Localização de Dispositivos Maliciosos usando Veículos Aéreos não Tripulados

Evilasio C. Junior[1], **Rafael Gomes**[2], **Leonardo S. Rocha**[2], **Rossana M. C. Andrade**[1]

[1] Universidade Federal do Ceará (UFC)
Fortaleza – CE – Brazil

[2]Universidade Estadual do Ceará (UECE)
Fortaleza – CE – Brazil

evilasiojunior@great.ufc.br, rafaellgom@larces.uece.br

leonardo.sampaio@uece.br, rossana@ufc.br

Abstract. *Internet access in public environments allows users to access their data online from anywhere. However, these environments can facilitate the action of malicious agents interested in promoting attacks to the network, and, because they are public places, making it challenging to locate these attackers. Nowadays, it is possible to detect an attack and, with that, a set of information about the device used in this action can be identified, which allows the access to be blocked. This information is not enough to determine the physical location of the attacker, which is essential to prevent future attacks, but it can assist in this task. Therefore, this work proposes a technique for the approximate location of a malicious device in a network, using trilateration to locate the target, with the aid of an unmanned aerial vehicle. The results indicate that the solution is capable of finding malicious devices.*

Resumo. *O acesso a internet em ambientes públicos permite que os usuários acessem seus dados online de qualquer lugar. Entretanto, esses ambientes podem facilitar a ação de agentes maliciosos interessados em promover ataques a rede e, por serem locais públicos, isso dificulta a localização desses atacantes. Hoje em dia é possível detectar um ataque e, com isso, um conjunto de informações sobre o dispositivo usado nesta ação pode ser identificado, o que permite que o acesso seja bloqueado. Essas informações não são suficientes para determinar a localização física do atacante, o que é essencial para impedi-lo de realizar ataques futuros, mas podem auxiliar nessa tarefa. Sendo assim, este trabalho propõe uma técnica de localização aproximada de um dispositivo malicioso em uma rede, utilizando trilateração para localizar o alvo, com o auxílio de um veículo aéreo não tripulado. Os resultados indicam que a solução proposta é capaz de encontrar o dispositivo malicioso.*

1. Introdução

Com a facilidade de acesso a Internet através de redes sem fio públicas, as pessoas têm acesso a seus dados *online* de qualquer lugar. Esse tipo de infra-estrutura permite a disponibilização de serviços e o desenvolvimento de cidades inteligentes

[Chamoso et al. 2018]. Contudo, esses ambientes públicos são mais propícios a problemas de segurança, que podem dificultar a localização de dispositivos usados para realizar ataques as suas redes [Watts 2016][Cirqueira et al. 2011].

Com o avanço dos estudos na área de segurança de redes, é possível identificar diversos tipos de tráfegos incomuns dentro de uma rede. Esses sistemas de identificação de intrusão (do inglês, *Intrusion Detection System* - IDS) são capazes de identificar informações, como endereço de MAC e a força do sinal entre o ponto de acesso e o dispositivo malicioso [Alotaibi and Elleithy 2016]. Essas informações podem ser usadas para bloquear o acesso da máquina atacante à rede, porém não são suficientes para identificar a localização destes dispositivos, o que é importante para evitar novos ataques. Entretanto, essas informações podem ser usadas como parte de uma estratégia para localizar esses dispositivos.

Uma forma de localizar fisicamente os dispositivos em ambientes públicos é utilizando veículos aéreos não tripulados (VANT), como drones. Segundo Mozaffari et al. (2019), esses veículos são vantajosos quando usados em soluções para ambientes de redes sem fio públicas, devido as suas características, como mobilidade, flexibilidade de trajeto e altitude adaptativa. Adicionalmente, os drones podem localizar alvos utilizando apenas sinais digitais [Halder and Ghosal 2016].

Nesse contexto, este trabalho propõe uma técnica para localização aproximada de um dispositivo imóvel usado para atacar uma rede, utilizando um drone e as informações obtidas por um IDS. Com a informação da assinatura da máquina do atacante e a força do sinal da rede, a técnica busca encontrar a distância do drone ao alvo e do alvo ao ponto de acesso usado pelo dispositivo atacante. Essas medições, juntamente com a localização do ponto de acesso e do drone, são utilizadas no cálculo da trilateração para determinar a localização aproximada da máquina atacante. Para validar a solução foram executadas simulações usando o Network Simulator 3 (NS-3) [Riley and Henderson 2010]. Os resultados indicam que a solução proposta encontrou a posição aproximada do alvo com tempo aproximado de dez segundos em quatro situações avaliadas.

O restante do artigo está organizado da seguinte forma: na Seção 2, é apresentada a fundamentação teórica sobre IDSs e trilateração. A solução de localização do atacante proposta é detalhada na seção 3, enquanto que a Seção 4 descreve os experimentos realizados. Na Seção 5, os trabalhos relacionados são discutidos e, por fim, na Seção 6 apresentamos as conclusões e trabalhos futuros.

2. Fundamentação Teórica

2.1. Sistemas de detecção de intrusão

Os sistemas de detecção de intrusão são capazes de monitorar passivamente ou ativamente atividades intrusivas em uma máquina específica e em um perímetro de rede [Tidjon et al. 2019]. Um IDS pode investigar atividades do sistema e do usuário, reconhecer padrões de ataques conhecidos e identificar atividades anormais da rede.

Brutch et al. (2003), classificou IDSs em três categorias com base nas técnicas usadas para detectar eventos de intrusão: aqueles baseados em assinatura, em anomalias ou em especificação.

IDSs que utilizam detecção baseada em assinatura, são capazes de verificar a ocorrência de assinaturas ou sequências predefinidas que indicam uma invasão. IDSs que usam a detecção baseada em anomalias, definem perfis de comportamento normal e classificam qualquer acesso ou tráfego diferente desse perfil, como uma intrusão. O perfil normal é atualizado à medida que o sistema aprende novos comportamentos. IDSs que operam com a técnica de detecção baseada em especificação, definem um conjunto de restrições que descrevem a operação correta de um programa e monitoram essa execução com relação às restrições definidas.

Em nossa proposta, utilizamos um sistema de detecção de intrusão por assinatura, pois são IDSs mais simples de implementar e simular. Entretanto, no futuro poderemos estudar as vantagens de usar outros tipos de IDS.

2.2. Trilateração

A trilateração é um cálculo que usa medições de distâncias para determinar uma posição no espaço tridimensional [Murphy and Hereman 1995]. Esse cálculo facilita sistemas de posicionamento em tempo real a encontrar alvos sem a necessidade da medição de ângulos. De uma forma simplificada, para calcular as coordenadas de um alvo fixo podemos utilizar um sistema simples de três equações, como definido na Equação 1 [Courtay et al. 2019].

$$\begin{cases} d_{N1}^2 = (x_A - x_{N1})^2 + (y_A - y_{N1})^2 + (z_A - z_{N1})^2 + e_{N1} \\ d_{N2}^2 = (x_A - x_{N2})^2 + (y_A - y_{N2})^2 + (z_A - z_{M2})^2 + e_{N2} \\ d_{N3}^2 = (x_A - x_{N3})^2 + (y_A - y_{N3})^2 + (z_A - z_{M3})^2 + e_{N3} \end{cases} \quad (1)$$

Na Equação 1, d_{Ni} representa a distância entre o nó i, cuja a posição é conhecida (por exemplo, um drone), e o alvo. X_{Ni}, Y_{Ni} e Z_{Ni} são as coordenadas X, Y e Z dos nós cuja localização já são conhecidas. X_A, Y_A e Z_A são as coordenadas do alvo. E e_{Ni} é o erro decorrente do ruído do sinal usado para calcular as distâncias do nó i ao alvo.

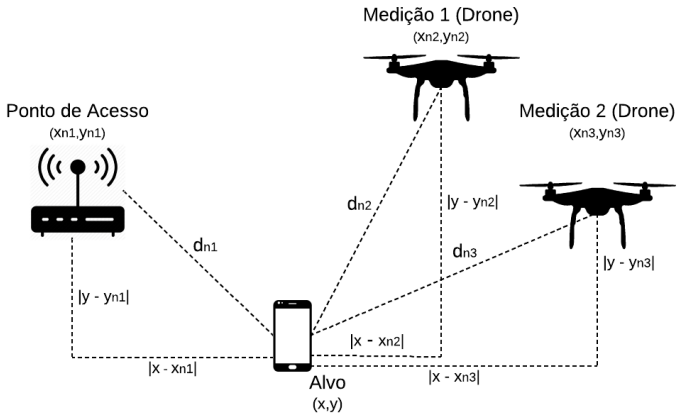

Figura 1. Exemplo de trilateração com drones

A Figura 1 apresenta uma exemplo de trilateração no contexto desse trabalho, na qual são usados duas medições de drones e um ponto de acesso. Note que no exemplo não é considerado o eixo z. Assim, para simplificação do cálculo, assumimos que o atacante

e o ponto de acesso estão na mesma altura de referência, logo os valores deles para o eixo z são zero e, para o drone, esse valor é igual a altura do drone no momento da medição.

O cálculo da trilateração busca resolver o sistema representado na Equação 1 de modo a determinar as coordenadas do alvo [Courtay et al. 2019]. Uma maneira de fazer isso é transformar a Equação 1 na Equação vetorial $u = V.a + e$, que pode ser alcançada, a partir do desenvolvimento dos termos do sistema de equações e subsequente subtração das distâncias na Equação 1, onde:

$$u = \begin{pmatrix} (d_{N1}^2 - d_{N2}^2) - (x_{N1}^2 - x_{N2}^2) - (y_{N1}^2 - y_{N2}^2) - (z_{N1}^2 - z_{N2}^2) \\ (d_{N1}^2 - d_{N3}^2) - (x_{N1}^2 - x_{N3}^2) - (y_{N1}^2 - y_{N3}^2) - (z_{N1}^2 - z_{N3}^2) \\ (d_{N2}^2 - d_{N3}^2) - (x_{N2}^2 - x_{N3}^2) - (y_{N2}^2 - y_{N3}^2) - (z_{N2}^2 - z_{N3}^2) \end{pmatrix} \tag{2}$$

$$V = 2 * \begin{pmatrix} (x_{N2} - x_{N1})\ (y_{N2} - y_{N1})\ (z_{N2} - z_{N1}) \\ (x_{N3} - x_{N1})\ (y_{N3} - y_{N1})\ (z_{N3} - z_{N1}) \\ (x_{N3} - x_{N2})\ (y_{N3} - y_{N2})\ (z_{N3} - z_{N2}) \end{pmatrix} \tag{3}$$

$$e = \begin{pmatrix} e_{N1} - e_{N2} \\ e_{N1} - e_{N3} \\ e_{N2} - e_{N3} \end{pmatrix} \tag{4}$$

$$a = \begin{pmatrix} x_A \\ y_A \\ z_A \end{pmatrix} \tag{5}$$

Dada essa transformação, podemos determinar os valores de x_A, y_A e z_A usando alguns artifícios matemáticos. Em nossa proposta, utilizamos a regra de Cramer [Courtay et al. 2019], devido a simplicidade de implementação e o rápido tempo de resposta (na casa de milissegundos), o que é importante para o nosso contexto de ambientes públicos. Desse modo, calculamos o valor de x_A, solucionando as equações 6 e 7.

$$v1 = \begin{pmatrix} 2 * (x_{N2} - x_{N1}) \\ 2 * (x_{N3} - x_{N1}) \\ 2 * (x_{N3} - x_{N2}) \end{pmatrix} \tag{6}$$

$$x_A = \frac{det((u - e).v1)}{det(V)} \tag{7}$$

De maneira análoga, podemos usar a regra de Cramer para calcular os valores de y_A e z_A e, com isso, encontrar a localização do alvo.

3. Técnica de Localização do Atacante

Este artigo apresenta uma técnica para localizar dispositivos maliciosos usados no ataque de redes sem fio em ambientes públicos. Essa técnica utiliza um IDS para detectar o dispositivo e o endereço MAC do mesmo. Essas informações são usadas pelo servidor em conjunto com um drone para encontrar o dispositivo. Em nossa proposta, utilizamos um IDS baseado em assinatura, devido sua maior simplicidade, porém, acreditamos que qualquer IDS que permita guardar informações da assinatura da máquina atacante poderia ser utilizado. A seguir detalhamos o passo a passo da técnica.

Ao detectar um ataque, o IDS no servidor restringe o acesso do atacante, e o drone é acionado. Então, o IDS envia para o drone e para o ponto de acesso ao qual o

dispositivo malicioso está conectado, o endereço MAC do atacante. O servidor também calcula a trajetória que o drone deve seguir. Além disso, o servidor mantém uma tupla T com três posições, para armazenar as informações advindas do ponto de acesso e do drone.

Quando recebe o endereço de MAC do atacante, o ponto de acesso envia ao servidor a força do sinal entre ele e a máquina atacante, além da localização do ponto de acesso. Já o drone, enquanto segue sua trajetória, usa a estratégia de *broadcast* do sinal wi-fi e o endereço MAC fornecido pelo servidor. Quando o drone encontra a máquina atacante, ele envia para o servidor a informação da localização do drone e a força de sinal entre ele e o alvo. Enquanto não for determinada a localização da máquina atacante, o drone continua buscando a máquina alvo e enviando as informações ao servidor. Finalmente, quando todas as posições da tupla são preenchidas, é utilizado o algoritmo de localização para calcular a posição do atacante.

A trajetória do drone segue a estratégia *SCAN* [Koutsonikolas et al. 2007], na qual a área onde o drone irá trafegar é dividida em um quadrado e em sub-quadrados equidistantes com centros conectados usando linhas retas. Nós utilizamos essa estratégia, pois a cobertura uniforme do campo de rede ajuda a garantir um erro pequeno de localização [Koutsonikolas et al. 2007].

Vale destacar que não faz parte do escopo dessa proposta a análise do custo energético do drone. Além disso, pressupomos que não haja obstáculos aéreos e que temos como determinar continuamente a localização do drone.

3.1. Cálculo da distância

Para calcular a localização do atacante com base na trilateração, é necessário três medições advindas de fontes diferentes. Em cada medição são obtidas as coordenadas da localização da fonte (ponto de acesso ou drone) e é calculada a distância da fonte ao atacante usando a força do sinal entre a fonte e o alvo, que é gerada com base na atenuação da energia do sinal de rádio entre os dois dispositivos. Esse cálculo está diretamente relacionado ao modelo de propagação do sinal [Abhayawardhana et al. 2005], que tem que ser adequado a configuração do ambiente.

Nesse trabalho utilizamos o modelo de Log Distância, que modela a propagação de redes sem fio em ambientes *indoor* e *outdoor* com e sem obstáculos [Al-Hourani and Gomez 2017]. A força do sinal para o modelo de Log Distância é calculada seguindo a Equação 8. Nessa Equação, P e P_0 representam a força do sinal (em dBm) para a distância d e d_0. O valor α é o coeficiente de atenuação, que é uma constante e depende do meio e da frequência utilizada na rede. Por último, n é o erro de medição da força do sinal. Esse erro de medição impacta no ruído do sinal da fórmula da trilateração. Desse modo, para calcular a distância, transformamos a Equação 8 na Equação 9.

$$P = P_0 - 10 * \alpha * \log_{10}\left(\frac{d}{d_0}\right) + n \quad (8) \qquad d = 10^{(P_0 - P + 10*\alpha*\log_{10}(d_0) + n)} \quad (9)$$

Os valores P e P_0 podem ser obtidos durante a medição. O valor d_0 é igual a 1 metro e o α, em ambientes terrestres, é igual a 3 [Al-Hourani and Gomez 2017], bastando

então determinar o valor n. De maneira empírica foi observado que em um ambiente sem obstáculos e coberto por um roteador doméstico, há pouca variação para o erro de medição da força do sinal entre o ponto de acesso, o drone e o atacante. Desse modo, para a nossa solução atual, calculamos o valor de n com base na medição do sinal entre o drone e o ponto de acesso. Para isso, basta isolar o valor de n na Equação 9 e calcular a distância entre o ponto de acesso e o drone, baseada em suas localizações, que são conhecidas.

3.2. Algoritmo de localização

O algoritmo 1 apresenta a nossa solução para calcular a localização do dispositivo malicioso aplicando a regra de Cramer. A tupla T contém as forças de sinais P e P_0 e os vetores de coordenadas da localização do dispositivo que enviou a informação ao servidor (ponto de acesso ou drone). O valor n é o erro de medição da força do sinal. Como estamos usando o valor n, que calculamos previamente, não utilizaremos o vetor de erros e (Equação 4), pois já estamos tratando os erros durante o cálculo das distâncias.

Algoritmo 1: CÁLCULO DA LOCALIZAÇÃO

Entrada: T e n
Saída: Localização da máquina atacante

1 **início**
2 $D = \{\}$
3 $vloc = (0, 0, 0)$
4 $i = 0$
5 **para** *cada* $t \in T$ **faça**
6 $D[i] =$ CalculaDistancia(t, n)
7 i++
8 **fim**
9 $u =$ GeraVetoru(T, D)
10 $V =$ GeraMatrizV(T)
11 $v1 = 2 * ((T[2].x - T[1].x), (T[3].x - T[1].x), (T[3].x - T[2].x))$
12 $v2 = 2 * ((T[2].y - T[1].y), (T[3].y - T[1].y), (T[3].y - T[2].y))$
13 $v3 = 2 * ((T[2].z - T[1].z), (T[3].z - T[1].z), (T[3].z - T[2].z))$
14 $x_A = \frac{det(u.v1)}{det(V)}$
15 $y_A = \frac{det(u.v2)}{det(V)}$
16 $z_A = \frac{det(u.v3)}{det(V)}$
17 $vloc = (x_A, y_A, z_A)$
18 **fim**
19 **retorna** $vloc$

Nas linhas 2 e 3 são inicializadas as variáveis auxiliares, responsáveis por alocar as distâncias e o vetor com a localização da máquina atacante. A linha 4 contém a inicialização do contador auxiliar. Nas linhas 5 a 8 são calculadas as distâncias e as linhas 9 e 10 usam os valores das distâncias e as localizações do ponto de acesso e do drone para calcular o resultado relativo as Equações 2 e 3. Já as linhas 11 a 16 apresentam a aplicação direta da regra de Cramer. Finalmente, na linha 17, as coordenadas calculadas são atribuídas ao vetor de localização do dispositivo malicioso.

4. Simulação e Experimentos

4.1. Configuração da simulação

A simulação foi executada utilizando o Network Simulator 3 (NS3) [Riley and Henderson 2010] em uma máquina virtualizada com 5GB RAM e processador core i7-8550U CPU 1,8GHz, rodando um sistema operacional Ubuntu 18.04.3 LTS. O código da simulação foi escrito na linguagem C++ e a análise dos resultados foi feita usando scripts escritos em pyhton 3.5[1].

Para a topologia de rede foi usado um *host* servidor, ligado por uma conexão ponto a ponto ao *host* usado como ponto de acesso (AP) wi-fi, um *host* móvel (drone) com conexão wi-fi e um número variado de outros *hosts* estáticos conectados a rede sem fio. A cada execução da simulação, um dos *hosts* estáticos não identificado é escolhido aleatoriamente para atuar como atacante.

A área coberta durante a simulação é de aproximadamente $100m^2$, a mesma área de cobertura de um roteador wifi doméstico. Inserimos também uma taxa de erros de envio de pacote de 0.001%. Essa taxa é sugerida em um dos exemplos do tutorial do próprio simulador. O intervalo entre o envio de pacotes é 1s. Finalmente, a velocidade de deslocamento do drone é constante e igual a 10m/s.

Configuração	Número de nós fixos	Número de nós móveis	Total de nós
ID 1	12	1	13
ID 2	52	1	53
ID 3	102	1	103
ID 4	252	1	253

Tabela 1. Configurações da simulação

Foram feitas 30 execuções para cada uma das quatro configurações utilizadas. Para cada configuração foi variado o número de *hosts* wi-fi fixos não identificados, conforme apresentado na Tabela 1. Note que usamos um drone (nó móvel), um servidor (nó fixo) e um AP fixo (nó fixo) em todas as configurações.

4.2. Resultados

A simulação foi avaliada em dois aspectos: (i) quanto à distância entre a localização encontrada e a localização real da máquina atacante; e (ii) quanto ao tempo despendido até a localização aproximada do alvo ser calculada.

Configuração	Distância (mm)	Tempo de execução (s)
ID 1	0.74 ± 0.57	10.28 ± 1.49
ID 2	0.5 ± 0.37	9.8 ± 0.84
ID 3	0.32 ± 0.26	9.63 ± 0.3
ID 4	0.19 ± 0.11	9.61 ± 0.19

Tabela 2. Resultados médios da simulação

[1]Os códigos da simulação estão disponíveis em: https://bit.ly/2LU55st

Para a distância, os resultados mostraram uma precisão de mm em todas as configurações avaliadas. As maiores distâncias ocorreram nas simulações do tipo 1 e 2. O tempo despendido durante as simulações variou entre 9 e 14 segundos. Novamente, as simulações do tipo 1 foram as que tiveram resultados piores. A Tabela 2 sumariza as médias e desvios padrões ($\pm$) para cada configuração.

4.3. Discussão

Os resultados muito positivos da nossa técnica em relação a distância estão diretamente relacionados ao erro de medição n utilizado. Como o simulador utiliza um valor n de referência que praticamente não varia, ao calcularmos o nosso próprio n, obtivemos um valor muito próximo do valor de referência do simulador, o que, consequentemente, permitiu a alta precisão do algoritmo.

Para os casos avaliados, o valor do erro de medição que utilizamos é suficiente. No entanto, não garantimos que esse comportamento seja o mesmo em um ambiente real. Nesse caso, poderíamos precisar calcular o valor de n de outra maneira. Porém, uma vez que a técnica proposta permite que outros tipos de cálculos para este valor sejam empregados, cremos que os resultados obtidos na simulação são suficientes para validar que a nossa técnica é capaz de calcular a localização aproximada do alvo.

Os resultados do tempo despendido para localizar o alvo, que independe do cálculo da localização, indicam que o tempo demandado para localizar a máquina atacante utilizando a técnica proposta é pequeno, próximo de 10s, para a área especificada.

Por último, apesar da variação mínima nos resultados, as simulações indicaram que o número de nós impacta pouco no desempenho da técnica. Cremos que os resultados estão relacionados ao maior espalhamento com menos nós dentro do ambiente.

5. Trabalhos Relacionados

Existe na literatura um grande número de trabalhos relacionados à detecção de ataques na rede [Meng et al. 2019] [Tidjon et al. 2019], entretanto, é difícil encontrar abordagens para a localização física do dispositivo atacante. No nosso contexto, destaca-se o estudo de Nobles et al. (2011), no qual é apresentada uma estratégia para o rastreamento de um invasor da rede em ambientes fechados. Isso é feito usando a força do sinal sem fio para calcular a distância entre o alvo e os vários pontos de acesso. Essa distância é então utilizada para localizar o alvo usando trilateração.

De maneira similar a Nobles et al. (2011), nossa proposta utiliza a força do sinal de rede e um algoritmo de trilateração. Entretanto, para calcular as distâncias usamos um ponto de acesso e um drone, o que permite que a nossa técnica possa ser utilizada em ambientes abertos e fechados, sem necessitar conhecer todos os pontos de acesso na rede. Sendo assim possível utilizá-la em locais com acesso público à rede sem fio.

Algumas pesquisas buscam encontrar âncoras virtuais usando drones. Por exemplo, em Halder et al. (2016) são apresentadas diferentes estratégias para localização de sensores em uma rede de sensores sem fio. Essas estratégias usam trilateração e alvos móveis e estáticas em ambientes abertos. Na mesma linha do estudo anterior, em [Sorbelli et al. 2018] são propostos dois algoritmos para localização de alvos estáticos em ambientes abertos, usando antenas direcionais e omnidirecionais. Esse trabalho compara

os resultados dos dois algoritmos propostos, através de uma simulação feita na linguagem de programação MATLAB. Há ainda trabalhos que buscam dispositivos de pessoas perdidas, como Acuma et al. (2017) e Sun et. al.. Acuma et al. (2017) propõem uma solução que identifica o sinal wifi de smartphones captados pela rede e um drone que capta esse sinal da rede, mapeiam o ambiente em zonas, com base nos sinais recebidos, e aplicam um algoritmo de *Random Forest* para encontrar a zona onde está o alvo. Já Sun et. al. (2018) utiliza uma ideia similar, mas busca filtrar as zonas usando novas medições do drone, trilateração e *Kalman filters*, com isso aumenta a precisão da localização encontrada.

Os estudos de Halder et. al. (2016) e Sorbelli et. al. (2018) focam na localização de nós alvos em redes de sensores sem fio, que se comunicam com o drone. Já Acuma et al. (2017) e Sun et. al. (2018) buscam dispositivos capturando sinais da rede wifi para mapear zonas específicas. Por outro lado, nós propomos uma técnica para localizar dispositivos atacantes utilizando um IDS que detecta o ataque e aciona o drone, que por sua vez usa as informações fornecidas pelo IDS para encontrar o alvo. Além disso, consideramos informações do ponto de acesso usado pelo dispositivo alvo, o que diminui a quantidade de medições que o drone precisa fazer. Tanto o cenário quanto a técnica proposta se diferencia de demais trabalhos apresentados na literatura.

6. Conclusão

Esse trabalho apresentou uma técnica para localização de uma máquina estática usada para atacar redes sem fio em ambientes públicos. Essa técnica foca em um cenário pouco explorado utilizando medições provenientes de um drone e de um ponto de acesso para calcular a localização do alvo, através de trilateração. A proposta foi avaliada com simulações geradas no NS 3 e os resultados indicaram que a técnica é capaz de localizar a máquina atacante em um pequeno período de tempo em uma área de $100m^2$ e com um número variado de nós. Como trabalhos futuros, pode-se estender a técnica para usar mais de um drone e alvos móveis na rede, e também avaliar outras soluções para calcular trilateração, como métodos baseados em eliminação gaussiana. Além disso, cenários com mais variáveis podem ser simulados.

Agradecimentos

Este trabalho foi realizado com apoio da CAPES, código de financiamento 001, e também do CNPq através da bolsa de produtividade DT-2 (Nº do processo 315543/2018-3) de Rossana M. de C. Andrade.

Referências

Abhayawardhana, V., Wassell, I., Crosby, D., Sellars, M., and Brown, M. (2005). Comparison of empirical propagation path loss models for fixed wireless access systems. In *2005 IEEE 61st Vehicular Technology Conference*, volume 1, pages 73–77. IEEE.

Acuna, V., Kumbhar, A., Vattapparamban, E., Rajabli, F., and Guvenc, I. (2017). Localization of wifi devices using probe requests captured at unmanned aerial vehicles. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE.

Al-Hourani, A. and Gomez, K. (2017). Modeling cellular-to-uav path-loss for suburban environments. *IEEE Wireless Communications Letters*, 7(1):82–85.

Alotaibi, B. and Elleithy, K. (2016). Rogue access point detection: Taxonomy, challenges, and future directions. *Wireless Personal Communications*, 90(3):1261–1290.

Brutch, P. and Ko, C. (2003). Challenges in intrusion detection for wireless ad-hoc networks. In *2003 Symposium on Applications and the Internet Workshops, 2003. Proceedings.*, pages 368–373. IEEE.

Chamoso, P., González-Briones, A., Rodríguez, S., and Corchado, J. M. (2018). Tendencies of technologies and platforms in smart cities: a state-of-the-art review. *Wireless Communications and Mobile Computing*, 2018.

Cirqueira, A. C., Andrade, R. M. C., and CASTRO, M. F. (2011). Um mecanismo de segurança com adaptação dinâmica em tempo de execução para dispositivos móveis. *XXXVIII Seminário Integrado de Software e Hardware (SEMISH)*.

Courtay, A., Le Gentil, M., Berder, O., Scalart, P., Fontaine, S., and Carer, A. (2019). Anchor selection algorithm for mobile indoor positioning using wsn with uwb radio. In *2019 IEEE Sensors Applications Symposium (SAS)*, pages 1–5. IEEE.

Halder, S. and Ghosal, A. (2016). A survey on mobile anchor assisted localization techniques in wireless sensor networks. *Wireless Networks*, 22(7):2317–2336.

Koutsonikolas, D., Das, S. M., and Hu, Y. C. (2007). Path planning of mobile landmarks for localization in wireless sensor networks. *Computer Communications*, 30(13).

Meng, Y., Li, J., Zhu, H., Liang, X., Liu, Y., and Ruan, N. (2019). Revealing your mobile password via wifi signals: Attacks and countermeasures. *IEEE Transactions on Mobile Computing*.

Mozaffari, M., Saad, W., Bennis, M., Nam, Y.-H., and Debbah, M. (2019). A tutorial on uavs for wireless networks: Applications, challenges, and open problems. *IEEE Communications Surveys & Tutorials*.

Murphy, W. and Hereman, W. (1995). Determination of a position in three dimensions using trilateration and approximate distances. *Department of Mathematical and Computer Sciences, Colorado School of Mines, Golden, Colorado, MCS-95*, 7:19.

Nobles, P., Ali, S., and Chivers, H. (2011). Improved estimation of trilateration distances for indoor wireless intrusion detection. *JoWUA*, 2(1):93–102.

Riley, G. F. and Henderson, T. R. (2010). The ns-3 network simulator. In *Modeling and tools for network simulation*, pages 15–34. Springer.

Sorbelli, F. B., Das, S. K., Pinotti, C. M., and Silvestri, S. (2018). Range based algorithms for precise localization of terrestrial objects using a drone. *Pervasive and Mobile Computing*, 48:20–42.

Sun, Y., Wen, X., Lu, Z., Lei, T., and Jiang, S. (2018). Localization of wifi devices using unmanned aerial vehicles in search and rescue. In *2018 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pages 147–152. IEEE.

Tidjon, L. N., Frappier, M., and Mammar, A. (2019). Intrusion detection systems: A cross-domain overview. *IEEE Communications Surveys & Tutorials*.

Watts, S. (2016). Secure authentication is the only solution for vulnerable public wifi. *Computer Fraud & Security*, 2016(1):18–20.