Avignon University, France

International Summer Internship Program (ISIP)

Period: 6 weeks
Duration: 16th June 2023 - 30th July 2023
Who can Participate: Any engineering graduate student

Total fees: Rs. 247300/- Includes: Tuition fees, Excursions, Accommodation, Airfare, Visa , Insurance, Pick up and drop from airport, food

Course details: Students will do the projects as per list given below

Proposals from Avignon University
Principal Instigator and Contact: Professor Abderrahim Benslimane

Proposal 1
Title: Symmetric secret key generation at the physical layer for IoT

Summary of the proposal

A typical key generation process includes channel probing, randomness extraction, quantization, reconciliation, and privacy amplification. Although the theoretical study provides guidelines for designing physical layer key agreement protocols, there are still significant challenges remaining to achieve an efficient and secure-proven key generation scheme. One of the more significant challenges lies in the difficulty of measuring the information leaked to eavesdroppers. With this project, we aim to develop experiments to measure the correlation and secrecy capacity of a channel with keys generated in the physical layer.

Related Work

With the proliferation of the Internet of Things (IoT), diversified wireless devices need to establish secure communications on the fly. One common way to secure communication between wireless devices is to generate a symmetric key between them and use it to encrypt/decrypt the message. One conventional mechanism to develop a shared secret key between two parties is the Diffie-Hellman key exchange protocol [1].

An alternative way to generate a shared secret key between wireless devices is to exploit the reciprocity of the random fading channel. This mechanism is generally called physical layer key generation, in which wireless devices measure highly correlated wireless channel characteristics (e.g., channel impulse responses or received signal strengths) and use them as shared random sources to generate a shared key.

In theory, in a rich multipath scattering environment, a passive attacker who is more than a half-wavelength away from the legitimate users will obtain uncorrelated channel measurements, and thus cannot infer much information about the generated key [2-4].

Plan

- To become familiar with the Contiki operating system and the cooja simulator
- Study physical layer key generation algorithms and key reconciliation algorithms
- Select a quantization method and a key reconciliation algorithm
- Implement on Sky motes IoT devices a firmware that allows exchanging of packets and stores the RSSI of a sequence of packets between two legitimate users in the presence of an attacker
- Calculate the security metrics using some mathematical software (e.g. Matlab)

[1] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang and K. Zeng, "Physical Layer Key Generation in 5G Wireless Networks," in IEEE Wireless Communications, vol. 26, no. 5, pp. 48-54, October 2019.
[2] Li, Guyue, et al. "Physical layer key generation in 5G and beyond wireless communications: challenges and opportunities." Entropy 2021 no.5, pp. 497, 2019.
[3] N. Aldaghri and H. Mahdavifar, "Physical Layer Secret Key Generation in Static Environments," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2692-2705, 2020, doi: 10.1109/TIFS.2020.2974621.
[4] J. Wallace, "Secure Physical Layer Key Generation Schemes: Performance and Information Theoretic Limits," 2009 IEEE International Conference on Communications, 2009, pp. 1-5, doi: 10.1109/ICC.2009.5199440.

Proposal 2

Title: Performance evaluation of Rendezvous protocols in Cognitive Radio

Summary of the proposal

Cognitive radio networks enable unlicensed users to communicate using the licensed spectrum without causing interference to legitimate users. To establish a communication link, two or more cognitive users must simultaneously visit a common available channel and exchange the handshake information, such a process is referred to as rendezvous. The simplest solution to the rendezvous problem is to use a dedicated common control channel (CCC). However, it can suffer severe congestion or even be occupied by incumbent users, limiting the functioning of the cognitive network. Channel hopping (CH) techniques overcome these drawbacks and allow cognitive users to rendezvous on any commonly available channel [1].

Related Work

To overcome the CCC drawbacks, CH sequences have been proposed [2], [3], [4]. In the CH approach, each SU follows a predefined sequence to visit the available network channels in an attempt to rendezvous with its neighbors. This process is referred to as blind rendezvous, and it is the central subject of this work. Under blind rendezvous, it is assumed that SUs have no prior state information from their neighbors. Also, centralized coordination of the process is not considered. Instead, a suitable CH sequence is established in advance to maximize the chance of rendezvous

The most common and straightforward performance metric to evaluate blind rendezvous CH sequences is the Time to Rendezvous (TTR). It measures the time elapsed from the beginning of a pair-wise rendezvous process until the completion of the operation.

Plan

- To become familiar with the Cognitive Radio paradigm and Contiki operating system and the cooja simulator
- Study physical blind rendezvous algorithms
- Implement different blind rendezvous algorithms in the Cooja simulator
- Compare the performance of the algorithms in Sky devices in terms of TTR

[1] E. O. Guerra, J. C. P. Garcia, V. Alfonso Reguera, T. M. Trang Nguyen and G. Pujolle, "A Novel Multi-Radio Rendezvous Scheme for Cognitive Radio Networks," *2019 12th IFIP Wireless and Mobile Networking Conference (WMNC)*, Paris, France, 2019, pp. 154-161, doi: 10.23919/WMNC.2019.8881570. (https://ieeexplore.ieee.org/abstract/document/8881570)

[2] L.A. DaSilva, I. Guerreiro, Sequence-based rendezvous for dynamic spectrum access, in: 2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, IEEE, 2008, pp. 1–7, http://dx.doi.org/10.1109/DYSPAN.2008.52.

[3] B.F. Lo, A survey of common control channel design in cognitive radio networks, Phys. Commun. 4 (1) (2011) 26–39, http://dx.doi.org/10.1016/j.phycom.2010.12.004.

[4] N.C. Theis, R.W. Thomas, L.A. Dasilva, S. Member, Rendezvous for cognitive radios, IEEE Trans. Mob. Comput. 10 (2) (2011) 216–227, http://dx.doi.org/10.1109/TMC.2010.60.

[5] A. Benslimane, A. Ali, A. Kobbane and T. Taleb, "A new opportunistic MAC layer protocol for cognitive IEEE 802.11-based wireless networks," *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, Tokyo, Japan, 2009, pp. 2181-2185, doi: 10.1109/PIMRC.2009.5449990.

Proposal 3
Title: Performance evaluation of Age of Information in Lora communication.

Summary of the proposal
Wireless networks have been widely deployed for many Internet-of-Things (IoT) applications, like smart cities and precision agriculture. Low Power Wide Area Networking (LPWAN) is an emerging IoT networking paradigm to meet three key requirements of IoT applications, i.e., low cost, large-scale deployment, and high energy efficiency. Among all available LPWAN technologies, LoRa networking has attracted much attention from both academia and industry, since it specifies an open standard and allows us to build autonomously.

Traditional metrics such as packet delay, jitter, and delivery times are not sufficient to determine the freshness of information once it reaches its destination [1]. The Age of Information (AoI) is defined as the time elapsed from the last observation (measurement) of certain information to its delivery to a given destination [2], [3]. It is a performance metric commonly used to measure the freshness of information experienced by a given user.

Related Work
LoRaWAN ensures data rates from 0.3 kbps up to 50 kbps, which are considered acceptable for transmitting real-time sensor data in the IoT, Machine-to-Machine (M2M), smart city, and industrial applications. However, the transmission of real-time image data, or anything that requires high bandwidth, may not be suitable on LoRa networks. This low data rate ensures the low power consumption of the edge node devices, therefore enabling the usage of the battery for a seamless deployment.

Plan

- To become familiar with LoRa technology
- To study the traffic patterns of IoT devices
- To become with Lora hardware and IoT platforms (TTN [4], Ubidots)
- Implement an architecture that allows the evaluation of the performance of a Lora-enabled IoT Network in terms of AoI

[1] J. C. Pérez García, A. Benslimane, and Z. Su, "Analysis on the AoI in Blockchain-based IoT Networks with Different Sensing Mechanisms," ICC 2022 - IEEE International Conference on Communications, Seoul, Korea, Republic of, 2022, pp. 4763-4768, doi: 10.1109/ICC45855.2022.9838842.

[2] S. Kaul, R. Yates and M. Gruteser, ”Real-time status: How often should one update?,” 2012 Proceedings IEEE INFOCOM, pp. 2731-2735, 2012.

[3] S. Lee, M. Kim, J. Lee, R. H. Hsu and T. Q. S. Quek, ”Is Blockchain Suitable for Data Freshness? An Age-of-Information Perspective,” IEEE Network, vol. 35, no. 2, pp. 96-103, March/April 2021.

[4] https://www.thethingsnetwork.org

Proposal 4

Title: Computation time and energy consumption of Cryptographic protocols in IoT devices.

Summary of the proposal

Internet of Things (IoT) is an emergent and evolving technology, that interconnects the cyber and physical worlds. IoT technology finds applications in a broad spectrum of areas such as homes, health, water and sanitation, transportation, and environmental monitoring. However, the endless opportunities and benefits of IoT come with many security challenges due to the reduced computation, communication, storage, and energy capabilities of IoT smart devices [1].

Power consumption and processing time are other factors that need to be considered in the tradeoff between the desired level of security and the resources in IoT nodes. Power consumption is especially important in battery-operated devices. In real-time applications, the processing time is critical and is defined as the interval between the initial request and the production of output.

Related Work

A heavyweight security solution can effectively solve the problems on the resource-rich device side, but might be infeasible for the resource-limited nodes to execute such solutions, especially in real-time systems. Based on this observation, it is very important to analyze the impact of cryptographic protocols on IoD devices, like sensors, Arduino-based and RaspberryPy devices.

Plan

- To become familiar with Cryptographic protocols in IoT networks and devices
- To become familiar with embedded devices coding (C/python)
- Implement different protocols and primitives
- Compare the performance of the algorithms in the different devices in terms of processing time and power consumption

[1] M. N. Khan, A. Rao and S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4132-4156, 15 March15, 2021, doi: 10.1109/JIOT.2020.3026493.

[2] A. Fotovvat, G. M. E. Rahman, S. S. Vedaei and K. A. Wahid, "Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8279-8290, 15 May15, 2021, doi: 10.1109/JIOT.2020.3044526.

[3] K. McKay, L. Bassham, M. Sonmez Turan, and N. Mouha, “Report on lightweight cryptography,” NIST, Gaithersburg, MD, USA, Rep. NISTIR 8114, 2017. Accessed: Jul. 3, 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8114/final

[4] K. Boakye-Boateng, E. Kuada, E. Antwi-Boasiako and E. Djaba, "Encryption Protocol for Resource-Constrained Devices in Fog-Based IoT Using One-Time Pads," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3925-3933, April 2019, doi: 10.1109/JIOT.2019.2893172.

Proposal 5
Title: Wi-Fi RSSI- based crowd counting.

Summary of the proposal

The ability to estimate the total number of people in an area can be useful for several applications for emerging technologies like 5G and 6G. Crowd counting could be supported by Internet of Signals technologies with huge beneficial for humans, for instance, Smart buildings can optimize energy consumption based on the number of people in the building [1], [2]. Retails can better plan their business by assessing which parts of the store get more visitors [3]. Smart cities can better plan the resources by estimating which areas of the city are more crowded [4].

In computer vision, for instance, photographic images of an area are used to identify the number of people present in the area. However, these methods 1) require a network of cameras to be installed in the area of interest and as such have a high deployment cost, 2) cannot work in the dark, 3) cannot work behind walls, and 4) pose privacy issues.

Related Work

Crowd counting based on wireless devices can be mainly classified into (i) device-based active and (ii) device-free passive methods. The device-based active methods rely on people to carry a communication device, which can limit their applicability. For this reason, there has recently been considerable interest in device-free methods, which do not require people to carry any device. Instead, device-free methods rely on the interaction of wireless signals with the people in the area of interest.

In this context, device-free counting can predict the number of people in a given area using the variance of the WiFi received signal strength indicator (RSSI).

Plan

- To become familiar with wireless channel characteristics, especially RSSI and propagation models.
- Study Artificial Intelligence Classifiers like Logistic Regression, KNeighborsClassifier, Decision Tree Classifier, and SVC.
- Create an experiment that records the RSSI of a wifi communication with a different number of people (up to 5 people) in the wifi channel.
- Use the collected data to train some classifiers to predict the number of people for a given RSSI.

[1] Y. Agarwal, B. Balaji, R. Gupta, J. Lyles, M. Wei, and T. Weng, “Occupancy-driven energy management for smart building automation,” in Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building. ACM, 2010, pp. 1–6.

[2] O. Ardakanian, A. Bhattacharya, and D. Culler, “Non-intrusive techniques for establishing occupancy related energy savings in commercial buildings,” in Proceedings of the 3rd ACM International Conference on Systems for Energy-Efficient Built Environments. ACM, 2016.

[3] O. Perdikaki, S. Kesavan, and J. M. Swaminathan, “Effect of traffic on sales and conversion rates of retail stores,” Manufacturing & Service Operations Management, vol. 14, no. 1, pp. 145–162, 2012.

[4] S. Depatla and Y. Mostofi, "Crowd Counting Through Walls Using WiFi," 2018 IEEE International Conference on Pervasive Computing and Communications (PerCom), Athens, Greece, 2018, pp. 1-10, doi: 10.1109/PERCOM.2018.8444589.

Proposal 6

Title: Discrete-event simulation for compartmental stochastic processes on graph.

Summary of the proposal

Discrete-event simulations [1] are common programs used to simulate large scale stochastic processes in order to evaluate their performances. The idea of such programs is based on events that occurs at random time, and then the dynamic evolution of complex systems can be studied. Many application domains are based on such approaches like performance evaluation of communication systems, virus propagation, road traffic management, etc.

We propose in this project to build from scratch a discrete-event simulator aiming to simulate compartmental stochastic processes. A well-known compartmental model that can be used as a benchmark is the Susceptible-Infected model [2], which is basically used to study epidemics. The simulator has to be reconfigurable such that variants of the SI model can be easily configured. We can cite for example SIR, SEIR and others specific compartmental stochastic models. All these models are based on Markov chain framework with particular transition rates. This is why simulation helps to understand both transient and stationary behavior of such complex system.

[1] Pierre-Jean Erard et Pontien Déguénon, Simulation par événements discrets, Lausanne/Paris, Presses polytechniques et universitaires romandes,

[2] Brauer F., « Compartmental models for epidemics», Centre for Disease Modelling, Preprint 2008-02, University of York. Consulté le 13 mars 2010.

Proposal 7
Title: Trust-based Certificate Management

Summary of the proposal

In the literature, several works rely on trust management to deal with untrusted nodes. Indeed, trust management provides continuous analysis of the behavior of nodes to predict their performance over time, which improves the revocation decision process and enhances the security of the networks. To make a revocation decision, trust-based revocation mechanisms use either non-voting strategy or voting strategy.

OpenSSL is a free and open-source cryptographic library that provides several command-line tools for handling digital certificates. Some of these tools can be used to act as a certificate authority.

Plan

The objectives of this project are:

- Implement a chain of certificate between a root and a client while creating intermediate pair
- Implement the certificate verification with two well-known methods:
- Certificate revocation lists
- Online certificate status protocol
- Implement a mechanism certificate based trust
- Design a BlockChain based trust certificate management

[1] S.-H. Ju and H.-S. Seo, “Certificate Management Scheme for IoT Services”, TEST management and engineering, vol. 83, pp. 4186-4194, 26 March 2020.
[2] I. Ud Din, M. Guizani, B. Kim, S. Hassan, and M. Khurram Khan, “Trust Management Techniques for the Internet of Things: A Survey”, IEEE Access, vol. 7, pp. 29763-29787, 2019.
[3] R. S. Krishnan, E. G. Julie, Y. H. Robinson, R. Kumar, P. H. Thong, and L. H. Son, “Enhanced certificate revocation scheme with justification facility in mobile ad-hoc networks”, Computers & Security, Vol. 97, pp. 101962, 2020.