técnica de IP *Spoofing*.

3.2.1. Submódulo MOD_VERIFY_IP-MAC()

O submódulo MOD_VERIFY_IP-MAC(), descrito no Algoritmo 2, trabalha em conjunto com o submódulo MOD_IP-MAC_SEARCH() (Seção 3.2.2) e gera resultados para a conclusão do módulo MOD_CONTROL(). MOD_VERIFY_IP-MAC() recebe os valores de ANL_IP_SRC e ANL_MAC_SRC gerados por MOD_CONTROL(). Sua primeira ação é iniciar o submódulo MOD_IP-MAC_SEARCH(). Após isto, é analisado o valor de DB_SERVER_STATUS gerado pelo submódulo MOD_IP-MAC_SEARCH().

DB_SERVER_STATUS poderá conter dois valores distintos, sendo eles **FAIL** quando o submódulo MOD_IP-MAC_SEARCH() não conseguiu executar o processo de localização dos endereços e **OK** quando o submódulo MOD_IP-MAC_SEARCH() executou com sucesso o processo de localização dos endereços. Caso o valor de DB_SERVER_STATUS for diferente de OK, SPOOFING_STATUS recebe o valor FAIL. Caso o valor de DB_SERVER_STATUS for igual a OK, o processo de verificação é iniciado. Primeiramente é verificado se o valor SEARCH_MAC recebido através da execução do submódulo MOD_IP-MAC_SEARCH() é igual a XX_XX_XX_XX_XX_XX. Em caso positivo, isto indica que o endereço MAC contido em ANL_MAC_SRC não encontra-se na base de dados da lista de endereços IP atribuídos. Com isto, SPOOFING_STATUS recebe o valor YES. Em caso negativo, a VERIFY_IP recebe o valor de SEARCH_IP extraída do submódulo MOD_IP-MAC_SEARCH(). Se o valor de VERIFY_IP for igual ao valor de

ANL_IP_SRC, os endereços de origens estão em conformidade e SPOOFING_STATUS recebe o valor NO. Por fim, caso o valor de VERIFY_IP for diferente de ANL_IP_SRC, o uso da técnica de IP *Spoofing* é identificado e SPOOFING_STATUS recebe o valor YES, finalizando a execução do submódulo, dando sequência no processo de análise.

Algoritmo 2: MOD_VERIFY_IP-MAC()

```
Entrada: ANL_IP_SRC, ANL_MAC_SRC.
Saída: SPOOFING_STATUS.
início
    MOD_IP-MAC_SEARCH()
    se DB_SERVER_STATUS != OK então
        SPOOFING_STATUS = FAIL
    fim
    senão
        se SEARCH_MAC == XX_XX_XX_XX_XX_XX então
            SPOOFING_STATUS = YES
        fim
        senão
            VERIFY_IP = SEARCH_IP
            se VERIFY_IP == ANL_IP_SRC então
                SPOOFING_STATUS = NO
            fim
            senão
                SPOOFING_STATUS = YES
            fim
        fim
    fim
fim
```

3.2.2. Submódulo MOD_IP-MAC_SEARCH()

O submódulo MOD_IP-MAC_SEARCH(), descrito no Algoritmo 3, possui a responsabilidade de localizar os valores de ANL_IP_SRC e ANL_MAC_SRC na base de dados da lista de endereços IPv6 atribuídos para a Homenet. Ele é iniciado através do submódulo MOD_VERIFY_IP-MAC() (Seção 3.2.1).

4. Avaliação

Nesta seção são apresentados os experimentos realizados para avaliar a solução proposta em uma Homenet. Primeiramente é detalhado a implementação do cenário de simulação contendo as tecnologias utilizadas, seguido dos experimentos realizados e seus resultados.

4.1. Cenário

O cenário e sua topologia foram implementados utilizando um ambiente virtual no qual possibilitou a execução da avaliação da solução proposta. Como ferramenta de simulação de redes de computadores foi utilizado o software GNS3, na versão nº. 1.3.9. Um ISP foi

implementado para simular um ambiente de internet no ambiente. Para a implementação dos roteadores da internet, foi utilizado o IOS c3640 da fabricante Cisco Systems.

Algoritmo 3: MOD_IP-MAC_SEARCH()

```
Entrada: DB_SERVER, ANL_IP_SRC, ANL_MAC_SRC.
Saída: SEARCH_MAC, SEARCH_IP, DB_SERVER_STATUS.
início
    Conexão com o DB_SERVER
    se DB_SERVER nao estiver acessivel então
        DB_SERVER_STATUS = FAIL
    fim
    senão se nao for possivel encontrar DB_SERVER então
        DB_SERVER_STATUS = FAIL
    fim
    senão
        DB_SERVER_STATUS = OK
        Localiza ANL_MAC_SRC em DB_SERVER
        se ANL_MAC_SRC nao for localizado então
            SEARCH_MAC = XX_XX_XX_XX_XX_XX
        fim
        senão
            SEARCH_MAC = ANL_MAC_SRC
            SEARCH_IP = IPv6 atribuído para o MAC localizado em
            DB_SERVER;
        fim
    fim
fim
```

A Figura 2 apresenta a topologia completa de implementação. Os roteadores A, B e C (ISP) se comunicam através do protocolo OSPFv3 e a distribuição automática de endereçamento IPv6 foi utilizado o serviço de DHCPv6-PD. O simulador GNS3 foi integrado ao software de virtualização VirtualBox, na versão nº. 4.3.30-r101610. Para a simulação dos *hosts* conectados aos roteadores clientes B e C, foi utilizado máquinas virtuais utilizando o sistema operacional GNU/Linux Debian 7. Cada um dos *hosts* (B-1 e C-1) possuem uma interface de rede conectada em seus respectivos *gateways* (roteadores clientes B e C) e recebem os endereços IPv6 automaticamente via SLAAC.

Homenet foi implementada no roteador Cliente A, onde foi utilizado o sistema operacional para *firmware* de roteadores OpenWRT, do modelo *Barrier Breaker*, na versão nº. 14.07-r42625. Para a conectividade de rede, foram configuradas duas interfaces *ethernet*, sendo *eth1* conectada diretamente no Roteador A do ISP, recebendo endereços automaticamente através de DHCPv6, e *eth0* conectada internamente para os *hosts* da Homenet. O *switch* com suporte a SDN e os *hosts* da Homenet foram implementados através da utilização do simulador SDN Mininet, na versão nº. 2.2.1. O sistema operacional utilizado foi o GNU/Linux Ubuntu, na versão nº. 14.04.3-LTS. No Mininet foram configurados um *switch* com suporte ao protocolo OpenFlow, na versão nº. 1.3, na qual possui suporte ao IPv6, um controlador SDN e três *hosts*. Para o controlador SDN, foi utilizado o software RYU, que também possui suporte ao protocolo OpenFlow 1.3 e,

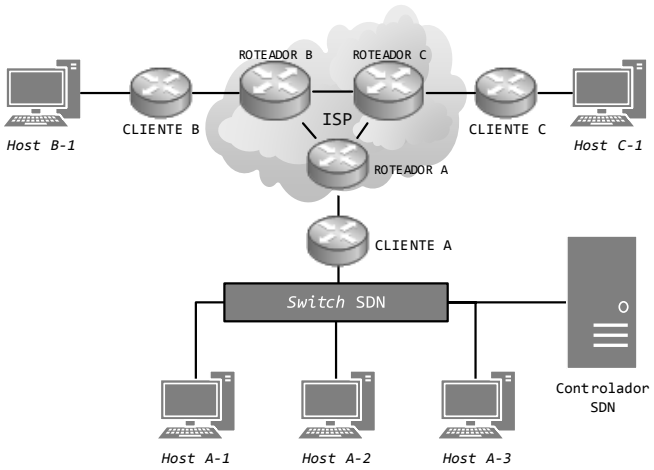

Figura 2. Cenário Completo de Simulação.

consequentemente, ao protocolo IPv6. O protocolo HNCP foi configurado no *host* hospedeiro da Mininet e todo o endereçamento, inclusive os dos *hosts* simulados no Mininet, foram atribuídos através do protocolo HNCP.

A base de dados dos endereços atribuídos pelo protocolo HNCP é alimentada através da captura do tráfego HNCP. Cada *host* da Homenet que se conecta à Homenet recebe os endereços IPv6 atribuídos para as suas respectivas interfaces de rede. Esta base de dados contém o endereço IPv6 e o endereço MAC das interfaces de cada *host* da Homenet. Para esta captura, foi desenvolvido o *script* denominado HNCP_CAPTURE, escrito em linguagem *Shell Script*. O *script* utiliza a ferramenta TCPDUMP aplicada com filtros específicos para capturar a troca de mensagens HNCP e armazenar os dados em um arquivo texto. Este arquivo texto é manipulado por SPOOFING_SRC_CONTROL no momento em que uma consulta é solicitada. Para que o submódulo do sistema MOD_IP-MAC_SEARCH() (Seção 3.2.2) execute a pesquisa solicitada, o sistema manipula o arquivo texto, validando o endereço IPv6 atribuído ao respectivo endereço MAC.

4.2. Desenvolvimento e Implementação da Solução Proposta

SPOOFING_SRC_CONTROL foi desenvolvido e implementando no controlador RYU. RYU foi desenvolvido na linguagem de programação Python, portanto, SPOOFING_SRC_CONTROL também foi desenvolvido em Python. O controlador RYU foi compilado para suportar a solução proposta. O sistema é iniciado pelo controlador quando o *switch* desconhece a origem e o destino (IPv6 e/ou MAC) do pacote que chega ao mesmo pois, em sua tabela de fluxo, não existem tais informações. Com isto, o *switch* envia o pacote para o controlador RYU que, antes de executar a função "*add_flow*", executa o SPOOFING_CONTROL através de sua função "*_packet_in_handler*".

SPOOFING_SRC_CONTROL efetua a verificação do endereço de origem da Homenet conforme o algoritmo do submódulo MOD_VERIFY_IP-MAC() (Seção 3.2.1). SPOOFING_SRC_CONTROL possui uma função, desenvolvida conforme o algoritmo do submódulo MOD_IP-MAC_SEARCH() (Seção 3.2.2), responsável por consultar os prefixos e os endereços IPv6 atribuídos para Homenet via HNCP. Com isto, a verificação do endereço de origem em cada pacote é realizada. Caso o endereço IPv6 de origem for

diferente da Homenet ou o endereço MAC de origem for diferente daquele contido na base de endereços atribuídos e o endereço de destino também for diferente da Homenet, o uso da técnica de IP *Spoofing* é identificado e o pacote é descartado pelo controlador.

4.3. Experimentos

Conforme ilustrado na Figura 2, a comunicação para a realização deste experimento foi efetuada entre os *hosts* da Homenet (*Hosts* A-1, A-2 e A-3) e os demais *hosts* externos, clientes do ISP (*Host* B-1 e *Host* C-1). O protocolo HNCP atribuiu dois prefixos IPv6 para a interface da Homenet em seu roteador e para os *hosts* internos (*Host* A-1, *Host* A-2 e *Host* A-3). Para a realização destes experimentos, o ambiente Homenet com suporte a *multihoming* não foi implementado.

Três experimentos do uso da técnica do IP *Spoofing* foram realizados no ambiente ilustrado na Figura 2. O experimento 1 valida a utilização do IP *Spoofing* na origem através da comunicação dos *hosts* da Homenet com os *hosts* externos (*Host* B-1 e *Host* C-1), comparando os endereços IPv6 e endereços MAC; O experimento 2 valida a comunicação na origem entre os *hosts* internos da Homenet (*Hosts* A-1, A-2 e A3), também comparando os endereços IPv6 e endereços MAC; E o experimento 3, valida a comunicação entre os *hosts* internos na Homenet com a comunicação externa porém, utilizando apenas a validação dos endereços de origem da Homenet através do prefixo IPv6 atribuído, não validando os endereços MAC dos *hosts* da Homenet.

Para a utilização do uso da técnica de IP *Spoofing* e MAC *Spoofing* em redes IPv6, foi utilizado o software NMAP (*Network Mapper*) na versão nº. 6.40. E para a validação, foi acrescentado a utilização do software Ping6, ferramenta de comunicação utilizada para medir quanto tempo em milissegundos (*ms*) um pacote de rede leva para ir até um determinado destino e retornar, utilizando o protocolo ICMPv6. O software Ping6 utilizado para a execução deste experimento foi disponibilizado através do conjunto de comandos de rede *inetutils-ping* na versão nº. 2:1.9.2-1. A utilização do software Ping6 se fez necessária para manter a comunicação entre os *hosts* e demonstrar a eficiência do sistema SPOOFING_SRC_CONTROL no momento em que uso da técnica do IP *Spoofing* pelo software NMAP foi identificada em cada *host*. Estes experimentos foram realizados 10 (dez) vezes com o objetivo de validar seus resultados, sendo que todas as sessões de repetição dos experimentos obtiveram os mesmos resultados.

4.3.1. Resultados

A Figura 3 apresenta os resultados de comunicação entre os *hosts* A-1, A-2 e A-3 com o *Host* B-1 (Figura 2 em uma Homenet (experimento 1) sem habilitar o sistema proposto. No período de tempo de 60 segundos, foi executado o NMAP, com os recursos de IP *Spoofing* e MAC *Spoofing* habilitados, e o Ping6 em todos os *hosts* da Homenet, sucessivamente, ao *host* B-1. Através deste experimento, foi constatado que Homenet é vulnerável ao uso das técnicas de de IP *Spoofing* e MAC *Spoofing*. O consumo do tráfego de rede foi medido através da captura dos resultados efetuada na interface de saída do roteador (*eth1*) da Homenet através do uso do software IFTOP, na versão nº.1.0pre2. NMAP totalizou o consumo médio de 5055 *bytes/s* (média de 1685 *bytes/s* por *host* da Homenet) e o Ping6 totalizou o consumo médio de 2412 *bytes/s* (média de 804 *bytes/s* por *host* da Homenet) do tráfego gerado através dos *hosts* internos da Homenet.

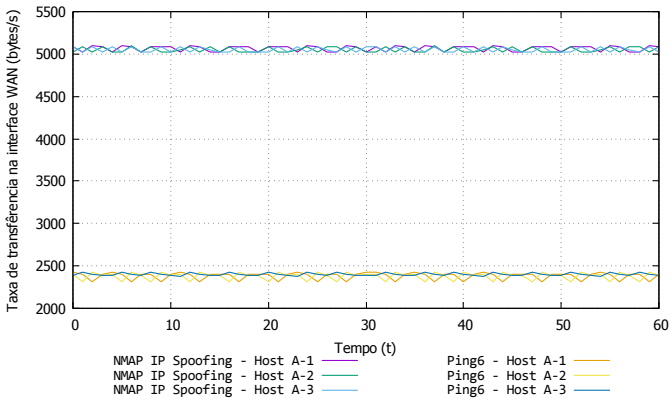

Figura 3. Aplicabilidade do IP *Spoofing* e MAC *Spoofing* sem a Solução Proposta.

A Figura 4 apresenta o resultado da mesma comunicação dos *hosts* A-1, A-2 e A-3 com o *host* B-1 em uma Homenet (experimento 1) porém, com o recurso SPOOFING_SRC_CONTROL habilitado no controlador SDN. Nos primeiros 20 segundos de execução, SPOOFING_SRC_CONTROL foi executado para validar o endereçamento do *host* A-1, onde a comunicação do mesmo foi encerrada no momento da detecção do IP *Spoofing*. Nos próximos 10 e 20 segundos (30 e 40), o mesmo processo foi executado no *host* A-2 e *host* A-3, encerrando a comunicação dos mesmos após a detecção do IP *Spoofing*. Este mesmo procedimento de testes foi executado para a validação de endereços MAC de origem, na qual obteve o mesmo resultado e comprovando que a solução também é eficiente para a combater o uso da técnica de MAC *Spoofing* na origem. No experimento 2, a solução proposta foi eficiente na mitigação e bloqueio do uso das técnicas de IP *Spoofing* e MAC *Spoofing* na origem. A captura dos resultados foram executados na interface *eth0* do Minenet através do software IFTOP. No experimento 3, somente o IP *Spoofing* foi detectado e bloqueado na comunicação com *hosts* externos da Homenet, isto porque neste experimento, não é possível fazer a comparação dos endereços MAC pois a base de consultas HNCP está relacionada apenas ao prefixo IPv6 atribuído para a Homenet. Isto também impactou no processo de verificação do IP *Spoonfig* gerado internamente na Homenet entre seus *hosts*.

4.3.2. Análises de Desempenho

As análises de desempenho foram realizadas para identificar o consumo do processamento e memória da solução no controlador SDN. Para isto, foi utilizado o software HTOP, na versão nº. 1.0.2, instalado diretamente no sistema operacional do controlador RYU.

A Figura 5 apresenta o resultado do consumo de processamento e de memória do controlador RYU sem a utilização da solução proposta. Dentro do período de 60 segundos, quando o controlador não manipulava a tabela de fluxo do *switch*, o mesmo apresentou uma variação entre 0.3% e 0.7% no consumo de processamento e 1.3% no consumo de memória. Nos segundos 11, 12, 13, 33, 34 e 35 o *switch*, que desconhecia as informações de origem e destino de dois pacotes de rede, encaminhou as mesmas para a verificação pelo controlador RYU, no qual validou os endereços de rede dos pacotes e adicionou as informações na tabela de fluxo do *switch*. Estas verificações geraram um

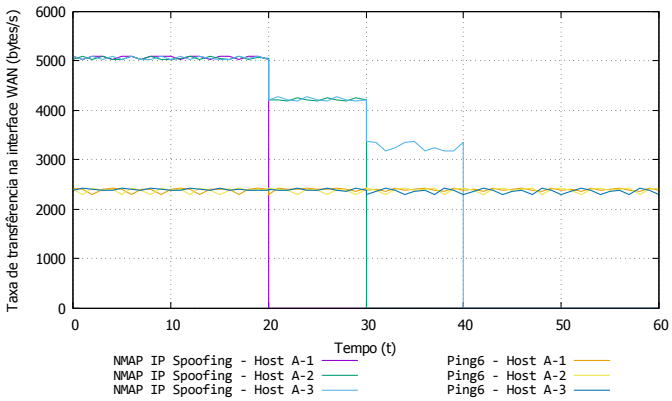

Figura 4. Aplicabilidade do IP *Spoofing* e MAC *Spoofing* com a solução proposta.

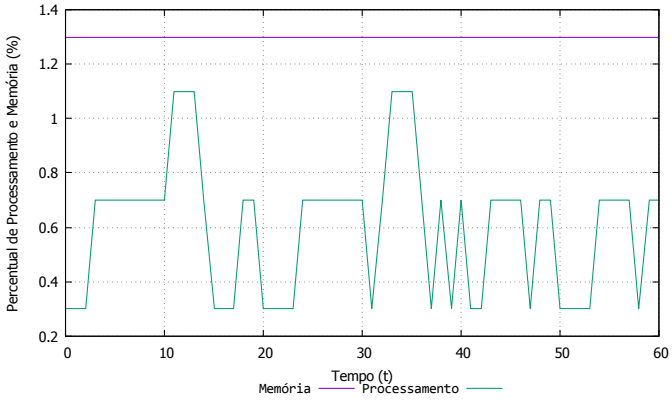

Figura 5. Uso dos Recursos Computacionais Sem o Uso da Solução Proposta.

pico de 1.1% no consumo de processamento cada. O consumo de memória RAM não foi alterado e os mesmos 1.3% de consumo não oscilaram durante toda a análise. Analisando os registros de eventos (*logs*) do controlador, foi constatado que o mesmo atualizou a tabela de fluxo do *switch* no período de tempo de 0,1 milissegundos.

A Figura 6 apresenta o resultado do consumo de processamento e de memória do controlador com o recurso da solução proposta habilitada. Dentro do período de 60 segundos, quando o controlador não manipulava a tabela de fluxo do *switch*, o mesmo apresentou uma variação entre 0.3% e 0.7% no consumo de processamento e 1.3% no consumo de memória. No segundo 17, o *switch* encaminhou as informações de endereçamento para o controlador qual não havia o uso da técnica de IP *Spoofing* e/ou MAC *Spoofing* para o controlador no qual, durante o processo de validação de endereços, obteve um pico de 1.1% no consumo de processamento (até o segundo 17) e nenhuma variação no consumo de memória ocorreu. Já nos segundos 35, 36 e 37, o *switch* encaminhou as informações de endereçamento de um pacote contendo o uso da técnica IP *Spoofing* e nos segundos 47, 48 e 49, as informações de endereçamento de outro pacote contendo o uso da técnica de MAC *Spoofing* ao controlador. Isto resultou, nos segundos 35, 36, 37, 47, 48 e 49, em um consumo de 1.2% de processamento e nenhuma variação no consumo da memória. Analisando os registros de eventos (*logs*) do controlador, também foi constatado que o mesmo atualizou a tabela de fluxo do *switch* no período de tempo de 0,1 milissegundos.

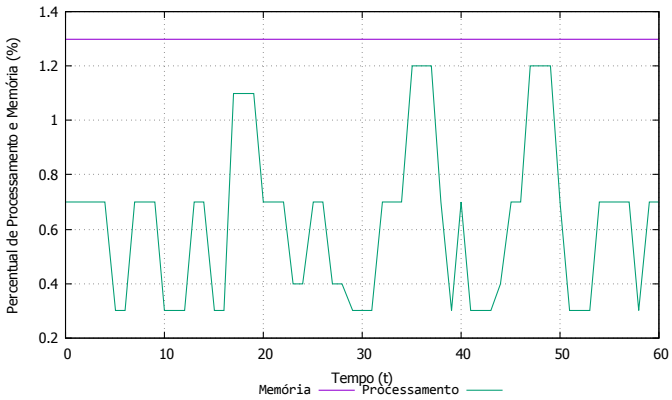

Figura 6. Uso dos Recursos Computacionais Com o Uso da Solução Proposta.

Os resultados comprovaram que a solução proposta consumiu o mesmo percentual do experimento ilustrado na Figura 5, quando o pacote não aplicava o uso da técnica de IP *Spoofing* e/ou MAC *Spoofing* e 0.1% a mais quando foi identificado. O tempo para o controlador atualizar a tabela de fluxo do *switch* também não foi impactado.

5. Trabalhos Relacionados

Existem diversos estudos relacionados a mitigação do IP *Spoofing* em redes IPv4. Por outro lado, poucos mecanismos de segurança são propostos para a prevenção em redes IPv6, em Homenet e principalmente tratam o problema diretamente em sua origem. Nesta seção são apresentados os trabalhos relacionados com o objetivo de fundamentar a mitigação do uso de técnicas de IP *Spoofing*. Este estudos foram selecionados por proporem soluções eficazes para o combate ao IP *Spoofing*, assim como métodos de filtragem de tráfego de rede utilizando SDN e de validação de endereçamento IP.

[Barbhuiya et al. 2013] apresentam um IDS ativo para a prevenção do IP *Spoofing* no processo de troca de mensagens do protocolo NDP. Os autores afirmam que a solução é eficaz para a validação de endereços MAC em redes IPv6. Os algoritmos desenvolvidos se destacam pela simplicidade no processo de identificação e comparação dos endereçamentos MAC e IPv6. [Yao et al. 2011] contribuem com o mecanismo denominado VAVE (*Virtual source Address Validation Edge*), desenvolvido através do *framework* do protocolo SAVI (*Source Address Validation Improvement*), o qual emprega o uso do protocolo Openflow para mitigar o IP *Spoofing* no tráfego de entrada em uma rede local. Um dos fatores negativos desta solução é que o protocolo SAVI necessita que sejam feitas adaptações nos protocolos atuais da internet, um fator negativo para que se torne um protocolo padrão perante à IETF. Já [Yan et al. 2011] desenvolveram um experimento de implementação do protocolo SAVI em uma rede local. Nesta contribuição, o fator positivo é que os autores consultam servidores DHCPv6 para efetuar o processo de validação através de mensagens NDP emitidas pelo SAVI. Por fim, [Mowla et al. 2015] propõem um mecanismo de defesa ao IP *Spoofing* no tráfego de dados recebidos, validando o tráfego legítimo e bloqueando o tráfego de *Spoofing*. A solução é composta por SDN com base na tecnologia CDNi (*Content Distribution Network Interconnection*), juntamente com a tecnologia ALTO (*Application Layer Traffic Optimization*). O objetivo é utilizar SDN para detectar IP *Spoofing*, seguindo de um mecanismo para alimentar re-

gras em *switches* SDN através do controlador utilizando os mapas de marcação (*mark*) fornecidos pelo servidor ALTO.

6. Conclusão e Trabalhos Futuros

IP *Spoofing* é um fator crítico perante as vulnerabilidades existente no protocolo IPv6. Este problema poderá se estender com as novas redes que estão surgindo, como por exemplo, à Homenet. No estudo realizado, foi proposto um mecanismo simples para a validação de endereçamento IPv6 na origem em uma Homenet. Os resultados obtidos demonstram a eficiência no processo de verificação dos endereços IPv6 de origem dos pacotes que estão saindo de uma Homenet, assim como o baixo consumo dos recursos computacionais utilizados pela solução no controlador SDN. Além disto, também foi constatado que a solução proposta pode ser eficiente para o combate ao uso da técnica de MAC *Spoofing*.

Para trabalhos futuros, o aprimoramento no processo de alimentação da base dos endereços de rede atribuídos para a Homenet deverá ser prioritário, estendendo-se na avaliação da solução proposta em um ambiente Homenet utilizando o recurso de *multihoming*, em um ISP com suporte à MSP e em redes convencionais IPv6.

Referências

Barbhuiya, F., Bansal, G., Kumar, N., Biswas, S., and Nandi, S. (2013). Detection of neighbor discovery protocol based attacks in IPv6 network. *Networking Science*, 2(4):91–113.

Haddad, W., Saucez, D., and Halpern, J. (2015). Multihoming in Homenet. Technical report, Internet Engineering Task Force. IETF draft, work in progress.

Hu, F., editor (2014). *Network Innovation through OpenFlow and SDN Principles and Design*. CRC Press, Boca Raton, FL.

Kreutz, D., Ramos, F., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., and Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76.

McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., and Turner, J. (2008). Openflow: Enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74.

Mowla, N., Doh, I., and Chae, K. (2015). An efficient defense mechanism for spoofed IP attack in SDN based CDNi. In *Proc. of the International Conference on Information Networking (ICOIN)*, pages 92–97.

Tanase, M. (2003). IP Spoofing: An Introduction. Disponível em: <http://www.symantec.com/connect/articles/ip-spoofing-introduction/>. Acesso em: abr. 2015.

Yan, Z., Deng, G., and Wu, J. (2011). Savi-based IPv6 source address validation implementation of the access network. In *Proc. of Computer Science and Service System (CSSS), 2011 International Conference on*, pages 2530–2533.

Yao, G., Bi, J., and Xiao, P. (2011). Source address validation solution with openflow/nox architecture. In *Proc. of Network Protocols (ICNP), 2011 19th IEEE International Conference on*, pages 7–12.