






Deception mechanisms for cyber-security enhancement in the Internet of Things


1st Ignacio Lacalle 
Communications Department
Universitat Politècnica de València
Valencia, Spain
iglaub@upv.es

2nd Salvador Cuñat 
Communications Department
Universitat Politècnica de València
Valencia, Spain
salcuane@upv.es

3rd Aristeidis Farao 
Department of Digital Systems
University of Piraeus
Piraeus, Greece
arisfarao@unipi.gr

4th Christos Xenakis 
Department of Digital Systems
University of Piraeus
Piraeus, Greece
xenakis@unipi.gr

5th Dionysis Xenakis 
FOGUS INNOVATION SERVICES
University of Athens
Athens, Greece
nio@di.uoa.gr

6th Carlos E. Palau 
Communications Department
Universitat Politècnica de València
Valencia, Spain
cpalau@com.upv.es

Abstract—This paper aims at providing a structured approach to the usage of deception mechanisms in Internet of Things deployments. Honeypots, honeynets and moving targeted defense elements are increasingly frequent, and their potential to overcome specific cyber-security issues in IoT is paramount. In this work, authors explore and expose actual implementations, reinforcing those that employ open source technologies, highlighting a remarkable digital twin approach. Arguably, the usage of such mechanisms will lead to refined implementations in the upcoming future.

Index Terms—deception mechanisms, IoT, honeypot, honeynet, cyber-security

I. INTRODUCTION

Cyber-security is one of the top concerns in IT nowadays, and, rightfully so, it will continue being for the foreseeable future. The eventuality of accessing to relevant private data, asking for ransoms after encrypting valuable information, performing eavesdropping, and other casuistry produce hassle to companies worldwide.

Cyber-attacks are a threat to all IT systems that interconnect among each other and/or to the internet. This includes deployments that highly rely on a distributed network of elements that monitor and actuate over physical elements, commonly known as Internet of Things (IoT). These environments, apart from facing the classic attack vectors (data tampering, injection, man-in-the-middle, DoS...), imbue certain intrinsic vulnerabilities that can be exploited by hackers.

The literature, and the implementation cases, have advanced in studying such characteristics, and in proposing solutions and counter-measures to still protect such environments. Traditional approaches encompass encryption, authentication, firewalls and Intrusion Detection Systems (IDS). Also, a continue observation of network traffic, together with frequent firmware

updates to patch any known vulnerabilities, are usual strategies in such scenarios.

However, still these layouts are highly exposed to a dynamic number of attack types. This is why, as also observed, there is the recent trend to include a specific kind of -advanced- cybersecurity instruments that could enhance the protection of such deployments: deception mechanisms. Decoy, disguise techniques and other sophisticated methods are grouped into this increasingly-used field of work, that might bring extraordinary benefits to IoT environments.

This paper attempts to understand the current impact of deception mechanisms in the protection of IoT deployments. While in the literature, many references can be found that explore the concept and implementation of deception techniques, there is not a narrowed analysis of their usage and benefits targeting only Internet of Things. Although several works have suggested their usage in IoT (see Section III), this article aims at going beyond such occurrences, including specific open source technologies that implement them, paving the way for the future specialisation of such applications. In order to do so, authors have performed purposive sampling review focused only in relevant, recent publications and implementation cases, aiming at being an updated reference.

The article is structured in five sections. Section I introduces the topic, signalling the direction of the attempted review. The content departs, in Section II, from an analysis of the special characteristics of IoT deployments that differentiate them from usual cyber-security scenarios. The research deepens the scope in Section III, where deception mechanisms are presented. First, defining and categorising them, and, later, contextualising their impact in IoT. Subsequently, a study is carried out in Section IV exposing actual implementations of such methods in real cases. Finally, Section V reflects on the usefulness of deception mechanisms to cover the IoT casuistry, and outlines potential future lines of research and development.

This work acknowledges the project AIAS, that has received funding from the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101131292

II. SPECIFIC CYBER-SECURITY CHALLENGES IN IOT

It is well known that successful attacks on IoT systems can result in significant costs for companies and people alike [1]. Operational processes could be fed from IoT data, whose tampering could lead to insurmountable economic losses. On the other hand, as IoT deployments may handle vast amounts of sensitive data generated by devices (e.g., in health-related wearable), this could have direct impact on persons. All of the previous can also affect (undermine) public trust in IoT technologies [2].

The distributed nature of IoT elements, as well as their characteristics (size, isolation) and a direct connection to physical monitoring/actuation, has led those to deal with huge amounts of data, thus increased exposure likelihood and direct cyber-threats. According to [3], the most relevant threats are software piracy and malware attacks. And, based on a thorough analysis, it was concluded that the most frequent attacks that IoT is vulnerable to are privacy issues and cybercrimes.

From another angle, the report [4] highlights the importance of insecure IoT endpoints, that are leveraged by attackers to infiltrate in the networks, ushering ransomware and malware assaults. Here, notably the generation of "botnets" (a net of synchronised, distributed elements with a goal) for Distributed Denial of Service (DDoS) represent a sophisticated threat vector [2]. Besides, the report indicates that routers and other entry points (e.g., industrial APs) are, generally, not enough protected, outlining a compelling call for action on direct practices [5].

The content presented in this section does not pretend to override or surpass previous, solid works performed in rigorous studies, such as in [6] or [7]. It rather aims at reflecting on the characteristics of the IoT deployments that make those cybersecurity attacks so relevant (thus, open to be protected by deception mechanisms). Therefore, to respond to the question of why the previous statements (such as the most frequent attacks) prevail in the sector.

To start answering such question, it is important to highlight that IoT devices require additional physical security measures, not present in other IT systems. A (potentially high) number of devices can be geographically dispersed, becoming vulnerable to physical tampering or hijacking, allowing unauthorised access. [2].

Beyond the additional physical protection, aspects that stand out in IoT deployments have been identified as follows:

- Although it has been with us around 15 years now, widely adoption of IoT is relatively new. This means that there is still a huge spectrum of cyber-threat options that are not yet well documented.
- Related to the previous, IoT is, up to now, a low standardised field, that characterises for its heterogeneity in platforms, tools, services, etc., with scarce programming and debugging guidelines, leading to potential attack vectors [8].
- IoT devices are, generally, quite constrained in resources. Active computing elements (IoT, edge, fog) might entail

limited capacity, which leads to two major concerns for cyber-security:

- Incapacity to undertake complex encryption mechanisms, or to engage with recommended authentication and authorisation practices. Thus, eavesdropping becomes feasible in many occasions [9].
- Network protocols, which might be battery-consumption intensive, are often selected based on energy-efficient parameters rather than on cyber-security prioritisation. In this regards, certain communication alternatives are not very well covered by usual threats knowledge [10].
- Retrofitting security alignment might be require. It is usual for IoT elements to interact with other, legacy, systems, that might entail encryption or communication schemas which integration might generate vulnerabilities [2].
- There is still a lack of culture, user awareness of protection and the global understanding of strategics and tactics for IoT deployments security [11]
- Due to the potential massive number of devices, and the (often) required device-to-device (D2d) interaction, a few elements emerge, enlarging the attack vector: (i) Life cycle transitions, oir DevOps (maintenance and scalability of code and infrastructure), (ii) increment of "the attack surface" due to many likely failure points. [3]
- Access to IoT devices sometimes require to rely on public networks, and are tied to mobility requirements, becoming more complex to protect them behind firewalls.
- Finally specific sectors have specific concerns, as for instance rural challenges in Smart Cities, as per [7].

As discussed, all the previous circumstances lead IoT deployments to have a huge attack surface. Since threats are polymorphic, different techniques, encompassing network, application and device-level must be applied to counteract [12].

Usual cyber-protection measures are equally applied, but works in the literature highlight specific observations that serve for understanding the uniqueness of IoT environment [13]:

- Instead of asymmetric ciphering schemas, symmetric key encryption should be tackled, putting special emphasis on the key construction (to avoid brute force attacks).
- Role-Based Access Control (RBAC) and other highly restrictive access policies for either accessing the devices or data are applied.
- Pentesting and fuzz testing in the code (especially in devices and edge elements) is a trend in complex systems [14].
- Cost reduction is paramount, as both hardware and firmware security on devices are expensive for companies [15].

Looking at the horizon, IoT deployments are prone to adapt to new technologies, which opens an extraordinary research field ahead. Emerging technologies such as blockchain, edge computing, and advanced global artificial intelligence (to en-

hance resiliency in a proactive manner [7]) present promising opportunities to enhance IoT security. Also, advanced mobile communications, with the advent of 6G networks, and the combination of the so-called IoT-Edge-Cloud Continuum [16] is the perfect example of it [17]. New cybersecurity and trust techniques are explored, such as 6G-enabled IoT-AI based digital twins [18].

III. OVERVIEW OF CYBER-DECEPTION MECHANISMS AND THEIR APPLICABILITY IN IoT

Cyber deception is a strategy in cybersecurity that involves creating a deceptive element or a network of them to act as decoys and divert potential attackers, as well as learn what attackers do once they think they have access to a system, to profile them or to better prepare in the future [19]. When attackers interact with the deceptions they not only reveal their presence but also their tactics, which allow to detect and analyse the threats before responding to them. Additionally, by deploying these deceptive artefacts across a network, cyber-deception aims to confuse attackers and delay their progress. Cyber-deception is used alongside other security measures to enhance security in a network [20].

As emphasised in Section II, modern IoT network often include a number of smart and potentially vulnerable elements that are Internet-connected such as smart household devices, all kinds of sensors for industrial environments, etc. These IoT devices often run critical operations such as data collection and real-time monitoring without much in the way of cyber security [21], which makes them attractive targets to malicious attackers [22].

This section will analyse the different kinds of deception mechanisms that are used to protect against malicious attacks, divided in two subsections, Section III-A will cover honeypots, how they are used and how they combine into honeynets and Section III-B will cover adaptive deception mechanisms in IoT networks.

A. Honeypots and Honeynets

Honeypot is a term used to reference a security resource whose value lies in being probed, attacked or compromised [23]. Honeypots are meant to be as flexible as possible, they are used to detect and deter attacks, to capture and analyse automated attacks or to act as early warning beacons. Honeypots are categorised into three broad classifications [24] as can be seen in Fig. 1:

- Research honeypots: Used to collect detailed information about attacks, focusing not only on how threats behave within the network but also on their operations in the wider context. This information helps design stronger defence systems, ensuring that sensitive systems have up-to-date security measures to defend against the attacks attracted by the honeypot.
- Production honeypots: Production honeypots are designed to detect compromises within the internal network and

deceive malicious actors. They are placed alongside genuine production servers and run similar services to blend in seamlessly.

- Honeytokens: Decoy elements like fake credentials, files, or database entries that, when accessed, trigger alerts and reveal unauthorised access into a network.

Honeypots are also divided by the amount of interaction they receive [25]:

- High-interaction Honeypot: fully operational, designed to engage attackers for extended periods, maximising the time they spend within the honeypot. It often contains data designed to appear confidential and includes "sensitive" user information
- Mid-interaction Honeypot: imitate application layer elements without having an actual operative system. Meant to confuse an attacker and stall them so the organisation has more time to react to the attack.
- Low-interaction Honeypot: meant to gather rudimentary information regarding the kind of threat and where it came from. Not meant to hold the attacker attention.

Additionally, when multiple honeypots and deception mechanisms are combined across multiple networks a Honeynet is created as seen in 1. By incorporating various types of honeypots, a honeynet can study multiple attack methods, such as distributed denial-of-service (DDoS) attacks, content delivery network (CDN) attacks, and ransomware attacks. While a honeynet is used for analysing different attack types, it contains all inbound and outbound traffic to safeguard the rest of the organisation's systems [26].

The most renowned entity that has helped shape modern Honeypots and their integration into Honeynets is the Honeynet Project [27]. The Honeynet Project is an international non-profit security research organisation that started learning attackers behavioural patterns in order to improve cyber security tools. The Honeynet Project extensively used Honeypots and Honeynets to achieve this.

B. Deception in IoT Contexts

Resource constrained Internet-of-Things devices are likely to be quickly compromised by attackers of given the chance, because strong security protections may not be suitable to be deployed [28]. Deceptive IoT endpoints can be used as honeypots to attract, confuse and delay the attacker and prevent them from attacking actually relevant elements. Additionally, fake information can be distributed by either the honeypots or the actual IoT elements to add another layer of deception into the network.

Low and high-interaction honeypots can be used in conjunction to simulate an IoT network, with the low-interaction honeypots acting as basic emulations of IoT devices that provide limited interaction capabilities and high-interaction honeypots that emulate APIs and servers. A combination of multiple of these kinds of IoT honeypots can be used to create a layered honeynet, with multiple layers of honeypots with varying levels of interaction. This, combined with fictitious

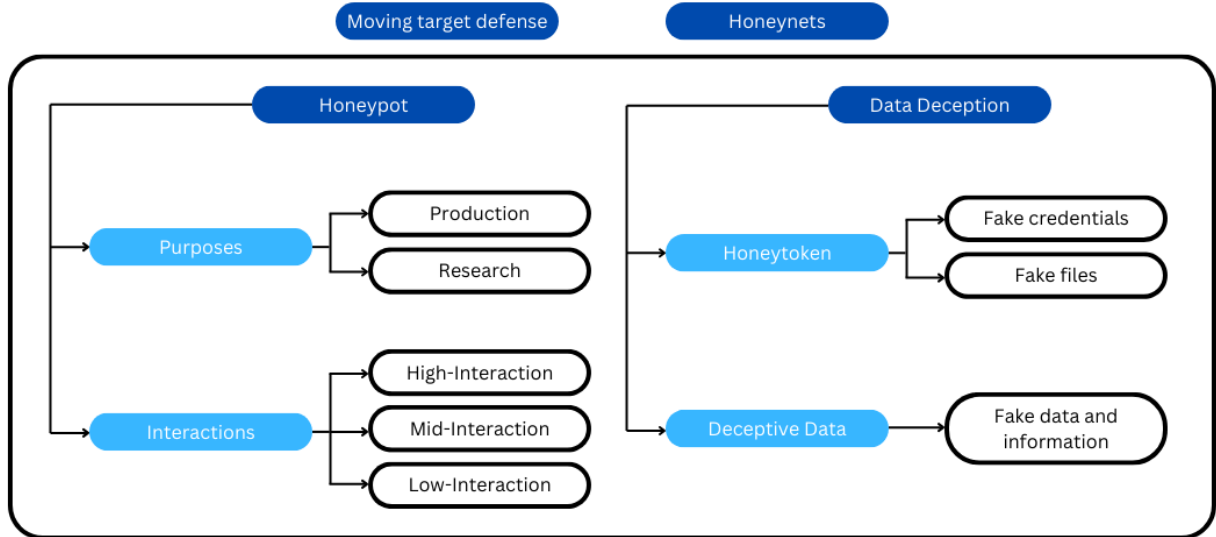


Fig. 1. Taxonomy of deception mechanisms

data streams used to generate false data as real as possible is an effective way of investigating attacker behaviour [29].

IoT networks also benefit greatly from Moving Target Defense paradigms. Moving Target Defense (MTD), also known as Adaptive Deception, addresses the vulnerabilities of static systems towards cyber-attacks since given enough time, attackers will identify vulnerabilities and exploits in a static system. MTD's purpose is to make systems dynamic, restricting attackers by limiting the time available to exploit those mentioned vulnerabilities. In an MTD system, attackers have a limited window to find and exploit vulnerabilities before the system changes. A vulnerability identified but not yet exploited might not exist in the system's next state. Even if a vulnerability is exploited, the system's future state may invalidate the exploit [30]. A possible solution is to expand a Honeynet into an MTD, achieving exponentially better results.

An example of MTD for IoT would be a strategy that constantly changes the IP addresses of network interfaces of connected IoT devices [31], which theoretically would improve the cyber security of the network but would also increase the network load of the system. Another alternative would be a strategy that randomises the IoT network's topology by shuffling the configuration of a network composed of decoy and real nodes [28], this unique solution would shuffle the elements of the IoT network confusing the attackers and luring them away from the network due to the complexity of the approach.

IV. RELEVANT CASE STUDIES AND TECHNOLOGY EXAMPLES

Several studies, since some years ago [32], have proposed the usage of deception mechanisms such as honeypots, honeynets or MTDs in IoT deployments, either being these simpler or more complex. This section aims at discussing significant implementations available in the literature, and proposes the

analysis of various open source tools and libraries that might be employed by the IoT community to explore the topic from a pragmatism approach. Lastly, a more holistic solution is presented, coming from the Horizon Europe project AIAS, that embodies various mechanisms in a complex Deception Layer within an AI-empowered architecture.

A. Significant Implementations in the Literature

Drawing from the execution of various, benchmarked, experiments, [33] employ raw logs of IoT devices as honeypots to analyse anomalous behaviours and detect potential attacks using various machine learning algorithms. As output, suggests to create a layer of confusion for attackers as countermeasures if attacks are detected. Usage of honeypots in IoT can also be seen in [34], where attack graphs are created, and an algorithm is created to allocate honeypots over. Close to the concept of adaptiveness of MTDs, a strategic game feeds the algorithm that is also based on data captured from the (simulated) network, applying Nash equilibrium theories. The study [35] works over the previous, using honeypots but introducing the trade-off among diversity in OSs. Here, the allocation considers as well the resources available and the OS used by each computing element, but stops at the theoretical network level.

The work [36] provides a solid analysis of simulation cases where deception mechanisms were used and analysed. Also, there, authors propose their own experimentation, following the MTD approach over the assumption of static network configurations. There, on top of an IoT network with real and decoy devices and servers, the work proposes to use Software Defined Networking (SDN) to maintain dynamicity in IoT traffic flows. There, decoy nodes are implemented as a deception technique and operating system diversity as a moving target defence approach for preventing the intrusion in the system. Previously, the usage of deception mechanisms

over SDN-enabled networks had already been explored in (also) simulation scenarios by [37]. However, then, the goal was to propose distributed honeypots (honeynets) to effectively mitigate Distributed DoS (DDoS) attacks.

More recently, an earlier job (2024) also based on game-theoretical investigations, [38] uses multi-agent reinforcement learning to study the problem of optimal deception asset deployment in IoT cybersecurity.

B. Discovered Tools and Libraries

Notwithstanding, apart from the advanced literature implementations (that mostly apply theory over simulated scenarios), the state of the art is complemented with actionable software to employ such techniques in real life.

Starting from 9 years ago, honeypots have been the most popular options for replicating open source software. *Honeything*¹ provided a honeypot for TR-069 IoT devices, including a web management interface, being useful for deployments including such devices. Later, *Kako*² appeared. It enlarged the number and type of IoT device vulnerabilities that it could detect. After implementation close to a real IoT device, it captures telnet, HTTP or HTTPS traffic and provides as an output a file (AWS SNS or JSON) with the identified attacks.

On 2019, *Honware* appeared for identifying exploits targeting Customer Premise Equipment (CPE) and Internet of Things (IoT) devices, via a high-interaction honeypot that was tested under the simulation of many cyber-attacks, all encapsulated on a custom Linux-kernel image [39]. By the same time, *HoneyIo4* also proposed to the open community a low-interaction honeypot utilising four Python scripts to simulate the expected Nmap DB scan responses for several IoT devices [40].

More recently, on 2021, a relevant open source tool appeared for replicating IoT honeypots. *Telnet IoT Honeypot*³. It creates a Python-developed honeypot emulating a telnet server to detect malware that exploits weak passwords, including the capacity of acting as a honey net to detect botnets. One year later, *RloTPoT*, came as a more modern, containerised option for modular, hybrid-interaction honeypot for lab Industrial environments. It supports many protocols (Telnet, SSH, CoAP, Modbus, MQTT) [41].

From another perspective, Moving Target Defence (MTD) examples are less but latest. Available since 2022, *Tosh*⁴ proposed a lightweight code for applying genetic algorithms to modify up to 13 parameters of a *nginx* decoy server. Around that time, *xuwkk*⁵ posted a MTD detection library contextualised to a power flow simulation tool. Lastly, on 2022, *Morphence*⁶ was created as an example of MTD against adversarial attacks, using models trained on MNIST and CIFAR10.

¹<https://github.com/omererdem/honeything>

²<https://github.com/darkarnium/kako>

³<https://github.com/Phype/telnet-iot-honeypot>

⁴<https://github.com/mikroskeem/tosh>

⁵https://github.com/xuwkk/Robust_MTD

⁶<https://github.com/um-dsp/Morphence>

Precisely on this type of attacks (adversarial), the most relevant analysis from what is ahead is provided as follows.

C. AIAS platform: deception mechanisms for increased IoT SMEs' cyber-protection

Lastly, there is the remarkable approach proposed by the on-going Horizon Europe Marie-Sklodowska-Curie project AIAS. There, a wide-spectrum platform, aimed at leveraging AI for increasing cyber-security for SMEs in Europe against adversarial attacks, is designed and implemented

The AIAS platform uses state-of-the-art technologies such as high-interaction honeypots, digital twins, and virtual personas in order to create a replica of a company or organisation through an innovative Deception Layer (DL). The DL is meant to confuse and mislead adversaries into interacting with the fake replica rather than the real AI systems, recording network environments and attack patterns. Additionally, digital twins dynamically show actual assets while the previously mentioned virtual personas mimic real human actions, enhancing the deception factor. This not only redirects harmful activity away from vital components but also gathers information on potential risks, thus helping enterprises understand and mitigate weaknesses in their AI infrastructure.

The DL uses advanced network monitoring and security analytics to analyse relevant data from the honeypots, digital twins, and virtual personas. These technologies are constantly inspecting network traffic for AI activity and cyber-attacks, thus enabling real-time detection of malicious activity. This strategy enhances the security of the organisation's AI models against evolving threats.

V. DISCUSSION OF THE FINDINGS AND CONCLUSION

After analysing the available literature and open source tools for the community, several reflections emanate.

First, although the theory of deception mechanisms is well elaborated, there are no clear works oriented to systematically study them for IoT characteristics. As developed in this work, the intrinsics of IoT deployments could be benefited from the decoy traits of honeypots, honeynets and moving target defences, but little evidences can be found.

As a matter of fact, literature pledges to game-theoretical approaches of adaptive honeypots and honeynets, but most of the references stop at small-scale lab simulations.

Only a few real implementations over real cases. Among the available options, traditionally, honeypots are the most used in validated implementation, as well as in open source libraries and tools. However, MTD are more prevalent during recent years. Nevertheless, the actionable solutions found are poorly maintained and burdensome to extend

Understanding that, therefore, the Technological Readiness Level is still low, projects such as AIAS are, then, necessary. The application of the theory to relevant cases (such as IoT SMEs) are the next steps to explore in the field.

REFERENCES

- [1] P. Radanliev, D. De Roure, C. Maple, J. R. Nurse, R. Nicolescu, and U. Ani, "Cyber risk in iot systems," University of Oxford Combined Work. Pap. Proj. Rep. Prep. PETRAS Natl. Cent. Excell. Cisco Res. Cent., Tech. Rep. 169701, 2019. [Online]. Available: <https://doi.org/10.20944/preprints201903.0104.v1>
- [2] O. O. Amoo, F. Osasona, A. Atadoga, B. S. Ayinla, O. A. Farayola, and T. O. Abrahams, "Cybersecurity threats in the age of iot: A review of protective measures," *International Journal of Science and Research Archive*, vol. 11, no. 01, pp. 1304–1310, 2024. [Online]. Available: <https://ijsra.net/content/cybersecurity-threats-age-iot-review-protective-measures>
- [3] T. S. AlSalem, M. A. Almaiah, and A. Lutfi, "Cybersecurity risk analysis in the IoT: A systematic review," *Electronics*, vol. 12, no. 18, p. 3958, 2023. [Online]. Available: <https://doi.org/10.3390/electronics12183958>
- [4] Asimily, "Iot device security in 2024: The high cost of doing nothing," *AI-Tech Park*, 2024. [Online]. Available: <https://ai-techpark.com/iot-device-security-in-2024-the-high-cost-of-doing-nothing-asimily/>
- [5] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, "A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review," *Sensors (Basel)*, vol. 23, no. 8, p. 4117, April 2023.
- [6] M. R. Islam and K. M. Aktheruzzaman, "An analysis of cybersecurity attacks against internet of things and security solutions," *Journal of Computer Communications*, vol. 8, pp. 11–25, 2020. [Online]. Available: <https://doi.org/10.4236/jcc.2020.84002>
- [7] E. Ahmady, R. Mojadadi, and M. Hakimi, "A comprehensive review of cybersecurity measures in the iot era," *Journal of Social Science Utilizing Technology*, vol. 2, pp. 288–298, 02 2024.
- [8] H. Szczepaniuk and E. K. Szczepaniuk, "Standardization of iot ecosystems: Open challenges, current solutions, and future directions," in *Internet of Things*. CRC Press, 2022, pp. 23–42.
- [9] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for iot under eavesdropper collusion," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281–1293, 2015.
- [10] S. Kumbhar, T. Faika, D. Makwana, T. Kim, and Y. Lee, "Cybersecurity for battery management systems in cyber-physical environments," in *2018 IEEE Transportation Electrification Conference and Expo (ITEC)*. IEEE, 2018, pp. 934–938.
- [11] C.-H. Muñoz-Flores and J. Olivella-Nadal, *Enablers and Inhibitors for IoT Implementation*. Cham: Springer International Publishing, 2021, pp. 25–48. [Online]. Available: https://doi.org/10.1007/978-3-030-70478-0_2
- [12] A. A. Mughal, "Cybersecurity hygiene in the era of internet of things (iot): Best practices and challenges," *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 2, no. 1, pp. 1–31, 2019. [Online]. Available: <https://researchberg.com/index.php/araic/article/view/113>
- [13] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the iot: Future research directions," *Electronics*, vol. 11, no. 20, p. 3330, 2022.
- [14] M. Eceiza, J. L. Flores, and M. Iturbe, "Fuzzing the internet of things: A review on the techniques and challenges for efficient vulnerability discovery in embedded systems," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10390–10411, 2021.
- [15] DiUS, "Iot security: Device and firmware encryption options," 2023, accessed: 2024-07-13. [Online]. Available: <https://dius-au.medium.com/iot-security-device-and-firmware-encryption-options-bec08384b9ce>
- [16] R. S-Julián, I. Lacalle, R. Vaño, F. Boronat, and C. E. Palau, "Self-* capabilities of cloud-edge nodes: A research review," *Sensors*, vol. 23, no. 6, 2023. [Online]. Available: <https://www.mdpi.com/1424-8220/23/6/2931>
- [17] C.-M. Chen, L. Yang, Y. Zhang, and X. Sun, "Edge learning for 6g-enabled internet of things: A comprehensive survey," *IEEE Communications Surveys Tutorials*, 2023. [Online]. Available: <https://ieeexplore.ieee.org/document/10255264>
- [18] S. Kumari, A. Thompson, and S. Tiwari, "6g-enabled internet of things-artificial intelligence-based digital twins: Cybersecurity and resilience," in *Emerging Technologies and Security in Cloud Computing*. IGI Global, 2024, pp. 363–394.
- [19] M. H. Almeshekah and E. H. Spafford, "Cyber security deception," *Cyber Deception: Building the Scientific Foundation*, pp. 23–50, 2016.
- [20] L. Zhang and V. L. Thing, "Three decades of deception techniques in active cyber defense-retrospect and outlook," *Computers & Security*, vol. 106, p. 102288, 2021.
- [21] H. project, *Know your enemy: Learning about security threats*. Addison Wesley, 2004.
- [22] Q. D. La, T. Q. Quek, J. Lee, S. Jin, and H. Zhu, "Deceptive attack and defense game in honeypot-enabled networks for the internet of things," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1025–1035, 2016.
- [23] L. Spitzner, *Honeypots: tracking hackers*. Addison-Wesley Reading, 2003, vol. 1.
- [24] I. Mokube and M. Adams, "Honeypots: concepts, approaches, and challenges," in *Proceedings of the 45th annual southeast regional conference*, 2007, pp. 321–326.
- [25] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Computers & Security*, p. 103792, 2024.
- [26] D. V. Silva and G. D. R. Rafael, "A review of the current state of honeynet architectures and tools," *International Journal of Security and Networks*, vol. 12, no. 4, pp. 255–272, 2017.
- [27] L. Spitzner, "The honeynet project: Trapping the hackers," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 15–23, 2003.
- [28] M. Ge, J.-H. Cho, D. Kim, G. Dixit, and I.-R. Chen, "Proactive defense for internet-of-things: moving target defense with cyberdeception," *ACM Transactions on Internet Technology (TOIT)*, vol. 22, no. 1, pp. 1–31, 2021.
- [29] S. Dowling, M. Schukat, and H. Melvin, "A zigbee honeypot to assess iot cyberattack behaviour," in *2017 28th Irish signals and systems conference (ISSC)*. IEEE, 2017, pp. 1–6.
- [30] R. E. Navas, F. Cuppens, N. B. Cuppens, L. Toutain, and G. Z. Papadopoulos, "Mtd, where art thou? a systematic review of moving target defense techniques for iot," *IEEE internet of things journal*, vol. 8, no. 10, pp. 7818–7832, 2020.
- [31] A. Judmayer, G. Merzdovnik, J. Ullrich, A. G. Voyiatzis, and E. Weippl, "A performance assessment of network address shuffling in iot systems," in *Computer Aided Systems Theory—EUROCAST 2017: 16th International Conference, Las Palmas de Gran Canaria, Spain, February 19–24, 2017, Revised Selected Papers, Part I 16*. Springer, 2018, pp. 197–204.
- [32] M. Ge, J.-H. Cho, C. A. Kamhoua, and D. S. Kim, "Optimal deployments of defense mechanisms for the internet of things," in *2018 International Workshop on Secure Internet of Things (SIoT)*. IEEE, 2018, pp. 8–17.
- [33] J. Pateria, L. Ahuja, and Seth, "Deception technology companions with iot-a platform of connected world and bluff," vol. 2555, 10 2022, p. 030001.
- [34] A. H. Anwar, C. Kamhoua, and N. Leslie, "Honeypot allocation over attack graphs in cyber deception games," in *2020 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2020, pp. 502–506.
- [35] A. H. Anwar and C. A. Kamhoua, "Cyber deception using honeypot allocation and diversity: A game theoretic approach," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2022, pp. 543–549.
- [36] Z. Rehman, I. Gondal, M. Ge, H. Dong, M. Gregory, and Z. Tari, "Proactive defense mechanism: Enhancing iot security through diversity-based moving target defense and cyber deception," *Computers & Security*, vol. 139, p. 103685, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404823005953>
- [37] Y. Zhou, G. Cheng, and S. Yu, "An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5366–5380, 2021.
- [38] Z. Rehman, I. Gondal, M. Ge, H. Dong, M. A. Gregory, and Z. Tari, "Proactive defense mechanism: Enhancing iot security through diversity-based moving target defense and cyber deception," *Computers & Security*, vol. 139, p. 103685, 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404823005953>
- [39] A. Vetterl and R. Clayton, "Honware: A virtual honeypot framework for capturing cpe and iot zero days," in *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 2019, pp. 1–13.
- [40] A. G. Manzanares, "Honeyio4: The construction of a virtual, low-interaction iot honeypot," 2017.
- [41] S. Srinivasa, J. Pedersen, and E. Vasilomanolakis, "Riotpot: a modular hybrid-interaction iot/ot honeypot," 10 2021.