IDENTIFICAÇÃO DE HUBS FALSOS EM REDES DE INTERNET DAS COISAS

Lucas Augusto Mota de Alcantara[1]; Paulo André da Silva Gonçalves[2]

[1]Estudante do Curso de Engenharia da Computação - CIn – UFPE; E-mail: lama2@cin.ufpe.br,
[2]Docente/pesquisador do Centro de Informática – CIn – UFPE. E-mail: pasg@cin.ufpe.br.

Sumário: Este trabalho estuda e demonstra como melhorar a eficiência de identificação de hubs falsos na Internet das Coisas ou *Internet of Things* (IoT) quando uma técnica de análise de desvio de relógio é utilizada. São identificados fatores que influenciam essa eficiência e estudados seus impactos. Em particular, foram identificados e estudados fatores como a temperatura do hub IoT, a intensidade do tráfego na rede e a capacidade de processamento do dispositivo responsável por fazer as medições e análises. Os resultados mostram que há influência significativa da temperatura enquanto os outros fatores identificados possuem pouca ou nenhuma influência no contexto da plataforma de testes utilizada. Este trabalho contribui demonstrando a importância de diversos fatores no cálculo do desvio de relógio, permitindo o desenvolvimento de técnicas de cálculo de desvio de relógio mais eficientes.

Palavras–chave: Desvio de Relógio; Internet das Coisas; Hub IoT; Redes Sem Fio; Segurança;

INTRODUÇÃO

Com crescente uso de dispositivos móveis e a necessidade de troca de informações entre eles, as redes de acesso sem fio à Internet estão se tornando cada vez mais populares e necessárias no nosso cotidiano. Devido ao crescente número de usuários conectados a essas redes e os diferentes tipos de dados que ali trafegam, tanto os dispositivos dessas redes quanto seus usuários se tornam alvo de uma variedade de ataques.

Um dos métodos conhecidos de ataque a redes sem fio consiste na instalação de um ou mais pontos de acesso falsos no ambiente em que elas estão sendo utilizadas. Esses pontos de acesso são capazes de adotar as mesmas características de identificação do ponto original e, com isso, impedir a sua detecção [1]. Dessa forma, um usuário que deseja se conectar a rede pode fazer isso utilizando um ponto de acesso falso sem perceber e, a partir disso, ficar vulnerável à interceptação dos seus dados, por exemplo.

No contexto da Internet das Coisas os pontos de acesso são conhecidos como Hubs IoT e a falsificação deles também possui impacto significativo. A Internet das Coisas é uma nova e promissora abordagem de rede composta por objetos físicos inteligentes (sensores, atuadores, eletrodomésticos, dispositivos eletrônicos, veículos, produtos industrializados em geral) que podem, dependendo da aplicação, realizar comunicações autônomas, interagir entre si e trocar dados com a Internet. A falsificação de um hub pode permitir a um atacante fazer com que objetos como uma lâmpada em uma residência ou escritório se conecte a ele. Em seguida, o atacante pode explorar a lâmpada para obter informações sobre a presença de pessoas no ambiente atacado, por exemplo.

As técnicas tradicionais de identificação de pontos de acesso falsos que existem atualmente são voltadas para serem utilizadas por administradores de rede e requerem a instalação de infraestrutura cara e dedicada, como analisadores de pacotes e monitores de sinais. Em redes de Internet das Coisas, a presença de administradores de rede e instalação

de infraestrutura de alto custo em todos os ambientes é inviável. Desta forma, é essencial o desenvolvimento de técnicas que possam ser utilizadas diretamente nos dispositivos dos usuários a fim de que estes possam automaticamente aplicar regras ou políticas de proteção contra tentativas de ataque.

Por conta disso, este trabalho estuda uma técnica simples e não custosa que pode ser utilizada nos dispositivos dos próprios usuários ou em sistemas finais conectados ao hub IoT: análise de desvio de relógio. Essa técnica serve como forma de se identificar unicamente dispositivos [2] e se baseia no cálculo de variações no intervalo de tempo do envio de *beacons* pelos hubs IoT. O objetivo deste trabalho é contribuir não só demonstrando a importância de diversos fatores que impactam a eficiência no uso da técnica, mas também permitindo o desenvolvimento de técnicas mais eficientes.

MATERIAIS E MÉTODOS

Para a realização deste trabalho, foram desenvolvidas ferramentas de *software* responsáveis por analisar *beacons* capturados, registrar o intervalo de tempo entre a chegada deles, efetuar o cálculo do desvio de relógio utilizando a técnica de otimização matemática do Método dos Mínimos Quadrados e então gerar tabelas com os valores de desvios de relógios calculados resultantes. Para isso foi utilizado um *notebook*, onde foi preciso realizar uma modificação no *driver* (programa responsável por gerenciar um dispositivo) do seu adaptador de rede sem fio, a fim de se aumentar a resolução de informações de tempo obtidas. Além disso, foram utilizados dois pontos de acesso sem fio (roteadores domésticos) e outros dois *notebooks* para comporem a rede. Por fim, foi desenvolvido um dispositivo capaz de monitorar e registrar a temperatura dos roteadores utilizando a plataforma de prototipação Arduino.

O desenvolvimento das ferramentas de software foi feito utilizando um sistema operacional baseado em Linux, usando a linguagem de programação C para a implementação dos algoritmos de cálculo do desvio de relógio, assim como para a produção das tabelas de saída com os resultados obtidos. Para isso, foram utilizadas em conjunto as ferramentas LaTeX para diagramação de texto e TShark para captura dos pacotes e aquisição dos dados. Também foi utilizada a linguagem Shell Script para automação da execução dos processos de captura de pacotes, cálculo do desvio e geração da tabela de saída. A modificação do *driver* foi feita para alterar a unidade de registro do tempo de recebimento dos pacotes capturados de milissegundos para nanossegundos.

Além do *notebook* responsável pela captura dos pacotes, foram utilizados mais dois aparelhos com o intuito de sobrecarregar a rede e os pontos de acesso utilizados através da transmissão de dados de um para outro em uma taxa de transferência relativamente alta.

Para verificar a influência da temperatura foram executados testes em uma sala com temperatura controlada, na qual a refrigeração estava direcionada ao ponto de acesso com o intuito de minimizar a variação da sua temperatura. Os resultados obtidos nesses testes foram comparados com aqueles de testes realizados em ambiente sem controle de temperatura, onde a temperatura do ponto de acesso varia conforme o tempo de uso.

Na análise da interferência do poder de processamento do dispositivo que realiza a captura dos pacotes, foram comparados resultados de testes em que o *software* responsável por efetuar a captura foi executado com diferentes níveis de prioridade de processamento dedicado à sua execução.

Para avaliar o impacto gerado pela quantidade de pacotes sendo transmitidos no ambiente foi necessária a utilização de dois roteadores. Nesse caso, um deles foi o que teve seu desvio de relógio calculado enquanto o outro roteador foi usado para a criação de uma rede local que foi utilizada pelos outros dois notebooks disponíveis para a transmissão de dados de um para o outro. Então, foram realizados testes com transmissão de dados entre

dois aparelhos para comparar com o caso em que não há um tráfego de pacotes tão intenso na rede.

Por fim, para avaliar a influência da carga de trabalho sobre o roteador foi adotado um procedimento semelhante ao anterior. A diferença está no fato de que o desvio de relógio calculado foi o do ponto de acesso usado para a criação da rede local para a transferência de dados entre os dois *notebooks*.

Os testes foram efetuados em ambiente residencial e também nas dependências da universidade. Entretanto, os comparativos foram realizados somente entre resultados de testes realizados no mesmo ambiente.

RESULTADOS

A Tabela 1 apresenta as médias, acompanhadas do desvio padrão correspondente, obtidas a partir de 11 capturas de 1.000 *beacons*, com e sem aplicação de carga ao ponto de acesso, e também variando o nível de prioridade de processamento atribuído à execução do *softwar*e de captura.

Tabela 1: AP2 – Prioridade vs Carga

	0 Mbps	10 Mbps
Padrão	34,896418 +/- 0,139890	34,834989 +/- 0,047579
Máxima	34,731987 +/- 0,048251	34,864243 +/- 0,053742

As Tabelas 2 e 3 apresentam médias de capturas realizadas em diferentes temperaturas do ponto de acesso, assim como uma média geral desses valores, acompanhada do seu desvio padrão.

Tabela 2: AP2 –Temperatura variável – Prioridade Padrão

29ºC	30ºC	31ºC	32ºC	Média
33,12038	32,94637	32,426101	30,415340	32,590363 +/- 0.851072

Tabela 3: AP2 –Temperatura variável – Prioridade Máxima

32ºC	33ºC	34ºC	35ºC	Média
29,272869	29,14085	29,11694	29,0234	29,101450 +/- 0,081840

A Tabela 4 contém o resultado de capturas em diferentes níveis de tráfego no ambiente e também diferentes níveis de prioridade de processamento.

Tabela 4: AP1 – Prioridade vs Tráfego

	0 Mbps	10 Mbps
Padrão	13,790217 +/- 0,106805	13,728206 +/- 0,034398
Máxima	13,773046 +/- 0,027381	13,808053 +/- 0,038036

DISCUSSÃO

A partir da Tabela 1 é possível verificar que o impacto gerado pela diferença do nível de prioridade de processamento é praticamente inexistente. Sem aplicação de carga, a diferença foi de 0,16, o que representa apenas 0,48% de variação. Com uma carga de 10 Mbps, houve uma variação de 0,03 no resultado com os diferentes níveis de prioridade, correspondendo a 0,09% de diferença, sendo ainda menor do que no caso anterior.

Avaliando a diferença produzida pela mudança na carga aplicada com prioridade padrão, houve uma variação de 0,06, o que representa 0,17%. Com prioridade máxima, a

diferença foi de 0,13, que corresponde a 0,38% de variação. Ambas as diferenças podem ser consideradas insignificantes.

Na Tabela 2, a primeira média obtida foi de 33,12, com uma temperatura de 29ºC, enquanto a última foi de 30,41 em 32ºC. Essa variação de 2,71 representa 8.2% de diferença. Na Tabela 3 observa-se que a mesma variação de 3 graus na temperatura produziu uma variação menor, de apenas 0,25, que corresponde a 0,86%. Isso evidencia uma característica não linear da variação do desvio em função da temperatura.

Analisando a tabela 4 verifica-se a influência produzida pelo tráfego de pacotes no ambiente. Com prioridade padrão, a variação no tráfego causou uma diferença de 0,07, correspondente a 0,53%. Com prioridade máxima a variação foi de 0,03, representando 0,23%. Isso indica que o tráfego não interfere de forma significativa no desvio obtido.

CONCLUSÕES

A partir dos resultados conseguidos neste trabalho, foi possível identificar quais variáveis apresentam mais influência sobre o valor calculado para o desvio de relógio de um ponto de acesso sem fio. Dentre as variáveis analisadas destacou-se a temperatura, onde uma variação de 6ºC chegou a gerar uma diferença de 12,41% entre os valores de desvio calculados.

Os outros fatores analisados foram o nível de prioridade de processamento para o software responsável pela captura dos pacotes necessários para o cálculo do desvio, a quantidade de tráfego de pacotes no ambiente e também o nível de carga sendo aplicada ao ponto de acesso monitorado no momento da medição. Porém, ao contrário da temperatura, estas variáveis não causaram alteração significativa nos valores obtidos para o desvio de relógio, tendo sido observadas variações máximas de 0,53%. Com isso, é possível afirmar que essas variáveis não interferem de forma significativa no valor obtido para o desvio de relógio de um ponto de acesso.

Com as informações deste trabalho, um administrador de rede que deseje utilizar a técnica do desvio de relógio como forma de identificação de pontos de acesso falsos instalados na sua rede deve levar em conta que os valores do desvio obtido para os roteadores originais da sua rede podem variar em função da sua temperatura, evitando assim a ocorrência de falsos-positivos. Dessa forma, a aplicação da técnica do cálculo do desvio de relógio se torna mais eficiente.

AGRADECIMENTOS

Gostaria de agradecer à minha família, que me possibilitou conquistar diversos objetivos até o momento, incluindo a participação neste projeto. Agradeço também ao meu orientador Paulo Gonçalves, que deu todo o auxílio necessário para que o trabalho fosse realizado da melhor forma possível.

REFERÊNCIAS

[1] Kurose, James F; Ross, Keith W., Redes de computadores e a Internet: uma abordagem top-down, 5. ed., São Paulo : Addison Wesley, 2010.

[2] Jana, S.; Kasera, S.K., On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews, Mobile Computing, IEEE Transactions on, vol.9, no.3, pp.449,462, March 2010.