Internship title: Self-healing Key Pre-distribution in IoT Networks

Location: ERIC or LIRIS Laboratory

Internship supervisors (Emails):

- Mohamed-Lamine Messai (mohamed-lamine.messai@univ-lyon2.fr)
- Hamida Seba (hamida.seba@univ-lyon1.fr)

Key words: Key management, Self-healing, IoT networks

Internship for a Master 2 student (or equivalent)

Duration: 5-6 months.

Desired starting date: February 2023

Context

Wireless Sensors Networks (WSNs) have gained a lot of interest over the last decade because of their use in several Internet of Things (IoT) applications such as building monitoring, health-care, smart cities, intelligent factories, ..., etc. To secure communications in these networks with cryptographic techniques, key management play an essential role [1]. Sensor nodes, that compose WSNs, have resource-limitation in term of energy, storage and computation capabilities. For these reasons, an asymmetric cryptosystem is not advisable for its resource-consuming. However, symmetric cryptosystems have a reasonable resource-consuming which make them well adapted for WSNs but requires a key management system to distribute, maintain, refresh and revoke pairwise keys between sensor nodes. In some IoT applications, sensor nodes are deployed in several epochs of the network lifetime to ensure the service continuity of the network [1, 2]. Proposed key management schemes based on a symmetric cryptosystem in IoT networks suffer from node compromising attacks.

When an attacker compromises a sensor node, all key material of this sensor node is disclosed which can affect communications within the network. To deal with this problem, several key management solutions are proposed [3, 4, 5, 6, 7]. These solutions address self-healing propriety. A key management scheme is self-healing when sensor nodes are able to recover lost session keys without the intermediary of a key distribution center. The meaning of self-healing differs when we have multiple deployments of sensor nodes. In an IoT network, the goal of self-healing is to diminish the impact of node compromising attacks. In other words, a key management scheme is qualified as self-healing if it assures that the security of an attacked network is improved over time. When an attacker captures nodes, the security of the network is affected. The self-healing feature ensures that the harm caused by the attacker disappears with time. Also, a self-healing scheme assures that post-deployed nodes are able to establish uncorrupted pairwise keys with previously deployed generations.

The main objectives of this internship are:

- Studying the state of the art of relevant self-healing key management approaches in IoT networks
- The implementation of a new self-healing key pre-distribution solution
- Performance evaluation of the proposed solution with existing solutions in the literature.

To apply: The candidate must have advanced skills (M2 level) in computer science (computer security skills are highly desirable). Please send your application with a CV, a cover letter, as well as your grades for the current academic year and last year to mohamed-lamine.messai@univ-lyon2.fr & hamida.seba@univ-lyon1.fr

References

[1] Messai, M. L., & Seba, H. (2016). A survey of key management schemes in multi-phase wireless sensor networks. Computer Networks, 105, 60-74.

[2] Rams, T., & Pacyna, P. (2012). A survey of group key distribution schemes with self-healing property. IEEE Communications Surveys & Tutorials, 15(2), 820-842.

[3] Guo, H., Zheng, Y., Li, X., Li, Z., & Xia, C. (2018). Self-healing group key distribution protocol in wireless sensor networks for secure IoT communications. Future Generation Computer Systems, 89, 713-721.

[4] Shen, J., Chang, S., Liu, Q., Shen, J., & Ren, Y. (2018). Implicit authentication protocol and self-healing key management for WBANs. Multimedia Tools and Applications, 77(9), 11381-11401.

[5] Han, S., Gu, M., Yang, B., Lin, J., Hong, H., & Kong, M. (2019). A secure trust-based key distribution with self-healing for internet of things. IEEE Access, 7, 114060-114076.

[6] Vadlamudi, C. V., & Vadlamudi, S. P. D. (2019). A novel self-healing key distribution scheme based on vector space access structure and MDS codes. International Journal of Communication Systems, 32(16), e4088.

[7] Patel, N., & Kumar, V. (2022). An efficient key distribution Scheme for WSN with Mutual Healing Capability. Multimedia Tools and Applications, 81(25), 36735-36749.