Towards adaptive security for mobile IoT

Asma Arab, Ghada Jaber, Abdelmadjid Bouabdallah

Towards adaptive security for mobile IoT

Asma ARAB Ghada JABER Abdelmadjid BOUABDALLAH

***Abstract*—The Internet of Things (IoT) is a groundbreaking concept that aims to establish seamless connectivity among a wide array of devices. The IoT devices has revolutionized various industries. However, the deployment of IoT devices in vulnerable environments has led to numerous security challenges, including but not limited to data privacy, device authentication, secure data transmission, and protection against malicious intrusions. Additionally, in various application domains nodes are not static, they can move across different networks and zone. This mobility introduces further security concerns, as IoT nodes encounter different threats and risk levels through the zones. Furthermore, security services must be capable of operating transparently to facilitate the continuous functioning of nodes during movement. This paper addresses the challenges and requirements that must be considered when designing solutions for IoT to secure communications while accommodating mobility. Additionally, the paper delves into adaptive security as research direction we identified to ensure security while supporting mobility for IoT.**

***Index Terms*—Iot , security , mobility, energy saving.**

I. Introduction

IoT has ushered in a new era of connectivity, enabling an unprecedented level of interaction and integration between physical and digital realms. The widespread deployment of IoT devices in various domains, ranging from healthcare, supply chain and transportation to smart homes, smart vehicles and industrial systems has brought significant concerns regarding the security of communication among these interconnected devices [1].

Indeed, security in IoT systems has become a major constraint due to the sensitive nature of the applications in which they are deployed. The manipulation and transmission of data in IoT applications must be safeguarded to ensure confidentiality, privacy, and integrity. This involves protecting sensitive data, mitigating threats and vulnerabilities, and ensuring the privacy and security of the transmitted information. Moreover, the resource limitations of IoT devices, including restricted memory and limited energy reserves, pose significant challenges in implementing robust security measures [2].

The mobility of IoT devices introduces additional security challenges, as these devices seamlessly transition between different locations and networks. Addressing the security concerns associated with mobile IoT devices is crucial, as it involves tracking devices in terms of their old and new locations, reducing handover delay, simplifying mobility management, and handling a reduced number of packets. Furthermore, the IoT devices may encounter different types of threats, attacks and vulnerabilities, which requires different security mechanisms of mobile IoT environments. Therefore, there's a need for adaptive and resilient security measures to ensure the continuous protection of data and devices.

In light of these challenges, extensive research has been conducted to investigate various security threats and vulnerabilities in IoT systems. The development of innovative security solutions that consider the mobility of IoT devices to ensure service continuity has become a critical area of focus. In this article, we provide an examination of the security challenges and requirements presented by mobile IoT. Additionally, we present adaptive security which we we consider as an interesting research perspective for further investigation in this domain.

The remainder of the paper is structured as follows: Section II provides an overview of mobility in IoT. In Section III, we detail the challenges and requirements in terms of security for mobile IoT. Section IV introduce adaptive security and its benefit for IoT, the research works conducted in this area, and a research contribution for adaptive security solution for IoT. The paper is concluded in Section V.

II. Mobility in IoT

The concept of mobility in IoT encompasses the dynamic process of nodes changing their location over both space and time. As a fundamental requirement for IoT systems, mobility has given rise to the emergence of the Internet of Mobile Things (IoMT), which has found diverse potential applications, as illustrated in Figure 1, in areas such as pallet tracking for logistics, healthcare, wildlife tracking and monitoring, agriculture, and smart farming, as well as smart vehicles.

In the context of mobility, ensuring session continuity is a crucial requirement, particularly in scenarios where the mobility solution must guarantee uninterrupted communication between the Mobile Node (MN) and the Correspondent Node (CN). Additionally, minimizing handoff delays, especially for MNs with high mobility rates, is essential. Furthermore, in cases where the end device changes its gateway, connection continuity becomes paramount to enable seamless data transmission to and from the CN without disruptions. Regardless of the type of mobility, the mobility management process must consider the resource constraints inherent in IoT devices [3].

When considering the security of communications between mobile IoT devices, it becomes imperative to identify the additional risks and vulnerabilities that these devices face. The dynamic nature of mobile IoT environments introduces new security challenges, including the need to address the resource limitations of IoT devices, minimize handoff delays, ensure session and connection continuity, and manage the mobility process effectively.

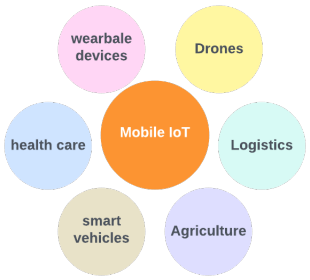

Fig. 1. Mobile IoT application fields

III. Challenges & Requirements for Secure Mobile IoT

The mobility of IoT nodes introduces a level of intricacy to the security environment. Consequently, in order to effectively tackle the security apprehensions within mobile IoT, it is crucial to identify the security needs that are accentuated by mobility.

A. Security Challenges for Mobile IoT

The mobility of devices in the context of IoT introduces unique security challenges compared to traditional IoT scenarios. These challenges have been extensively discussed in the literature [4]–[6]. The challenges include:

- **Insecure Protocols:** The protocols used for data sharing and transmission in mobile IoT are susceptible to attacks that can compromise authorization and access control. The extensive range of user roles and the lack of predetermined security measures within the protocol infrastructure contribute to vulnerabilities in mobile IoT.
- **Insecure Infrastructure:** The infrastructure supporting data transmission for mobile IoT devices is a significant contributor to vulnerabilities. The architectural configuration plays a pivotal role in network accessibility and determining its security priorities.
- **Inefficient Transport and Data Encryption:** Unencrypted traffic is often broadcasted to prevent performance degradation, leading to vulnerabilities associated with access control such as eavesdropping, as the majority of messages remain unencrypted.
- **Resource Constraint:** The resource constraint in mobile IoT inhibits the implementation of robust security measures without negatively impacting the performance of the devices.
- **Cross-Domain Identification and Trust:** When a mobile device moves from one domain to another, it raises the question of how the new domain can authenticate the device and determine the appropriate permissions to grant it [7].

B. Security Requirements for Mobile IoT

In the context of mobile IoT, several security requirements must be met to ensure the integrity and confidentiality of data and the overall security of the system [5], [8]. These requirements include:

- **Light-weight Solutions:** Security solutions for mobile IoT must consider the resource limitations in IoT devices, aiming to strike a balance between efficient methods and optimizing energy consumption to ensure secure yet energy-efficient communication in IoT systems.
- **Decentralized Management:** Centralized approaches for the management of mobile IoT security are often impractical. Therefore, security mechanisms should be positioned as close to where they are needed while accommodating resource-constrained devices, typically involving decentralized management for clustered system segments.
- **Scalability:** Security measures in mobile IoT systems must be scalable to effectively handle the potentially vast IoT landscape, accommodating new devices and users joining or leaving the system.
- **Heterogeneity:** Security solutions must accommodate the diverse aspects of mobile IoT, including varying devices and technologies, without being tied to a particular technology.
- **Robustness and Reliability:** Security solutions must exhibit robustness and reliability, capable of handling device faults and expanding attack vectors. Self-repair functionality is necessary to detect and rectify faults, and security measures should promptly respond to threats in real-time.
- **Device Policy Compliance:** It is essential for security solutions to comply with device-specific policies and refrain from breaching security measures, as such breaches can potentially enable unauthorized applications to gain control over the device, posing a threat to the entire network.

In summary, the challenges and security requirements of mobile IoT highlight the need for robust and adaptable security measures to counter vulnerabilities and ensure secure communications in mobile IoT systems. In a decentralized IoT environment where the devices are mobile,the risk levels vary across geographical zones. Therefore, the static security solutions that takes into consideration the presented challenges and requirements becomes inefficient. Indeed, the use of lightweight solutions may expose legitimate IoT nodes to vulnerabilities in high-risk areas, while the deployment of complex solutions could result in excessive energy consumption, leading to energy depletion in IoT nodes even in low-security requirement scenarios. To tackle this challenge, adaptive security solutions have emerged as a promising approach. In the following, we will present adaptive security and the research efforts conducted in this field

IV. Adaptive security : a future approach for securing mobile IoT

A. adaptive security for IoT

Adaptive security in the context of IoT refers to a security approach that can dynamically adjust and modify security

measures in response to changing conditions and threats within a system. One of the key benefits of adaptive security in IoT is its ability to provide real-time adaptation features for IoT device security, such as subsystem isolation and lightweight authentication protocols [9]. This dynamic adjustment of security measures enables IoT systems to respond to emerging threats and vulnerabilities effectively. Additionally, adaptive security can facilitate the implementation of communication aware adaptive key management, ensuring end-to-end security for active IoT devices [10]. This is particularly important in IoT networks where secure communication is essential for maintaining the integrity and confidentiality of data transmitted between devices. Moreover, adaptive security can contribute to the trustworthiness of IoT systems by enabling continuous deployment of trustworthy IoT systems that can adapt to evolving conditions and threats while maintaining their reliability and security [11]. This is crucial for ensuring the overall integrity and resilience of IoT deployments [12].

B. existing adaptive security solutions for IoT

Numerous research works have been conducted to advance adaptive security solutions tailored for IoT applications. For instance, [13] focus on developing adaptive security solutions for smart IoT applications in eHealth, introducing a risk-based adaptive security approach that dynamically learns and adjusts to evolving environments, preempting unforeseen threats. [14] propose an adaptive risk-based access control model designed for IoT applications, which dynamically modifies user permissions by incorporating real-time risk assessments and monitoring user activities throughout access sessions, utilizing smart contracts to deliver adaptive features. Additionally, [15] introduce the Adaptive Lightweight Physical Layer Authentication (ALPLA) scheme, employing a one-class classifier support vector machine (OCC-SVM) specifically crafted for 5G mobile networks in the realm of IoT, with a distinct focus on the physical layer. [16] offer a comprehensive exploration of adaptive authentication methods harnessing machine learning, emphasizing that the discussed methods may not be directly applicable to the distinctive context of IoT. Furthermore, [17] present a thorough survey of self-adaptive security mechanisms tailored for IoT-based multimedia services, investigating several self-adaptive security approaches, encompassing context-based security, architecture-based self-protection, and self-adaptive authentication.

Moreover, authors in [18] advocate for the integration of multiple encryption modes characterized by diverse power consumption and security levels to tackle the challenges of security in low-power IoT devices, achieved through the Dynamic Partial Reconfiguration (DPR) to dynamically configure the hardware security module, aligning with the available power budget. Authors in [19] detail an adaptive security specification method for 6G IoT networks, employing artificial intelligence to navigate the balance between security and energy consumption, with a specific focus on dynamic security configuration to augment energy efficiency. The paper [20] present an adaptive security framework for 5G-based IoT systems, dynamically adapting security levels in response to changing contextual conditions to mitigate energy consumption. [21] delve into the critical trade-off between security and energy considerations in edge-assisted IoT, suggesting tailoring the complexity of security schemes to specific security levels as a strategy to conserve energy consumption.

C. securing mobile IoT through adaptive security

The concept of adaptive security is particularly pertinent in the realm of mobile IoT. Firstly, the decentralized nature of IoT environments, in conjunction with varying risk levels across geographical zones, presents challenges for conventional fixed and static security services. The mobility of IoT devices further exacerbates the inadequacy of standard security measures, thereby necessitating the development of novel, intelligent, and adaptable security solutions. Indeed, the widespread distribution, openness, and substantial processing power of IoT objects render them susceptible to attacks, thereby underscoring the imperative for adaptive security measures. Moreover, the presence of resource constraints, heterogeneity, the generation of massive real-time data by IoT devices, and the dynamic behavior of networks collectively underscore the indispensability of adaptive security solutions [12].

Therefore, adaptive security presents a promising research direction for mobile IoT, as it enables the deployment of a diverse array of defense mechanisms tailored to the specific contextual environment. This adaptability encompasses addressing various types of attacks, threats, risk levels, and vulnerabilities encountered by mobile IoT devices as they traverse different zones and networks. The dynamic nature of mobile IoT environments requires the adaptation of security measures to ensure the continuous protection of data and devices. Furthermore, the implementation of adaptive security can play a pivotal role in energy conservation by facilitating the use of lightweight security mechanisms in low-risk environments, thereby mitigating the energy exhaustion associated with complex defense mechanisms. Our ongoing research focuses on the development of an authentication method for mobile IoT, which is underpinned by an architecture integrating Software-Defined Networking (SDN) controllers and fog nodes. This architecture aims to ensure seamless management of handovers and session continuity for mobile IoT devices. Additionally, it aims to minimize energy consumption while ensuring secure communication during the movement of IoT devices.

V. Conclusion

IoT devices has revolutionized various industries, introducing a myriad of security challenges, particularly in mobile IoT environments. The dynamic nature of IoT devices, coupled with their mobility across different networks and zones, presents unique security concerns, requiring adaptive security measures. This paper has elucidated the security challenges and requirements inherent in mobile IoT, emphasizing the need for robust security solutions that can dynamically adapt to varying risk levels and environmental contexts.

The concept of adaptive security has emerged as a promising research direction for securing mobile IoT devices. Adaptive security entails the dynamic adjustment of security measures in response to evolving conditions and threats within IoT systems. Moreover, adaptive security solutions have the potential to address the energy conservation aspect by enabling the deployment of lightweight mechanisms in low-risk environments, thereby mitigating excessive energy consumption. In conclusion, the adoption of adaptive security as a research direction for mobile IoT is imperative in addressing the dynamic security challenges posed by the mobility of IoT devices.

REFERENCES

[1] T. Domínguez-Bolaño, O. Campos, V. Barral, C. J. Escudero, and J. A. García-Naya, "An overview of iot architectures, technologies, and existing open-source projects," *Internet of Things*, p. 100626, 2022.

[2] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "Twenty security considerations for cloud-supported internet of things," *IEEE Internet of things Journal*, vol. 3, no. 3, pp. 269–284, 2015.

[3] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue, and J.-C. Prévotet, "Internet of mobile things: Overview of lorawan, dash7, and nb-iot in lpwans standards and supported mobility," *IEEE Communications Surveys & Tutorials*, vol. 21, DOI 10.1109/COMST.2018.2877382, no. 2, 2019.

[4] K. Nahrstedt, H. Li, P. Nguyen, S. Chang, and L. Vu, "Internet of mobile things: Mobility-driven challenges, designs and implementations," in *2016 IEEE First international conference on internet-of-things design and implementation (ioTDI)*, pp. 25–36. IEEE, 2016.

[5] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-internet of things (m-iot): A survey," *IEEE access*, vol. 8, pp. 167 123–167 163, 2020.

[6] I. Mohiuddin and A. Almogren, "Security challenges and strategies for the iot in cloud computing," in *2020 11th international conference on information and communication systems (ICICS)*, pp. 367–372. IEEE, 2020.

[7] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet of things Journal*, vol. 6, no. 2, pp. 1606–1616, 2018.

[8] S. Pal, M. Hitchens, T. Rabehaja, and S. Mukhopadhyay, "Security requirements for the internet of things: A systematic approach," *Sensors*, vol. 20, no. 20, p. 5897, 2020.

[9] S. Tedeschi, C. Emmanouilidis, J. Mehnen, and R. Roy, "A design approach to iot endpoint security for production machinery monitoring," *Sensors*, vol. 19, no. 10, p. 2355, 2019.

[10] C. Tamizhselvan, "A novel communication-aware adaptive key management approach for ensuring security in iot networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 11, p. e4605, 2022.

[11] N. Ferry, P. H. Nguyen, H. Song, E. Rios, E. Iturbe, S. Martinez, A. Rego *et al.*, "Continuous deployment of trustworthy smart iot systems." *The Journal of Object Technology*, 2020.

[12] W. Aman and E. Snekkenes, "Managing security trade-offs in the internet of things using adaptive security," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 362–368. IEEE, 2015.

[13] H. Abie and I. Balasingham, "Risk-based adaptive security for smart iot in ehealth," in *Proceedings of the 7th International Conference on Body Area Networks*, pp. 269–275, 2012.

[14] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Developing an adaptive risk-based access control model for the internet of things," in *2017 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and ieee smart data (SmartData)*, pp. 655–661. IEEE, 2017.

[15] M. Abdrabou and T. A. Gulliver, "Adaptive physical layer authentication using machine learning with antenna diversity," *IEEE Transactions on Communications*, vol. 70, no. 10, pp. 6604–6614, 2022.

[16] R. Pramila, M. Misbahuddin, and S. Shukla, "A survey on adaptive authentication using machine learning techniques," in *Data Science and Security: Proceedings of IDSCS 2022*, pp. 317–335. Springer, 2022.

[17] I. Singh and S.-W. Lee, "Self-adaptive and secure mechanism for iot based multimedia services: a survey," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 26 685–26 720, 2022.

[18] N. Samir, Y. Gamal, A. N. El-Zeiny, O. Mahmoud, A. Shawky, A. Saeed, and H. Mostafa, "Energy-adaptive lightweight hardware security module using partial dynamic reconfiguration for energy limited internet of things applications," in *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–4. IEEE, 2019.

[19] B. Mao, Y. Kawamoto, and N. Kato, "Ai-based joint optimization of qos and security for 6g energy harvesting internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7032–7042, 2020.

[20] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy efficiency in security of 5g-based iot: An end-to-end adaptive approach," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6589–6602, 2020.

[21] S. Shen, K. Zhang, Y. Zhou, and S. Ci, "Security in edge-assisted internet of things: challenges and solutions," *Science China Information Sciences*, vol. 63, pp. 1–14, 2020.