Sujet de thèse :

Vers une résilience accrue des réseaux 5G/6G : approche multi-échelle pour la détection et le contournement de menaces réseau

Mohand Yazid Saidi et Mohamed Amine Ouamri
Laboratoire L2TI (UR 3043), Equipe Réseaux

Description du sujet

Cette thèse propose de développer des approches avancées pour détecter et contrer les attaques réseau, plus particulièrement les attaques de déni de service par flooding ciblant le trafic de contrôle des réseaux 5G/6G. En combinant des architectures LSTM et leurs variantes avec une analyse comportementale fine du trafic, l'objectif est de concevoir un système capable de détecter les anomalies en temps réel et de déployer automatiquement des mécanismes de mitigation adaptés, garantissant ainsi la résilience des réseaux 5G/6G.

Contexte et problématique

Les réseaux 5G, fondés sur l'architecture NFV/SDN, séparent le plan de contrôle (SMF) du plan utilisateur (UPF), offrant scalabilité et flexibilité via la virtualisation des fonctions réseau. Cette séparation, bien que révolutionnaire, expose de nouvelles vulnérabilités : le trafic de contrôle devient une cible privilégiée pour les attaques de flooding, pouvant saturer les UPF et interrompre les flux utilisateurs critiques (télémédecine, véhicules autonomes, IoT).

Les approches traditionnelles basées sur signatures ou règles statiques s'avèrent inadaptées face à des attaques polymorphes et évolutives. Cette thèse ambitionne de surmonter ces limites par une approche comportementale proactive combinant :

- Détection multi-échelle via LSTM, BiLSTM et mécanismes d'attention,
- Modèles hybrides CNN-attention pour motifs spatiaux-temporels,
- Mitigation adaptative temps réel préservant la QoS légitime

Plateforme expérimentale et méthodologie

Phase 1 (6 mois) : État de l'art et analyse des vulnérabilités du trafic de contrôle 5G.
Phase 2 (6 mois) : Développement d'une plateforme Open5GS complète intégrant :

- Plan contrôle (SMF) + Plan données (UPF)
- Simulateur de terminaux utilisateur
- Générateur d’attaques de type flooding évolutives

Phase 3 (6 mois) : Génération de datasets incluant/constitué de trafic de contrôle (normal/malveillant) + benchmarks.
Phase 3 (15 mois) :

- Proposition de diverses approches basée sur l’apprentissage pour la détection et la mitigation en temps réel d’attaques évolutives :
    - LSTM/BiLSTM + Attention pour patterns temporels
    - CNN hybrides pour motifs multi-granularité
    - Transfer learning attaques zero-day

- IDS intelligent avec capacités mitigation incluant les propositions précédentes.
- Validation expérimentale complète (précision, F1-score, robustesse, impact QoS).

Phase 4 (3 mois) : Rédaction du manuscrit de thèse.

Objectifs scientifiques et résultats attendus

- Détection proactive d'anomalies sur le trafic (plus spécifiquement sur le trafic de contrôle)
- Contournement adaptative en temps réel (blocage sélectif, throttling intelligent, généralisation attaques zero-day via transfer learning).
- Assurer la préservation de la QoS du trafic légitime pendant les attaques.
- Plateforme open-source réutilisable pour la génération de trafic dans les réseaux 5G.

Profil des candidats

- Connaissances en IA nécessaire (plus spécifiquement en apprentissage profond).
- Connaissances des réseaux 5G/6G est un plus.
- Anglais nécessaire.

Mots clés

Apprentissage profond, cybersécurité, réseaux 5G/6G, anglais, réseaux informatiques et/ou télécoms

Contacts

- Mohand Yazid SAIDI saidi@univ-paris13.fr
- Mohamed Amine OUAMRI mohamedamine.ouamri@univ-paris13.fr