Nouvelles techniques de localisation des cyberattaques dans les réseaux sans fil.

ANQUETIL Eloi - IR4
BERGER Richard - IR4
BONFILS Kim - IR4
SISSUNG Félix - IR4

BOUDEBS Mihaela
BENZEKKI Kamal

Semestre 8 2023

Table des matières

1 Introduction

Le Projet Scientifique 2 (PSIR 2) représente une phase cruciale d'application pratique des stratégies élaborées lors de notre précédente recherche sur la cybersécurité des réseaux sans fil. Sous la direction de M. Kamal BENZEKKI, cette phase se concentre sur la simulation et la mise en œuvre réelle des méthodes de détection et de localisation des cyberattaques, en particulier celles utilisant les technologies 5G et les drones dans des attaques de type Man in the Middle. En recréant des scénarios d'attaque complexes, notre équipe vise à tester la robustesse et l'efficacité de nos solutions dans un environnement contrôlé.

Ce projet offre également une occasion exceptionnelle pour les étudiants de mettre en pratique leurs compétences théoriques dans un cadre réaliste et dynamique. En participant à la PSIR 2, les étudiants bénéficient d'une expérience immersive qui renforce leur compréhension des concepts de cybersécurité et affine leur capacité à répondre efficacement aux défis technologiques actuels. Cette application directe de la théorie à la pratique est fondamentale pour préparer les futurs ingénieurs à contribuer activement à l'évolution de la sécurité dans le domaine des technologies avancées.

2 Objectifs du Projet

2.1 Problématique

Dans le cadre de notre recherche sur la cybersécurité, une problématique centrale émerge suite à l'augmentation des incidents impliquant des attaques Man in the Middle orchestrées par des drones dans le contexte des entreprises. Ces incidents, soulignés par des publications récentes, révèlent une vulnérabilité croissante face à l'intégration des technologies de drones et de la 5G. Ces attaques posent non seulement un risque de sécurité pour les infrastructures critiques, mais elles remettent également en question l'efficacité des systèmes de détection et de réponse existants.

Notre projet de recherche s'attache donc à répondre à cette problématique urgente : comment la convergence de la 5G et de l'utilisation de drones dans des attaques Man in the Middle redéfinit-elle les méthodes de détection et de localisation des cybermenaces dans un contexte entrepreneurial ? Cette question découle directement de la prise de conscience des menaces réelles et récentes, et de la nécessité de développer des solutions avancées pour contrer efficacement cette nouvelle forme d'attaque. L'enjeu est de taille, car il s'agit de protéger les entreprises contre des intrusions de plus en plus sophistiquées, tout en assurant la continuité et la sécurité des opérations commerciales.

2.2 Hypothèses

Dans le cadre de notre étude sur la sécurité des réseaux sans fil confrontés aux attaques Man in the Middle orchestrées par des drones, nous formulons plusieurs hypothèses clés :

Influence des caractéristiques de la 5G :

Nous postulons que les spécificités techniques de la 5G, comme la bande passante élevée, la faible latence et le débit de données accru, jouent un rôle prépondérant dans l'efficacité des méthodes de détection de ces attaques. Ces caractéristiques pourraient soit faciliter la détection rapide des anomalies dues à des intrusions, soit compliquer cette détection en raison de la complexité accrue des données transitant dans le réseau.

Impact de la convergence de la 5G et des drones :

Nous supposons que l'utilisation conjointe de la 5G et des drones dans des scénarios d'attaque Man in the Middle redéfinit les enjeux de sécurité, en augmentant la surface d'attaque et en modifiant les vecteurs traditionnels d'attaques cybernétiques. Cette convergence pourrait entraîner de nouvelles formes de vulnérabilités spécifiques à ces technologies.

Modification détectable des performances de la 5G :

Enfin, nous considérons que l'introduction délibérée d'un dispositif Man in the Middle au sein de la liaison 5G pourrait altérer ses performances de manière détectable. Cette perturbation pourrait se manifester par des anomalies dans les paramètres de réseau, comme des variations de latence ou de débit, qui pourraient être exploitées pour identifier et localiser l'attaque.

2.3 Analyse théorique et expérimentale de l'état de l'art

2.3.1 Synthèse des Méthodes et Outils

Dans notre étude, nous avons principalement utilisé MATLAB pour la simulation et la modélisation des attaques. Un code spécifique a été dans un premier temps repris, puis développé pour simuler les attaques de type Man in the Middle (MITM) dans les environnements 5G. Par ailleurs, nous avons utilisé Cisco pour représenter la topologie du réseau, ce qui nous a permis de visualiser et de comprendre la configuration et l'impact des attaques sur le réseau.

2.3.2 Identification des Solutions Partielles

Nous avons identifié plusieurs solutions partielles à notre problématique. Par exemple, certaines études ont proposé des solutions de détection basées sur la caractérisation des signatures des attaques MITM dans les environnements 5G. D'autres recherches se concentrent sur l'utilisation des drones pour surveiller les réseaux et détecter les intrusions en temps réel. Ces solutions, bien qu'efficaces dans certains contextes, présentent des limitations en termes de portée, de coût et de complexité de mise en œuvre.

2.3.3 Difficultés et Contraintes

Les freins technologiques incluent la complexité des infrastructures 5G et la nécessité de dispositifs sophistiqués pour la surveillance et la détection des attaques. Sur le plan scientifique, l'intégration des technologies de détection avec les protocoles existants reste un défi majeur. Les contraintes humaines concernent nous étudiant n'ayant pas les formations requises pour gérer ces technologies avancées, tandis que les contraintes financières portent sur les coûts élevés des équipements et des logiciels de simulation.

Un rappel détaillé du plan d'expérience est situé dans l'Annexe 1.

3 Méthode et résultats expérimentaux

3.1 Question de recherche

La conception de notre expérience est étroitement liée à une des hypothèses formulées dans notre recherche, visant à répondre à la problématique de la sécurité des réseaux sans fil face aux attaques Man in the Middle (MITM) orchestrées par des drones dans un environnement 5G. Cette section explique la justification de notre approche expérimentale et précise l'orientation de notre étude pratique.

Une des hypothèses centrales de notre étude est que l'introduction délibérée d'un dispositif Man in the Middle au sein de la liaison 5G pourrait altérer ses performances de manière détectable. Cette perturbation pourrait se manifester par des anomalies dans les paramètres de réseau, comme des variations de latence ou de débit, qui pourraient être exploitées pour identifier et localiser l'attaque.

Pour vérifier cette hypothèse, nous avons conçu une série d'expériences utilisant MATLAB pour la simulation des attaques MITM et Cisco pour la représentation de la topologie du réseau. Les raisons de cette approche sont les suivantes :

Capacités Avancées de MATLAB : MATLAB offre des outils puissants pour la simulation et la modélisation des signaux 5G, permettant de créer des scénarios réalistes et de simuler l'impact des attaques

MITM sur la performance du réseau. Cela nous permet de mesurer avec précision les variations de latence et de débit dans différents scénarios d'attaque. **Code Matlab dans l'annexe 3**

Visualisation de la Topologie avec Cisco : Utiliser Cisco pour représenter la topologie du réseau nous permet de visualiser la configuration et de mieux comprendre l'impact spatial des attaques. Cela aide à identifier les points faibles et les vecteurs d'attaque potentiels dans l'infrastructure réseau. **Visualisation de la topologie dans l'annexe 2**

Représentation Réaliste des Attaques : En combinant les capacités de simulation de MATLAB avec les outils de visualisation de Cisco, nous pouvons recréer des scénarios d'attaques réalistes. Cette approche permet de tester l'efficacité des méthodes de détection basées sur les anomalies de performance réseau.

Finalement, l'orientation de notre étude pratique est donc axée sur la détection des anomalies de performance réseau causées par des attaques MITM. En mesurant et en analysant les variations de latence et de débit, nous espérons développer des méthodes de détection robustes qui peuvent être intégrées dans les systèmes de sécurité existants pour améliorer la résilience des réseaux 5G contre les cyberattaques.

Un rappel détaillé du plan d'expérience est situé dans l'Annexe 1

3.2 Méthode de travail pour la partie expérimentale

Pour notre projet sur la détection des cyberattaques dans les réseaux 5G utilisant des drones, nous avons adopté une approche méthodique combinant simulation et expérimentation pratique. Voici les étapes détaillées de notre méthode de travail :

Simulation Préliminaire avec MATLAB

3.2.1 Recherche et Adaptation de Code

Nous avons commencé par rechercher des codes existants dans la littérature spécialisée traitant des attaques de type Man in the Middle (MITM) dans les réseaux sans fil. Un code de base a été sélectionné pour sa pertinence et son adaptabilité à notre contexte. Ce code a ensuite été modifié pour simuler les particularités des attaques MITM dans un environnement 5G, en intégrant des paramètres spécifiques tels que la bande passante élevée et la faible latence.

3.2.2 Utilisation de MATLAB

MATLAB a été choisi pour sa puissance dans la simulation et la modélisation des signaux 5G. L'outil nous a permis de créer des scénarios réalistes et de mesurer avec précision les variations de latence et de débit dans différents contextes d'attaque.

3.2.3 Répartition des Tâches

Pour minimiser les erreurs et optimiser l'efficacité, une seule personne de l'équipe a été désignée pour gérer le code, assurant ainsi une continuité et une cohérence dans les modifications apportées. Expérimentation Pratique avec un Drone

3.3 Résultats et Analyse

Les résultats de notre étude expérimentale ont confirmé notre hypothèse principale : l'introduction d'un dispositif MITM dans un réseau 5G génère des anomalies détectables dans les performances du réseau. Voici un résumé des principales observations :

3.3.1 Détection des Anomalies de Performance

Les simulations et les expérimentations pratiques ont montré que les attaques MITM causent des variations significatives de la latence et du débit dans le réseau 5G. Ces anomalies peuvent être détectées et analysées pour identifier la présence d'une attaque.

3.3.2 Impact des Caractéristiques de la 5G

Les spécificités de la 5G, telles que la faible latence et la bande passante élevée, influencent à la fois la détection et la complexité des attaques. Par exemple, la bande passante élevée permet une détection plus rapide des anomalies, tandis que la faible latence complique parfois l'identification précise des intrusions.

3.3.3 Visualisation des Données

En utilisant les outils de visualisation de MATLAB, nous avons pu représenter graphiquement les résultats obtenus. Les graphiques ont illustré les variations de latence et de débit, montrant clairement les impacts des attaques MITM sur le réseau.

3.3.4 Validation des Méthodes de Détection

Les méthodes de détection basées sur les anomalies de performance ont prouvé leur efficacité. Les résultats montrent que ces méthodes peuvent être intégrées dans les systèmes de sécurité existants pour améliorer la résilience des réseaux 5G contre les cyberattaques.

4 Conclusion

Ce projet sur la détection des cyberattaques dans les réseaux 5G en utilisant des drones a permis de mettre en évidence plusieurs aspects cruciaux de la sécurité des infrastructures modernes. En combinant simulation et expérimentation pratique, nous avons pu valider notre hypothèse principale : l'introduction d'un dispositif Man in the Middle (MITM) dans un réseau 5G engendre des anomalies de performance détectables, notamment des variations significatives de la latence et du débit.

Les résultats obtenus démontrent que les caractéristiques spécifiques de la 5G, telles que la bande passante élevée et la faible latence, jouent un rôle déterminant dans la détection et la complexité des attaques. Alors que la bande passante élevée facilite la détection rapide des anomalies, la faible latence peut parfois compliquer l'identification précise des intrusions. Ces observations soulignent la nécessité de développer des méthodes de détection robustes et adaptées aux particularités des réseaux 5G.

L'utilisation des drones dans nos expérimentations a également mis en lumière l'augmentation de la surface d'attaque et la modification des vecteurs traditionnels d'attaques cybernétiques. Cette convergence entre la 5G et les drones crée de nouvelles vulnérabilités spécifiques qui doivent être prises en compte dans la conception des futures infrastructures de sécurité.

En conclusion, ce projet a non seulement confirmé les hypothèses initiales, mais il a aussi ouvert des perspectives pour des recherches futures sur l'amélioration des systèmes de détection des cyberattaques. Les défis technologiques, scientifiques, humains et financiers identifiés au cours de cette étude offrent des pistes claires pour les développements futurs. Il est essentiel de continuer à explorer ces voies afin de renforcer la résilience des réseaux 5G face aux cybermenaces croissantes.

Pour les futures recherches, il serait pertinent de se concentrer sur l'intégration des technologies de détection avancées avec les protocoles existants et de développer des solutions plus sophistiquées et accessibles pour la surveillance et la détection des intrusions. La formation des ingénieurs et des techniciens spécialisés dans ces technologies sera également cruciale pour garantir une sécurité optimale des réseaux sans fil de nouvelle génération.

5 Bibliographie

Références

[1] Bruce Sussman ; *The Drone Cyberattack That Breached a Corporate Network* ; 10.21.22

[2] Linh LE, Tu N NGUYEN, Kun SUO, Jing HE ; *5G network slicing and drone-assisted applications : a deep reinforcement learning approach* ; October 2022

[3] F. Castillo, P. García-Fernández, R. Manzoor, R. D. Luna-Ramírez, A. M. Meissner, C. Carrascosa, A. R. Figueiras-Vidal ; *A Survey of Control Architectures for Social Robots : From Direct to Cloud-Based Approaches* ;2019

[4] A. R. Figueiras-Vidal, R. Manzoor, C. Carrascosa, A. M. Meissner, F. Castillo, R. D. Luna-Ramírez ;*Swarm Robotics : A New Approach to Distributed Artificial Intelligence* ; 2019

[5] Federal Aviation Administration (FAA) (USA) ; *Unmanned Aircraft Systems (UAS) – Part 107* ; 2022

[6] M. Alotaibi, A. Alshahrani, A. Alotaibi ; *A Review on Unmanned Aerial Vehicles (UAVs) Cyber-Physical Systems (CPS) : Applications, Risks, Vulnerabilities, Threats, Challenges, and Future Directions* ; 2020

[7] Charan Gudla, Md. Shohel Rana, and Andrew H. Sung ; *Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles*

[8] TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU *Architectural framework for machine learning in future networks including IMT-2020* 06/2019

[9] Sandra ONDRUSOVA *5G Implementation Guidelines* July 2019

6 Annexe 1

6.1 Rappel du plan d'expérience

Configuration de l'Environnement de Simulation

Dans cette première phase, nous débuterons par l'installation de MATLAB, l'environnement de simulation privilégié. Cela inclut également l'intégration des outils de simulation pertinents pour le domaine de la communication sans fil. Une fois MATLAB installé, nous procéderons à la configuration minutieuse de l'environnement de simulation, en définissant les paramètres nécessaires pour assurer la précision et la cohérence des résultats obtenus.

Modélisation du Canal de Communication

À l'aide des puissantes fonctionnalités de MATLAB, nous allons créer un modèle détaillé du canal de communication sans fil. Cette modélisation englobera les caractéristiques spécifiques au contexte de la 5G, intégrant les canaux de propagation et tenant compte des effets de fading qui influent sur la qualité de la transmission.

Génération de Signaux 5G

Nous explorerons les capacités de génération de signaux 5G simulés, offertes par MATLAB. Cela implique la configuration des paramètres essentiels tels que les fréquences porteuses, les modulations, ainsi que les propriétés des antennes utilisées dans la communication sans fil.

Simulation de la Transmission

Cette étape consistera à établir une simulation complète de la transmission entre l'émetteur et le récepteur. Pour rendre cette simulation plus réaliste, nous essaierons d'introduire des modèles de bruit et de perturbation, reflétant ainsi des conditions similaires à celles rencontrées dans des environnements réels. Nous intégrerons également un dispositif "Man in the Middle" qui interagira entre l'émetteur et le récepteur pour créer une cyber attaque.

Analyse des Performances

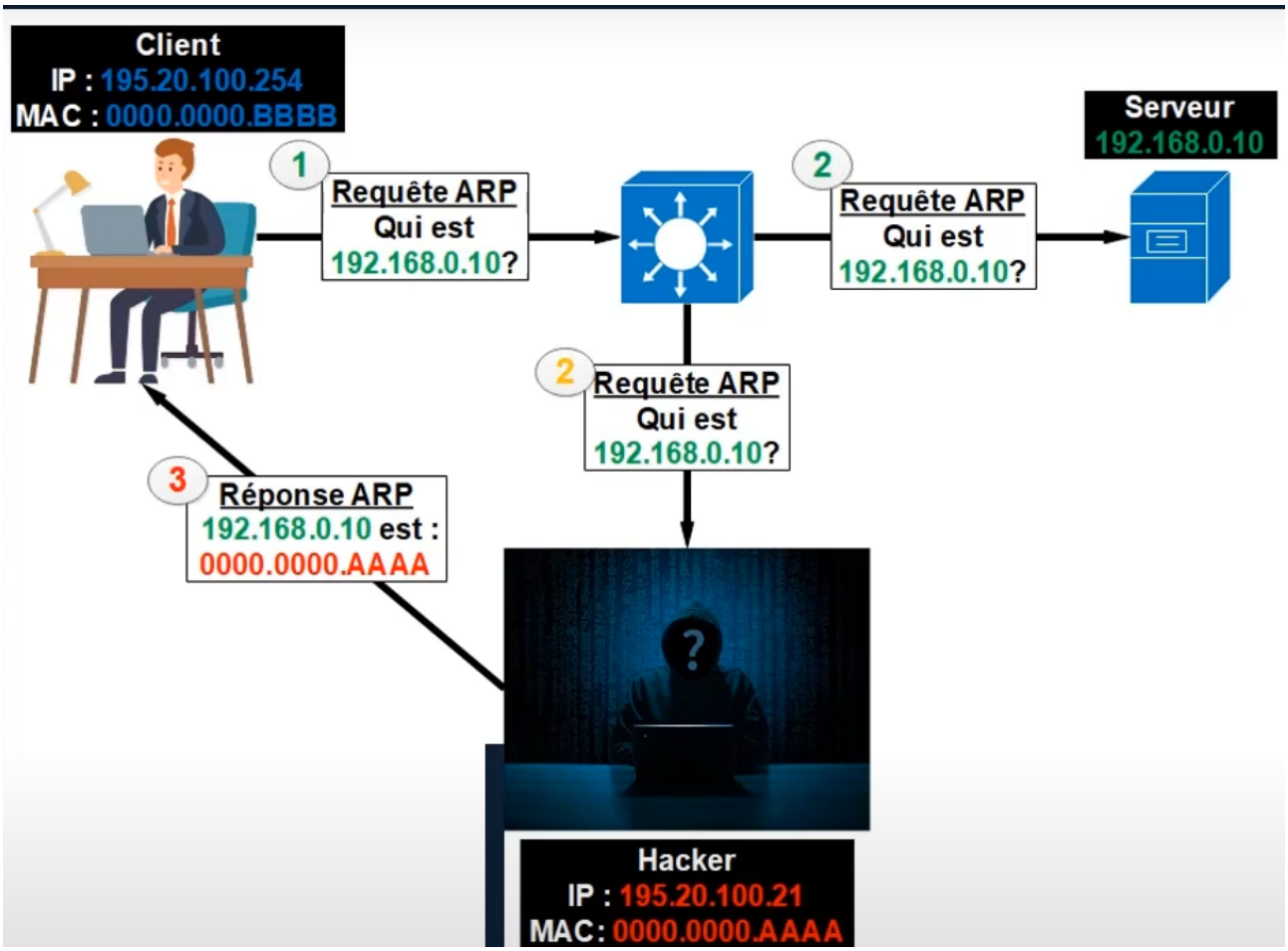
En utilisant des fonctions spécifiques de MATLAB, nous procéderons à la mesure rigoureuse des paramètres de performance, notamment le débit, la latence et d'autres métriques cruciales. L'analyse détaillée nous permettra d'évaluer l'impact de divers paramètres sur les performances de la liaison 5G avec la technologie " MITM".

Visualisation des Résultats

Les outils de visualisation de MATLAB seront exploités pour représenter graphiquement les résultats obtenus au cours de la simulation. Des graphiques informatifs illustreront de manière visuelle l'évolution des performances en fonction des paramètres étudiés, offrant une compréhension plus approfondie des technologies utilisées dans la simulation.

7 Annexe 2

7.1 Représentation de l'attaque en image



Topologie Cisco Packet Tracer basée sur l'image ci-dessus.

8 Annexe 3

8.1 Code Matlab

Code basé sur :

`https://fr.mathworks.com/help/control/ug/detect-attack-in-microgrid-using-dynamic-watermarkin`
`html`