Artefato WTICG'23 Apêndice: Artigo #235027 Segurança em Internet das Coisas: Uma Análise de Comportamento de Rede sob Ataque

Alexandre M. Carrer[1], **Cíntia B. Margi**[1]

[1]Departamento de Sistemas Digitais e Computação
Escola Politécnica da Universidade de São Paulo (EPUSP) – São Paulo, SP – Brazil

{alexandrecarrer,cintia}@usp.br

Resumo. *Para viabilizar mecanismos de detecção e mitigação de ataques em Internet das coisas (IoT) é vital entender como diferentes ataques afetam o desempenho da rede. A literatura em geral contém análises de ataques da camada de rede. Neste trabalho implementamos ataques de camada de enlace (Blackhole e Greyhole) e de camada de transporte (Flooding) e analisamos o comportamento da rede observando a taxa de resposta do servidor e a indisponibilidade do protocolo de roteamento. As simulações foram realizadas com diferentes densidades de atacantes e diferentes distâncias do atacante ao servidor. Os resultados demonstram a capacidade de relacionar as métricas coletadas com o tipo de ataque e localização aproximada do nó atacante.*

1. Selos Considerados

Os autores julgam como considerados no processo de avaliação o Selo D - Artefatos Disponíveis; Selo F - Artefatos Funcionais; e o Selo R - Artefatos Reprodutíveis com as informações deste documento e do repositório do Github com os códigos necessários para a reprodução dos resultados no ambiente de simulação utilizado, o Cooja.

2. Informações básicas

Os códigos pode ser encontrado no Github do link: `https://github.com/AleMarquis/ArtigoWTICGSBSeg23`. Neste repositório são abordadas as questões de instalação e modificação do sistema operacional Contiki-NG para a implementação dos ataques (arquivos .c) e a simulação dos resultados por meio dos arquivos de configuração do Cooja (arquivos .csc)

O README do repositório apresenta informações de (i) Como instalar o Sistema Operacional Contiki-NG e o Emulador Cooja; (ii) Como modificar o Sistema Operacional para aplicar os ataques implementados; (iii) Como simular os ataques com base nos arquivos de configuração do Cooja (.csc)

2.1. Dependências

A dependência necessária a ser instaladas para a execução do artigo é o Sistema Operacional Contiki-NG.

O tutorial de instalação do Contiki-NG pode ser encontrado na documentação do sistema operacional. É recomendada a instalação via Imagem do Docker

para a replicação deste artigo. O passo-a-passo da instalação pode ser encontrado neste link: `https://docs.contiki-ng.org/en/develop/doc/getting-started/Docker.html`

3. Instalação

Com o Sistema Operacional instalado, o usuário deve realizar sua modificação para a implementação dos ataques abordados no artigo

Os ataques implementados no artigo são de duas categorias distintas, *Blackhole* e *Greyhole*, que são ataques implementados no *Framer* do sistema operacional, e *Flooding*, que é implementado na aplicação do dispositivo. Assim, em cada pasta dentro da raiz deste repositório contém os arquivos necessários para replicar os experimentos do artigo. Em todas as pastas com o nome dos ataques, temos os arquivos do *Framer* e a pasta intitulada *Attack*, que possui a aplicação e o código compilado dos nós, para sua implementação.

A instalação deve ser feita substituindo os códigos do *framer* do Contiki-NG e duplicando a pasta com os binários dos nós na pasta *example* do Sistema Operacional desta maneira:

Para cada implementação de ataque deve ser feito, a partir da pasta que leva o nome do ataque:

- Substituir framer-802154.c e framer-802154.h do Contiki no caminho: contiki-ng/os/net/mac/framer com os códigos disponibilizados na pasta framer deste repositório
- Inserir a pasta Attack na pasta de examples do Contiki no caminho: contiki-ng/examples

4. Teste mínimo

O Teste mínimo apresenta como executar as simulações com as variáveis pré-programadas para cada um dos ataques.

Com o Contiki-NG instalado e os ataques implementados, basta abrir o Cooja escrevendo o comando `cooja` no terminal. Se a instalação foi correta, a interface gráfica do Cooja, software usado para as simulações, será aberta. Para preparar os ambientes de simulação basta ir em File $\rightarrow$ Open Simulation e selecionar o arquivo .csc dentro da pasta contiki-ng/examples/Attack

Depois disso, basta iniciar a simulação clicando em Simulation $\rightarrow$ Start Simulation. Informações importantes como a troca de mensagens entre nós e atributos essenciais podem ser encontradas na aba Mote Output do Cooja em: View $\rightarrow$ Mote Output

5. Experimentos

Os experimentos realizados são replicáveis com os códigos disponibilizados no repositório do Github. Experimentos na rede simulada, como com alterações de número de nós atacantes, modificação do greyholeDropRatio podem ser realizadas modificando os códigos nas partes que acompanham comentários.

Os códigos que foram comentados e podem facilmente serem modificados são os alterados durante a pesquisa relatada no artigo. Dentro de cada aplicação de ataque, são eles:

- Attack
  - Makefile
  - udp-attack-client.c
  - udp-attack-server.c
- Framer
  - framer-802154.c
  - framer-802154.h

Caso deseje alterar algumas configurações da simulação, como analisar também a energia dos nós pelo Módulo Energest, ou mudar o ID dos nós atacantes, isto pode ser feito modificando os códigos originais. Estas modificações relevantes são acompanhadas de comentários explicativos. São exemplos de como realizar modificações nos experimentos:

- O módulo Energest pode ser inserido no Makefile dentro da pasta Attack;
- Mensagens do framer podem ser desativadas no Mote Output seguindo o comentário da linha 50 do arquivo framer-802154.c;
- O ID dos atacantes podem ser modificados alterando a variável attackerNode no framer-802154.c **E** no udp-attack-client.c