

# Misbehavior detection systems in IoT environment: A survey

Rahma Trabelsi<sup>1,\*</sup>, Ghofrane Fersi<sup>1</sup> and Mohamed Jmaiel<sup>1</sup>

<sup>1</sup>ReDCAD Laboratory, ENIS, University of Sfax, Tunisia

## Abstract

The rapid expansion of IoT systems has a double-edged weapon. Indeed, they have significantly broadened their range of applications. However, this led to new security issues. In fact, IoT systems are known for their sensitivity to several attacks which may reduce its reliability and availability. So it is primordial to protect IoT systems against these attacks. The first step to fight against these attacks is to detect any misbehavior that may lead to an attack. Such a process should be automatized for further efficiency. In this survey, we present some attacks in order to understand them and we introduce some misbehavior detection systems mechanisms that ensure security in IoT systems. We classify misbehavior detection systems depending on their main detection features. We also highlight the advantages and drawbacks of each type.

## Keywords

Misbehavior detection systems, IoT, Survey

## 1. Introduction

Internet of Things (IoT) [1] [2] is a large-scale environment that connects different devices through the Internet. In other words, IoT networks consist of interconnected devices (sensors, actuators, and smart objects) that collect and exchange data over the Internet. These devices often have limited resources and may be vulnerable to various security threats. The evolution of IoT engendered new security issues. So Securing IoT systems against malicious attacks has become a fundamental requirement. In order to secure IoT systems, researchers have proposed lightweight cryptographic solutions [3]. Cryptographic algorithms can encrypt data transmitted between IoT devices and servers. Even if data are intercepted, they remain unreadable to unauthorized access. So, implementing cryptographic solutions enhances the resilience of IoT systems against various cyber-attacks, including man-in-the-middle attacks, replay attacks, and data tampering. Also, different access control solutions [4] have been proposed in order to prevent unauthorized access. Several technologies like fog computing [5] and blockchain are used to implement access control solutions. Several researchers concentrated on evaluating the behavior of different participants in IoT networks. They proposed a misbehavior detection


---


TACC 2023: Tunisian-Algerian Joint Conference on Applied Computing, November 06–08, 2023, Sousse, Tunisia

\*Corresponding author.

✉ rahma.trabelsi@redcad.org (R. Trabelsi); ghofrane.fersi@redcad.org (G. Fersi); mohamed.jmaiel@redcad.org (M. Jmaiel)

ORCID 0000-0002-3931-9399 (R. Trabelsi); 0000-0003-0427-5127 (G. Fersi); 0000-0002-2664-0204 (M. Jmaiel)

 © 2023 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

systems which are security mechanisms designed to identify and respond to abnormal or suspicious activities.

Misbehavior detection systems are essential for protecting computer networks and systems from malicious activity. They help identify abnormal behavior, such as malware attacks, intrusion attempts and alert system administrators so they can take appropriate security measures. The study of misbehavior detection systems is becoming increasingly important. These systems play a key role in threat prevention, data protection, online security and efficient resource management, making them a critical area of research and development for many industries and sectors.

In this paper, we focus on presenting an overview of several misbehavior systems and their evaluation.

The remainder of this paper is organized as follows: Section 2 presents the related work. Section 3 gives a brief review of several attacks. Section 4 overviews different misbehavior detection systems and classified them. Finally, the conclusion, current limitations and future directions are discussed in Section 5.

## 2. Related Work

In this section, we present existing surveys that have studied misbehavior detection systems and specify the difference and the novelty of our paper compared to them. Authors in [6] focused specifically on misbehavior detection in VANET. They provided a resume on different attacks like jamming attacks and sybil attacks. The authors in [7] presented several attacks and focused on machine learning-based misbehavior detection systems for vehicular networks. They categorized solutions into various domains based on architecture, approach, node-centric and datacentric schemes.

The paper [8] provides an analysis of intrusion detection systems (IDS) based on deep learning techniques proceeded by various systems for detecting intrusions. In anomaly detection systems, they assumed that challenges can be summarized into factors such as normality, adaptability, dynamic profile update, noisy data, false alarm rates and complexity. A survey of deep learning-based Industrial Internet of Things (IIoT) misbehavior detection in smart cities was proposed in [9]. In this work, the authors investigated how deep learning techniques can enhance the efficiency of any application in the proposed domain. In [10], authors presented anomaly-based detection systems and identified present-day issues and challenges like the fact of obtaining specific data is time-consuming, expensive, and not always possible. The paper [11] presents an overview of signature-based IDS systems developed using various machine learning approaches. The novelty of our survey compared with existing ones is that our survey does not focus on a specific domain. In fact, we present different misbehavior systems in various IoT domains. Also, we present a new classification of misbehavior detection. In fact, we classified solutions into three main types which are behavior-based, signature-based and reputation-based detection systems.

**Table 1**

Comparison of the existing surveys

| Paper             | Attacks    | Application domain | Behavior based | Signature based | Reputation based |
|-------------------|------------|--------------------|----------------|-----------------|------------------|
| [6]               | Yes        | Vanet              | No             | No              | No               |
| [7]               | Yes        | Vanet              | No             | No              | No               |
| [8]               | No         | General            | No             | No              | No               |
| [9]               | Yes        | IIoT               | No             | No              | No               |
| [10]              | No         | General            | Yes            | No              | No               |
| [11]              | No         | General            | No             | Yes             | No               |
| <b>Our survey</b> | <b>Yes</b> | <b>General</b>     | <b>Yes</b>     | <b>Yes</b>      | <b>Yes</b>       |

### 3. Frequent attacks in IoT

This section provides an overview of attacks that affect IoT networks. We categorize these attacks depending on their corresponding layer in the IoT three-layer architecture.

#### 3.1. Physical attacks

Physical attacks are directed toward the hardware components within the system.

- Jamming: is a disruption in the channel of communication. For example, the adversary continually launches a radio frequency to make noise in the network.
- Node tampering: is an attack in which the attacker alters physically the compromised node in order to obtain sensitive information.
- Malicious node injection: is an attack where the attacker physically injects a malicious node between two or more nodes.
- Malicious code injection: The attacker physically introduces a malicious code into a node in an IoT system. Then it could get full control of IoT system.
- Sleep deprivation attack: The attacker sends repetitively numerous packets to the nodes leading to their shutdown.

#### 3.2. Network attacks

These attacks concerned the network layer of IoT systems.

- Man in the middle attack: is where an attacker is looking to interrupt the connection between two parties. The attacker has the possibility not only to read the traffic data but also to modify it.
- Deny of service (DoS): is an attack that makes the service unavailable or prevents the user from services. The most of the DoS attacks target the TCP protocol.
- Distributed deny of services(DDoS): is similar to DoS but in DDoS, the incoming traffic to the victim originates from many different sources. The DDoS attack is more difficult to fix.
- Sinkhole attack: In this attack, attacker node advertises a beneficial path to attract many nearby nodes to route traffic through it.

- Sybil attack: is an attack where a malicious node uses several identities on the same physical node. Using this attack large parts of a network can be taken under the attacker's control without deploying physical nodes.

### 3.3. Application attacks

These attacks are mainly software attacks.

- SQL injection: is the act of passing SQL code into interactive web applications that are employed in database services.
- Phishing attack: in this attack, an attacker could get access to passwords, credit cards and other sensitive data via hacking an email, phone, or social media.
- Virus, Worms, Trojan horse and Spyware: A potential adversary has the capability to harm the system through the utilization of malicious code. These code instances are distributed via email attachments or by downloading files from the Internet. The worm possesses the capacity to autonomously replicate itself without requiring any human intervention.

## 4. Misbehaviour detection systems

Misbehavior detection systems in IoT refer to techniques and algorithms used to identify abnormal or malicious behavior in IoT networks and devices. These systems can detect and prevent a variety of malicious activities, such as DoS attacks, unauthorized access, data tampering, and more. There are several methods used for misbehavior detection in IoT networks, including:

- Behavior-based detection: This involves monitoring the normal behavior of devices and identifying any deviation from the expected behavior. Behavior detection can be achieved through techniques such as statistical analysis, machine learning, and rule-based systems. Anomaly detection is considered as a behavior-based sub-type. In this paragraph, we will present behavior/anomaly based detection systems. The authors in [12] present a method for using deep learning to detect anomalies in IoT systems. They propose using a combination of autoencoders and recurrent neural networks to analyze sensor data and identify patterns that deviate from normal behavior. They evaluate the performance of their method on a dataset of real-world IoT sensor data and demonstrate that it is effective at detecting anomalies.

A method for detecting anomalies in smart hospitals was proposed in [13]. The main contribution of this article is that the proposed method can be used in real-time. The authors propose to use a combination of statistical methods and machine learning techniques to analyze data behavior. They also propose a new algorithm for anomaly detection that is based on the k-nearest neighbors (k-NN) method and is specifically tailored to the characteristics of IoT data and systems in smart hospitals.

A real-time anomaly detection system for industrial robots was proposed in [14]. This work automatically learns normal patterns from time series data in training. This solution is tested by injecting faults into the robot and observing how the robot resolves them.

The evaluation shows that the proposed model can detect anomalies spatially and temporally. The authors in [15] identified compromised devices using an anomaly detection method that merges federated learning with linguistic analysis, adapted to specific device categories. The evaluation showed that detection performance is around 94% for positive and 99% for negative samples.

An anomaly-based intrusion detection system is proposed in [16]. This work is based on a deep-learning model called Pearson-Correlation Coefficient - Convolutional Neural Networks (PCC-CNN) to detect network anomalies. The evaluation shows that this model is computationally efficient.

A proposed approach called BRIoT [17] utilizes behavior rule specification in order to detect misbehavior in IoT devices within Cyber-Physical Systems (CPS). BRIoT allows the specification of both normal and abnormal behavior for each IoT device and uses this information to identify and prevent misbehavior. The known attacks that have been investigated in that paper are spoofing attack, capture attack, DoS and energy exhaustion attack. This approach is based on a device being monitored by a peer device (or more than one peer IoT device to increase the detection strength). If a peer monitoring IoT device is itself malicious and performs attacks, its misbehavior would be detected by another peer IoT device. The authors claim that BRIoT is effective at detecting a wide range of misbehaviors and is able to adapt to changing operating environments. They also present the results of an experimental evaluation of BRIoT, which showed that it is able to detect misbehavior with high accuracy and low false positive rates.

The authors in [18] presented a pattern recognition algorithm named as "Capturing-the-Invisible (CTI)" to find the hidden process in industrial control device logs and detect behavior-based attacks being performed in real-time. This solution is a new process discovery algorithm that detects and monitors issues from device logs. The evaluation shows that this approach discovers more anomalies than other solutions and consumes less time. The main drawback of the behavior-based detection systems is its high false positive rate. In fact, in this strategy, each behavior that differs from the "normal" pattern is considered as abnormal which is not always true. Furthermore, there is a difficulty to specify why is considered as "normal" behavior? In addition to that, the anomaly-based detection systems are inefficient in the detection of the new attacks. To overcome this, it is required that the system remains all the time in a continuous training which exhausts its resources and degrades its performance.

- Signature-based detection: This method involves identifying known malicious patterns or "signatures" in network traffic or device behavior. Signature-based detection can be used to detect known attacks, such as known malware or known attack techniques. A blockchain signature-based intrusion detection in IoT was proposed in [19]. In this work, the key concept is to employ blockchain technology to gradually construct a dependable signature database.

The authors in [20], proposed a lightweight misbehavior detection scheme that relies on formal verification and automatic model checking in a medical cyber physical system. The authors in [21] generate the rules for modern attacks based on signature attacks. In their work, they used machine learning algorithms for generating effective rules to support lightweight IDS systems.

In spite of the ability of the signature-based misbehavior detection system to detect most of the known attacks, it faces difficulties to detect new attacks that it does not have its corresponding signature. Also this system is unable to detect polymorphic attacks. Contrarily to the anomaly-based misbehavior detection systems, the signature-based system suffer from high False Negatives since it is unable to detect many real attacks. Also, such systems are unable to detect attacks when the traffic is encrypted.

- Reputation-based detection: This method involves maintaining a reputation score for each device or user based on their past behavior. Devices or users with a low reputation score may be flagged as potential threats and further monitored or restricted.

The authors in [22] proposed a new model for grouping agents in IoT systems based on their reputation. This approach is based on blockchain technology to create a decentralized and tamper-proof system for storing and managing agent reputation information. They proposed to use blockchain to create a distributed ledger that stores the reputation of each agent, which can be used to group agents into different trust levels. This reputation-based model is intended to improve the security and reliability of IoT systems by allowing devices to communicate with only trusted peers. Additionally, the use of blockchain technology would ensure the integrity and transparency of the reputation information. A lightweight reputation-based RPL protocol is proposed in [23] in order to evaluate the behavior of IoT nodes. The authors used weight factors as new parameters to calculate reputation. In this approach, the network lifetime is divided into a series of evaluation periods in order to compare normal packet loss with the actual packet loss and then they can evaluate the behavior of all neighbors.

The authors in [24] introduced a novel trust evaluation framework that integrates multiple sources, incorporating the contextual elements and the reputations of involved nodes in the assessment of a user's trustworthiness. They used context-aware feedback in the evaluation of the behavior. They proposed the implementation of a monitor mode which is designed to proactively detect malicious users even before they initiate communication with the cloud. By putting malicious users in monitor mode, it assists fog nodes to prevent any security issues. The evaluation shows that the proposed approach is effective and reliable to evaluate the trustworthiness of a user.

The inaccurate reputation information in reputation-based system may lead to both false positives and false negatives. Additionally, reaching the steady state in these systems requires time and resources. Hence, many attacks may occur before reaching that state. Also the reputation based systems rely only on reputations received from other nodes. Hence, compromising a set of these node leads to reduce significantly the efficiency of these solutions.

Table 2 displays a comparison between different misbehavior systems. It is possible to combine two or more misbehavior detection systems. This can provide a more comprehensive approach to detecting malicious activity, as each method has its own strengths and weaknesses. In the next paragraph, we present some hybrid approaches.

- Hybrid systems: A DoS attack detection using hybrid IDS was proposed in [25]. This model is based on a combination between signature-based IDS and anomaly-based IDS. In this solution, if the malicious behavior reached the signature-based detector without

**Table 2**

A comparison of the methods for misbehavior detection in IoT networks

| System                     | Benefits  | Limits   |
|----------------------------|---|--|
| Anomaly detection          | Can detect unknown or previously unseen malicious activity.         | Can have a high rate of false positives.   |
| Signature-based detection  | Can detect known malicious patterns in network traffic.             | May not be able to detect unknown or previously unseen malicious activity.                           |
| Reputation-based detection | Can detect malicious devices or users based on their past behavior. | May not be able to detect new malicious devices or users that have not yet established a reputation. |

any detection, it will be traced and carefully monitored by the anomaly-based detector. The authors in [26] proposed a new misbehavior detection approach that utilizes a behavior detection system and a distributed signature scheme in order to detect and prevent malicious activity in IoT devices within medical CPS. After the behavior rule set is identified, they transform it to a state machine for lightweight misbehavior detection. The behavior-rule-to-state-machine transformation process is automatic. The proposed approach is lightweight and efficient, making it suitable for use in resource-constrained IoT devices. The authors also present the results of an experimental evaluation of the proposed approach, which showed that it effectively detects and prevents misbehavior in medical CPS.

The authors in [27] proposed a hybrid anomaly detection method that combines signature and behavior-based methods to improve detection performance. For the purpose of signature-based detection, they employed the standard deviations calculated from the normal data to serve as the classification criteria. This solution provides a real-time control system. The evaluation shows that the proposed method improved the precision and recall compared to other ones.

## 5. Conclusion and future directions

This survey has provided valuable insights into misbehavior detection systems. We overviewed firstly different attacks. Through careful analysis of attacks, a better understanding of several attacks is ensured. Secondly, we presented several misbehavior detection systems.



In this field, we provided a new classification which is based on the type of detection system. This classification has led to a better understanding the advantages and limits of each type. This survey has provided a wide scope of different detection approaches, which provides a conclusive overview. The limitation of our work is that it was restricted to a small number of existing "misbehavior detection systems". Hence, we plan to continue our investigation by completing this survey with most proposed approaches for detection of misbehaviors. We can extend this work in the future by covering other solutions.

## Funding

Dr. Ghofrane Fersi: project 22PEJC-D3P1 "Système IoT basé sur blockchain pour la supervision sanitaire sécurisée des patients lors des pandémies",Tunisian Ministry of Higher Education and Scientific Research.

## References

- [1] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, M. Iranmanesh, The internet of things (iot) in healthcare: Taking stock and moving forward, *Internet of Things* 22 (2023) 100721. URL: <https://www.sciencedirect.com/science/article/pii/S2542660523000446>. doi:<https://doi.org/10.1016/j.iot.2023.100721>.
- [2] A. Hemmati, A. M. Rahmani, The internet of autonomous things applications: A taxonomy, technologies, and future directions, *Internet of Things* 20 (2022) 100635. URL: <https://www.sciencedirect.com/science/article/pii/S2542660522001160>. doi:<https://doi.org/10.1016/j.iot.2022.100635>.
- [3] M. N. Khan, A. Rao, S. Camtepe, Lightweight cryptographic protocols for iot-constrained devices: A survey, *IEEE Internet of Things Journal* 8 (2021) 4132–4156. doi:10.1109/JIOT.2020.3026493.
- [4] A. Ouaddah, H. Mousannif, A. Abou Elkalam, A. A. Ouahman, Access control in the internet of things: Big challenges and new opportunities, *Computer Networks* 112 (2017) 237–262.
- [5] G. Fersi, Fog computing and internet of things in one building block: A survey and an overview of interacting technologies, *Cluster Computing* 24 (2021) 2757–2787.
- [6] R. W. van der Heijden, S. Dietzel, T. Leinmüller, F. Kargl, Survey on misbehavior detection in cooperative intelligent transportation systems, *IEEE Communications Surveys & Tutorials* 21 (2019) 779–811. doi:10.1109/COMST.2018.2873088.
- [7] A. Boualouache, T. Engel, A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks, *IEEE Communications Surveys & Tutorials* 25 (2023) 1128–1172. doi:10.1109/COMST.2023.3236448.
- [8] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, S. A. Bahaj, H. U. Khan, Deep learning for intrusion detection and security of internet of things (iot): Current analysis, challenges, and possible solutions, *Sec. and Commun. Netw.* 2022 (2022). URL: <https://doi.org/10.1155/2022/4016073>. doi:10.1155/2022/4016073.



- [9] N. Magaia, R. Fonseca, K. Muhammad, A. H. F. N. Segundo, A. V. Lira Neto, V. H. C. de Albuquerque, Industrial internet-of-things security enhanced with deep learning approaches for smart cities, *IEEE Internet of Things Journal* 8 (2021) 6393–6405. doi:10.1109/JIOT.2020.3042174.
- [10] A. Chatterjee, B. S. Ahmed, Iot anomaly detection methods and applications: A survey, *Internet of Things* 19 (2022) 100568. URL: <https://www.sciencedirect.com/science/article/pii/S2542660522000622>. doi:<https://doi.org/10.1016/j.iot.2022.100568>.
- [11] M. Masdari, H. Khezri, A survey and taxonomy of the fuzzy signature-based intrusion detection systems, *Applied Soft Computing* 92 (2020) 106301. URL: <https://www.sciencedirect.com/science/article/pii/S1568494620302416>. doi:<https://doi.org/10.1016/j.asoc.2020.106301>.
- [12] L. Aversano, M. Bernardi, M. Cimitile, R. Pecori, L. Veltri, Effective anomaly detection using deep learning in iot systems, *Wireless Communications and Mobile Computing* 2021 (2021). doi:10.1155/2021/9054336.
- [13] A. M. Said, A. Yahyaoui, T. Abdellatif, Efficient anomaly detection for smart hospital iot systems, *Sensors* 21 (2021). URL: <https://www.mdpi.com/1424-8220/21/4/1026>. doi:10.3390/s21041026.
- [14] T. Chen, X. Liu, B. Xia, W. Wang, Y. Lai, Unsupervised anomaly detection of industrial robots using sliding-window convolutional variational autoencoder, *IEEE Access* 8 (2020) 47072–47081. doi:10.1109/ACCESS.2020.2977892.
- [15] T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, A.-R. Sadeghi, Diot: A federated self-learning anomaly detection system for iot, in: *2019 IEEE 39th International conference on distributed computing systems (ICDCS)*, IEEE, 2019, pp. 756–767.
- [16] M. Bhavsar, K. Roy, J. Kelly, O. Olusola, Anomaly-based intrusion detection system for iot application, *Discover Internet of Things* 3 (2023) 5.
- [17] V. Sharma, I. You, K. Yim, I.-R. Chen, J.-H. Cho, Briot: Behavior rule specification-based misbehavior detection for iot-embedded cyber-physical systems, *IEEE Access* 7 (2019) 118556–118580. doi:10.1109/ACCESS.2019.2917135.
- [18] A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, L. Mostarda, Capturing-the-invisible (cti): Behavior-based attacks recognition in iot-oriented industrial control systems, *IEEE Access* 8 (2020) 104956–104966. doi:10.1109/ACCESS.2020.2998983.
- [19] W. Li, S. Tug, W. Meng, Y. Wang, Designing collaborative blockchain signature-based intrusion detection in iot environments, *Future Generation Computer Systems* 96 (2019) 481–489.
- [20] I. You, K. Yim, V. Sharma, G. Choudhary, I.-R. Chen, J.-H. Cho, Misbehavior detection of embedded iot devices in medical cyber physical systems, in: *Proceedings of the 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE '18*, Association for Computing Machinery, New York, NY, USA, 2020, p. 88–93. URL: <https://doi.org/10.1145/3278576.3278601>. doi:10.1145/3278576.3278601.
- [21] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, K. Sakurai, Rule generation for signature based detection systems of cyber attacks in iot environments, *Bulletin of Networking, Computing, Systems, and Software* 8 (2019) 93–97.
- [22] G. Fortino, F. Messina, D. Rosaci, G. M. L. Sarné, Using blockchain in a reputation-based

- model for grouping agents in the internet of things, *IEEE Transactions on Engineering Management* 67 (2020) 1231–1243. doi:10.1109/TEM.2019.2918162.
- [23] A. Patel, D. Jinwala, A reputation-based rpl protocol to detect selective forwarding attack in internet of things, *International Journal of Communication Systems* 35 (2022) e5007.
- [24] Y. Hussain, H. Zhiqiu, M. A. Akbar, A. Alsanad, A. A.-A. Alsanad, A. Nawaz, I. A. Khan, Z. U. Khan, Context-aware trust and reputation model for fog-based iot, *IEEE Access* 8 (2020) 31622–31632. doi:10.1109/ACCESS.2020.2972968.
- [25] M. M. Shurman, R. M. Khrais, A. A. Yateem, Iot denial-of-service attack detection and prevention using hybrid ids, in: *2019 International Arab Conference on Information Technology (ACIT)*, 2019, pp. 252–254. doi:10.1109/ACIT47987.2019.8991097.
- [26] G. Choudhary, P. V. Astillo, I. You, K. Yim, I.-R. Chen, J.-H. Cho, Lightweight misbehavior detection management of embedded iot devices in medical cyber physical systems, *IEEE Transactions on Network and Service Management* 17 (2020) 2496–2510. doi:10.1109/TNSM.2020.3007535.
- [27] H.-Y. Kwon, T. Kim, M.-K. Lee, Advanced intrusion detection combining signature-based and behavior-based detection methods, *Electronics* 11 (2022). URL: <https://www.mdpi.com/2079-9292/11/6/867>. doi:10.3390/electronics11060867.