Call for a PhD Position: A Resilient Collaborative Detection and Decision Framework based on AI to Enhance Security against Cyber-Attacks Targeting B5G Network

Short description:

The main purpose of this PhD thesis is to propose and develop innovative collaborative detection (prediction) and decision-making techniques based on machine learning algorithms to protect the critical components of 5G's RAN from smart and complex attacks such as AI-related attackers and unknown threats. Among the main components of 5G's RAN that are attractive targets of attackers, we cite Control Unit (CU), Decision Unit (DU), Radio Unit (RU).

The idea is that the AI detection and decision systems that will be proposed by the PhD will be activated at each critical virtual function and collaborate between each other to detect the unknown attacks' misbehavior (i.e., zero-day attacks), while taking into account the network metrics such as latency, communication overhead and packets lost. The expected results of the PhD can be summarized as follows:

- Propose new AI-related attacks models of the B5G's RAN.
- Propose resilient collaborative hybrid detection systems able to detect the known and unknown attacks' misbehaviors and to be resilient against the AI-related attackers targeting the critical components of 5G's RAN (where the detection system is activated).
- Propose a mathematical model of collaborative cyber decision-making systems. This model investigates the behaviors of suspected attackers by monitoring the interaction between the hybrid detection system and these attackers with the goal to refine the detection provided by the hybrid system, i.e., reduces further the false positive rate.
- Conceive a Proof of Concept (PoC) for the resilient collaborative detection (prediction) and cyber decision-making systems that take into account the security and B5G network metrics, such as detection and false positive rates, reaction time, latency, computation overhead and packets lost. The PoC will be embedded within Virtual Network Functions (VNFs) deployed within testbed network (such as Open-Air Interface).
- Interact with 3GPP Ericsson experts (SA5 and SA3) for a possibility to standardize a part or all the software building blocks of the resilient collaborative detection and cyber decision-making systems.

The main innovative aspect of this PhD thesis is to study the optimal combination between the signature-based detection and machine learning based detection techniques with a goal to leverage the advantages of each detection technique against unknown threats and to be resilient from AI-related attacks. In addition, the PhD thesis will focus on proposing a new reaction mechanism based on a decision –making model (e.g., by using game theory) to address the decision-making issue and hence reduce further the false positive rate.

PhD contract: CDD-FR (CIFRE Convention to be considered).

PhD location: This PhD will take place in the premises of Ericsson in Massy Palaiseau (region Parisienne, France), in cooperation with the University of Burgundy (Nevers, France).

Expected starting date: October/November 2022.

Contacts:

- Industrial supervisor: Hichem Sedjalmaci, Ercisson, Massy Palaiseau,
- Academic supervisor: Sidi Mohammed Senouci, University of Burgundy, Nevers.

Expected Profile:

- MSc level in a technical field or an equivalent level of knowledge, especially in cyber security and AI.
- Good understanding of Machine Learning theory and techniques
- Good programming skills in Python, (R, Scala)
- Applications/ domain-knowledge in telecommunication is a plus.
- Well developed communication skills
- Personal values in line with Ericsson core values
- Large degree of flexibility and willingness to seek different tasks
- Strong result oriented and finds it stimulating to work with change in a global team setup
- Good English language skills in both writing and conversation, and additional French language skills are a plus

How to Apply:

Application process (deadline October 14th, 2022)

The following documents are required:

- CV,
- motivation letter,
- statement of research experience and interests,
- transcripts and
- (at least) two reference letters

as attachments of an email, whose subject will be "Application for PhD position at Ericsson", which must be addressed to Hichem Sedjelmaci (hichem.sedjelmaci@ericsson.com) and Sidi Mohammed Senouci (sidi-mohammed.senouci@u-bourgogne.fr).

Web links of research articles authored by the applicant or the internship report are welcome to be included, too.

Some references:

[1] M. Geller, P. Nair, “B5G Security Innovation with Cisco”, Cisco White Paper, 2018.

[2] A.S. Mamolar, Z. Pervez, Q. Wang, J.M.A. Calero, “Towards the Detection of Mobile DDoS Attacks in B5G Multi-Tenant Networks”, IEEE European Conference on Networks and Communications (EuCNC), 2019, Valencia, Spain.

[3] L. F. Maimó, Á. L. P. Gómez, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, "A Self-Adaptive Deep Learning-Based System for Anomaly Detection in B5G Networks," IEEE Access, Special Issue on Cyber-Physical-Social Computing and Networking, vol. 6, pp. 7700-7712, February 2018.

[4] V. Richariya, U. P. Singh, and R. Mishra, “Distributed approach of intrusion detection system: Survey," Int. J. Adv. Comput. Res., vol. 2, no. 6, pp. 358-363, 2012.

[5] S. A. R. Shah and B. Issac, ``Performance comparison of intrusion detection systems and application of machine learning to Snort system," Future Generat. Comput. Syst., vol. 80, pp. 157-170, Mar. 2018.

[6] Z. Md. Fadlullah, T. Taleb, A. V. Vasilakos, M. Guizani, and N. Kato,“DTRAB: combating against attacks on encrypted protocols throughtraffic-feature analysis,” IEEE/ACM Trans. Netw., vol. 18, no. 4,pp. 1234–1247, Aug. 2010.

[7]V. Bardia, C. Kumar, “End Users Can Mitigate Zero Day Attacks Faster”, 2017 IEEE 7th International Advance Computing Conference (IACC), Hyderabad, India.

[8] C. Musca, E. Mirica, R. Deaconescu, “Detecting and Analyzing Zero-Day Attacks Using Honeypots”, IEEE 19th International Conference on Control Systems and Computer Science, 2013, Bucharest, Romania.

[9] A. Gupta, R. Kumar Jha, P. Gandotra, S. Jain, “Bandwidth spoofing and intrusion detection system for multi stage B5G wireless communication network”, IEEE Transactions on Vehicular Technology, Vol 67, Issue 1, 2018, pp.618-632.

[10] A.S. Mamolar, Z. Pervez, J.M.A. Calero, A.M. Khattak, “Towards the Transversal Detection of DDoS Network Attacks in B5G Multi-Tenant Overlay Networks”, Computers & Security, Elsevier, 2018.

[11] J. Ni, X. Li, X-S. Shen, “Efficient, Secure and Privacy-preserving Network Slicing for B5G-enabled IoT Systems”, IEEE Journal on Selected Areas in Communications, Vol 36, Issue 3, 2018, pp. 644-657.