ISSN 2278-3091
Volume 9, No.1.5, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse0191.52020.pdf
https://doi.org/10.30534/ijatcse/2020/0191.52020

Intrusion Detection in the Internet of Things

ABDELOUAHED BAMOU[1*], MOULAY DRISS EL OUADGHIRI[1], BADRADDINE AGHOUTANE[1]
[1] IA Laboratory Science Faculty My Ismail University of Meknes, Morocco.
abdelbamou@gmail.com, dmelouad@gmail.com, b.aghoutane@gmail.com

ABSTRACT

The IoT has been booming in recent years and is evolving rapidly, but attacks against it are also continuing to evolve in a worrying way. In order to take full advantage of these systems, it is worth securing them. Among the greatest security tools to defend IoT against attacks that threaten these low-resource systems (processor, memory, storage, ...), we find Intrusion Detection Systems (IDS). The objective of this paper is to provide a general study on IoT IDS and implementation techniques based on IDS specifically classical methods as well as learning methods.

Key words: Internet of Things; Intrusion-Detection System (IDS); IDS based on anomalies; Deep learning; Machine learning.

1. INTRODUCTION

The IoT is a smart community which connects all matters to the net for the reason of exchanging facts with agreed protocols [1]. In IoT network, objects are connected with smart tiny sensors. IoT gadgets can talk with each different without human intermediation [2]. IoT offers diverse services like smart houses, smart towns, voice Assistants, lighting and switches. fitness tracking, smart environment,…

With the improvement of IoT programs, there are many IoT protection problems that cannot be left out. If safety this troubles are not addressed then the private data may be leaked at any time. For this reason, the safety difficulties have to be addressed:

- Confidentiality: an attacker can without difficulty intercept the message passing from sender to the receiver so that content can be modified and privacy may be leaked. So that comfy message passing is required in iot.
- Integrity: the message must not be altered in transit; it have to be received at receiver node identical as its far dispatched at sender node. integrity ensures that message has now not been altered with the aid of unauthorized individuals even as in transmission [3].
- Information and resources must be accessible or available when needed. Attacks can handicap this availability, such as: jamming, denial of service (DoS), black hole attacks,...
- Authenticity: authenticity includes evidence of identity [4]. Users should be capable of become aware of every differing's identification with which they may be interacting. It can be proven via authentication method so the unauthorized entity can't participate in the verbal exchange [5].
- Non-repudiation: non-repudiation guarantees that the sender and receiver cannot deny having dispatched and acquired the message respectively [6].
- Information freshness: it assures that ancient information is not reused. Data need be new [7].

The evaluation, prevention and detection of these attacks that threaten the IoT must be a concern in order to protect this network of heterogeneous and low-resource devices. IDSs can play an important role in this case; they can recognize these attacks by filtering malicious activity on the network.

This paper begins with a review of the most famous intrusion detection techniques in IoT. Then, we define the principle overview of classical and learning techniques used to broaden IDS in IoT.

2. GENERAL STUDY OF INTRUSION DETECTION SYSTEM

2.1 Intrusion Detection System

Intrusion Detection Systems (IDS) are security tools that enhance the security of information and communication system resources and networks (Intrusion is an undesirable movement which is hurtful to nodes or networks). IDS is utilized to watch the vindictive traffic particularly node and network. It can go about as a second line of protection which may defense the system from intruders [8]. It can examine and explore machines and client activities, recognize known and obscure attacks and distinguish wicked system action. It fills in as a caution or system observer, it keeps away from harm of the frameworks by producing an alarm before the aggressors start to attack. It can identify both inside and outer attacks, inward attacks are propelled by malignant or bargained network that have a place with the system; while outer attacks are propelled by outsiders who are started by outside system.

There are for the most part three segments of IDS: Monitoring, Analysis and recognition, Alarm:

The monitoring module screens the system deals. Analysis and recognition might be a center part of IDS which identifies the intrusion reliable with determined algorithm. Alert

module dispatch a caution if intrusion is identified [9].
IDSs are commonly categorized consistent with deployment; detection methodology, decision quality, Responses on Attacks, and implementation strategy.

2.2. Deployments: Location Based IDS

To decide the movement of system and activate the caution as when the system is under the attack, the IDS ought to screen the system at the specific focus. Two common checking spots are said as beneath:

2.2.1) Host-based

Host-based Intrusion Detection Systems (HIDSs) are installed on a host machine (i.e., a device or a Thing). They monitor and analyze activities related to system application files and operation system. HIDSs are preferred against insider intrusion deterrence and prevention.

2.2.2) Network-based (NIDS)

NIDS scans the packets in the network for abnormal packets. They are very efficient against external attacks. For the rest of this paper we'll focus on NIDS.
The following metrics based on the figure 1 can be used to validate the IDS:

	No Alert	**Alert**
No attack	True negative	False positive
Attack is happening	False negative	True positive

Figure 1: Performance indicators for the IDS

-True positive: the attack is in progress and the IDS has been correctly detected and alerted.
- True negative: no attack, no warning, the IDS correctly sees that the behavior is normal.
- False Positive: No attack, but the IDS incorrectly sees that the attack is occurring and gives a false alarm.
- False negative: the attack is in progress however, the IDS detect nothing and therefore, no alert.
- The detection rate is a ratio of the detections found on all intrusions.
- Accuracy indicates is a well-ordered intrusion report on all data entered. It represents the ability of the IDS to distinguish intrusions from normal states.
- Resource consumption (processor, memory, power, bandwidth) are the parameters of system performance.
- The type of attacks processed (Dos, sinkhole, ...), the perfect is that IDS can detect all types of attacks.

IDS must have a high detection rate and accuracy, but it must not annoy network administrators (the level of false positives must be minimal). Moreover, it should not reduce system performance, which is fatal for low-resource IoT systems [10].

2.3. Detection methodology

The mission of IDSs is to create an alert when they identify intrusion activity on the system. This is possible using many types of detection methods. IDS approaches are classified into three categories: signature-based, anomaly-based, specification-based and hybrid [11].

2.3.1) Signature-based detection

This approach recognizes attacks using their signatures stored in the internal IoT database. It is also called a rule-based detection technique. Each time an attack signature is found, a warning is issued. This process is extremely efficient and fast to identify known attacks, however it cannot take into account attacks that do not exist in the database [12]. This technique is simple to use, it only requires attack patterns to be stored in a database. However, it requires specific knowledge of the individual attack, and more storage space as the number of attacks increases. In addition to a regular update of the database with new attack signatures [13].
In order to implement this system, known attack profiles are generated from which signatures are formed. An example of a signature could be: "If there are at least three unsuccessful connection attempts within one minute, an alarm is triggered".

2.3.2) Anomaly-based detection:

This technique compares a recorded normal behavior with a current data stream; and if an activity differs from this normal behavior, it is considered an intrusion [14]. The anomaly can be recognized by statistical data analysis, exploration and algorithmic learning approaches.
Anomaly-based IDS allows unknown attacks to be taken into account. However, previously unknown legitimate activity can also be classified as malicious (false positive) and is a very expensive method for objects with limited resources [15].
The authors in [16] projected associate anomaly-based technique for identifying botnets dependent on the normal of 3 measurements, TCP control fields total, number of associations for every sensor and packet length to form the conventional behavior. Author A.BAMOU and his group analyzed the nodes behavior for distinguishing Denial of Service Attacks in IoT; they thought-about energy consumption of the node as a parameter. They established models of standard energy consumed by the nodes in normal tasks and if any node is abnormal in power consumption then the node is under attacks [17]. Anomaly detection mechanism for resource affected IoT devices was projected by Summerville et al. [18]. The authors pretend that the protocols in IoTs are basic which bring about comparable network payloads, so they performed feature assortment utilizing bit-pattern matching. Another creative strategy was developed in 2015 by Pongle et al. [19] for identifying wormhole attacks in IoT systems. The methodology depended on the quantity of packets shared between nodes; on the off chance that packet rate of exchange is high contrasted with an ordinary conduct; at that point an alarm is activated. In any case, just explicit attacks were being recognized.

2.3.3) Specification detection:

This method is similar to anomaly detection. Except that in this approach the input specifications are manually developed to capture legitimate behavior; when the behavior deviates from these specifications, it is then considered an intrusion.

This method reduces the high rate of false alarms compared to anomaly detectors. No learning algorithm is required, but the challenge is that different specifications are required for different platforms or environments [20]. Most manually decided specification approaches depend heavily on the expertise of the security team and the network administrator. Inappropriate specifications lead to an increase in false positives and true negatives.

An example of specification-based approaches has been implemented to combat distributed denial of service (DDOS) attacks, in which the maximum capacity of each middleware layer is predefined and if the number of requests matches or exceeds the capacity, an alert is triggered to the network administrator [21]. Another example has been proposed by Le. et al. [22] for the RPL protocol where the protocol behavior is fed into a finite state machine to monitor network intrusions and malicious behavior.

2.3.4) Hybrid detection

This type of IDS consolidates signature and anomaly-based methodologies. A hybrid IDS uses two modules, one that recognizes signature-dependent attacks while the other discovers anomalies based on the typical network driving profile. A hybrid IDS improves accuracy by reducing false positives, but requires much more processing resources because both modules must run in parallel.

The vast majority of IDSs based on current anomalies are actually hybrid. They start by identifying an anomaly and then attempt to link it to the corresponding signature.

2.4. NIDS Placement Strategies

The strategy of placing IDS in a network can both maximize the benefits and minimize the limitations of the mechanism. The IDS can be placed in a solitary node from which network traffic is monitored or dispersed across multiple nodes.

2.4.1) Centralized:

In this approach, the IDS are placed on any centralized component, either at the node boundary or on any host. When the IDS are placed at the border router, it can analyze all traffic between the node and the Internet, while traffic that does not pass through the border router is not monitored. In addition, when part of the network is compromised, the centralized IDS may not monitor the nodes during the attack. Furthermore, this design does not seem suitable for IoT networks "comprising a large number of different nodes" because on the one hand, IoT components and applications are essentially dispersed, and on the other hand, the fact that an IDS remains in a single local node and only provides protection for that node is not fair. And on the other hand, the IDS risks to intense all the resources of the node running it.

2.4.2) Distributed:

In the distributed position, nodes may also be responsible for observing their neighbors. Nodes that watch their neighbors are referred to as watchdogs. To begin with, the nodes are called leader nodes, linked nodes or subnodes, forming a hierarchical data structure. The work of each node may change after a while due to system reconfiguration or an attack. At that time, each node displays a node that is unmatched in evaluating its inbound and outbound traffic. When a node identifies an attack, it communicates a message to alarm opposing nodes and to separate the attacker.

2.4.3) Hybrid IDS placement

It joins centralized and distributed investment ideas to capitalize on their strong strengths and stay away from their drawbacks.

The primary method of hybrid placement is to organize the network into clusters or regions, and only the node with more resources in each cluster hosts an IDS instance. This node then becomes responsible for monitoring the opposing nodes in its cluster. As opposed to distributed placement, nodes, which are regularly more robust, can host IDS instances.

Of all the above methods, the hybrid approach that best suits the situation and structure of the IoT network can be adopted. Manually designing a specific hybrid approach for each criterion is not practical, so it is necessary to use intelligent techniques that adapt to the needs.

2.4. Implementation strategies

An IDS can be implemented using a variety of techniques. We can divide them into two categories: Classical methods and learning techniques.

3. CLASSICAL METHODS

By classical methods, we mean all traditional methods different from the learning methods used to implement NIDS in IoT.

3.1. Hierarchical IDS.

The network is divided into groups. Here, nodes that are close to each other for the most part have a place with an equal group. Each group is led by a leader, called cluster head (CH), who controls the member nodes and contributes to the network review. However, most of the important coordination for signature or anomaly checking is done within the groups.

3.2. Mobile agent-based IDS.

The IDS is implemented in the form of a mobile agent that can move between the nodes of the network, while making the necessary observations to decide on the presence of attacks.

3.3. Distributed and collaborative IDS.

In this case, attacks are recognized by a few nodes working collaboratively, in fact the IDS is placed on a few nodes that monitor distinct parts of a framework, then the collected information is then shared between the different nodes, which make a common choice to decide whether the network behavior is normal or not.

3.4. Reputation-based IDSs.

This is a variant of distributed and collaborative IDSs, in which the consideration of nodes is evaluated based on their past behavior. Subsequently, each node has a reputation that can be established and calculated using trust management mechanisms.

3.5. IDS based on game theory.

Game theory (GT) is a mathematical construct that defines the conditions of cooperation, non-cooperation and repetition between rationally independent decision-makers. It is used to establish a mathematical model to capture behavior in strategic situations [23].
Recently, game theory methods have been used for intrusion detection where, in a two-player context, the attacker (intruder) is one player and IDS is the other player. Once IDS has detected an attack, it reacts to minimize the loss of the system. The IDS reactivity to a separate attack is a problem of maximization; it tries to maximize gains. In Wang et al., uncooperative game theory was used to treat IDS. They propose a methodology that dynamically modifies objects filtered by the host-based IDS, in accordance with probable attacks dependent on uncooperative games [24].

3.5. IDSs based on statistical detection.

It contains the generation of a stochastic profile for the traffic to be monitored. From this point, the network is observed and the actual traffic is compared to the reference profile. The IDS signals an anomaly if the behavior exceeds a certain threshold with respect to the generated profile. Statistical models can be single or multivariate models and time series.

4. IDS FOR IOT SYSTEMS SUPPORTED LEARNING TECHNIQUES

Machine learning and deep learning (ML/DL) are powerful techniques for deciding "normal" or "abnormal" behaviors in an IoT environment. Input information from each member of the IoT system can be gathered and explored to distinguish between behaviors that are harmful to the system. In addition, ML/DL techniques could be important in anticipating new attacks, which are frequently variants of past attacks, by learning from existing models.
The effectiveness of machine learning techniques in image recognition, fraud detection, and text classification has encouraged security researchers to use these algorithms, relying on input learning datasets, even in traditional attack detection methods such as signature and anomaly-based methods to enhance the security of IoT networks [25].
In deep learning methods, known for their ability to extract high-level features from large data sets, can be a powerful mechanism to detect small variants of attacks. They can identify hidden patterns in training data and rely entirely on recognizing the true face (of the attack) of any variant.
Compression capabilities and unsupervised pre-training are the main features of DL deployed on NIDSs under IoT constraints.
Two modules are fundamental for the construction of an IDS with learning techniques: one for learning and one for classification, as shown in Figure 2 [26]:

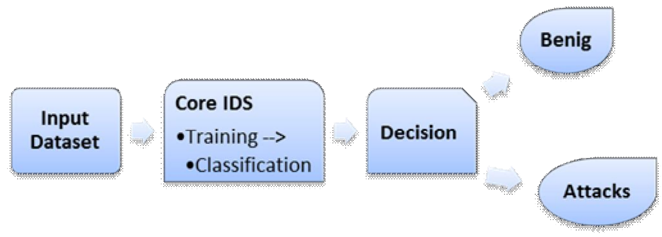

Figure 2: Typical scheme IDS

The collection of information is an essential step to build up a dataset[27] in IoT because, there is no specific dataset containing ordinary attacks for the IoT that can be used to identify attackers[28]. After Dataset input, a data normalization and balancing phase is necessary for any machine learning algorithm.[29].
In this section, we discuss the most promising ML and DL algorithms used in IDS for IoT.

4.1. IDS based on machine learning algorithms

Machine learning can be divided into two different models based on training data types: supervised and unsupervised, after that each type has several model machine-learning-based IDSs (Figure 3).
Supervised models form their classification or prediction model on the basis of capture the relationships between the input parameters (features) and the required output. Then, at the primary phase of supervised learning, models are expected to train the algorithms, which are then used to foresee or classify the new input.
Unsupervised learning methods, which are generally intended to analyze unlabeled data, aims to categorize the input data into distinctive groups by examining the similarity between them [30].

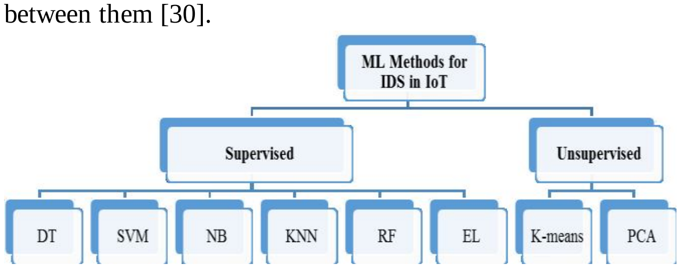

Figure 3: Classification of Machine learning methods

The following table 1 presents the advantages and disadvantages of each technique [31].

Table 1: The advantages and disadvantages of the traditional machine learning models

Algorithms	Advantages	Disadvantages
Support Vector Machines (SVM)	Take in helpful data from little train set; Strong generation capacity.	Do not work correctly on huge information or many classification tasks; aware of kernel function parameters
k-Nearest neighbor (KNN)	Apply to gigantic and nonlinear information; Train rapidly; Robust to noise;	Low precision on the minority class; Long test times; Sensitive to the parameter K
Naïve Bayes (NB)	Solid to noise; Able to learn incrementally	Do not work on attribute-related data
Decision tree (DT)	Automatically choice features; Robust interpretation	Classification result drifts to majority class; Disregard the relationship of data
Random forest (RF)	It allows the selection of features with few input parameters; and allows over-fitting	Not suitable when the required training data is large or real-time.
K-means clustering	Simple, can be trained rapidly; Strong scalability; Can fit to big data	Sensitive to parameter K and does not give good results on non-convex data.
Principal component analysis (PCA)	Reduces the dimensionality of the model, thus its complexity.	Needs other ML methods to establish an effective security approach.
Ensemble learning (EL)	It provides better results than a single classifier and resists over-fitting.	Need more processing time than a single classifier.

4.2. Techniques used in IDS based on Deep learning (DL) methods

Recently, the applications of DL to IoT systems have become an imperative research topic [32]. The most vital advantage of DL over traditional ML is its superior performance in large datasets.

Deep networks are constructed for supervised learning, unsupervised learning and the combination of these learning types, which is called hybrid DL. The common DL algorithms used for IDS in IoT is shown in (Figure 4):

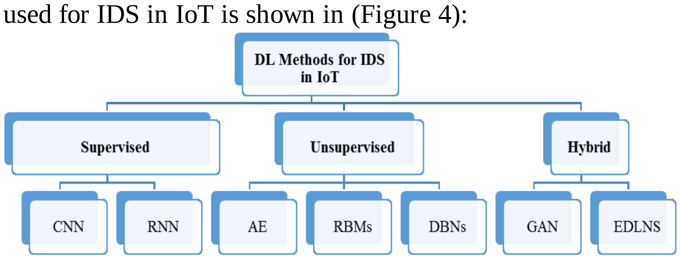

Figure 4: Classification of Deep learning methods

The following table 2 presents the Comparison of various deep learning models discussed above.

Table 2: Comparison of various deep learning models

Algorithms	Functions	Advantages	Disadvanta-ges
Convolution-al neural networks (CNNs)	Feature extraction; Classificat-ion	With CNN the handcrafted feature extraction is not necessary.	Great computational cost; so, executing them on resource-con-strained devices is challenging.
Restricted Boltzmann machines (RBMs)	Feature extraction; Feature reduction; Denoising Training.	many vital features can be extracted using an RBM feedback mechanism	
Deep belief networks (DBNs)	Feature extraction; Classificat-ion	They are trained with unlabeled data in an iterative way for a significant illustration of the features.	
AutoEncoder (AEs)	Feature extraction; Feature reduction; Denoising Training	Useful for reducing dimensionality without prior knowledge of the data. And for automatic feature learning.	Consumes considerable computing time.
Recurrent neural networks (RNNs)	Feature extraction; Classificat-ion	Powerful for sequential data at input. So useful for IoT security if the data is sequential.	The problem with exploding gradients.
Generative adversarial networks (GANs)	Data augmentat-ion; Adversarial training	The GAN does not need any stochastic process, and it can keep its adjustment after equilibrium has been reached, and it can be formed even with missing data.	It is difficult to find the balance between the Generator and the Discriminator.

5. FUTURE DIRECTIONS

5.1 Intrusion detection as a service of Fog Computing.

Fog Computing is seen as an alternative to traditional Cloud Computing, in which the various Cloud Computing services are not provided by remote data centers, but by local machines that are under the control of the local network operator[33]W. Implementing IDS at the edge for IoT security can reduce delays, realize near-real-time detection systems, improve energy efficiency and enhance scalability of IoT thin objects.

Such an implementation can provide an efficient framework for data processing with reduced network traffic load [34].
The integration of IDSs on Fog Computing platforms is therefore a promising area of research for the future. The functionality of IDSs can then be offered as services.

5.2 Zero-day attacks,

From day to day, the "zero-day" type of attacks are increasing, threatening the IoT. IDSs based on traditional methods such as anomalies or signatures fail to detect this type of attack, while those based on learning methods can handle them, which is the main advantage of these IDSs.
Zero-day attacks are metamorphic threats that automatically reprogram themselves each time they circulate or are transmitted. Therefore, it is difficult to detect them by traditional methods [35].Therefore, IDSs capable of detecting zero-day attacks in IoT networks need to be developed.

6. CONCLUSION

Despite the evolution of the Internet of Things, its security must be taken into account with more sincerity. However, the resources of IoT devices are limited, and IDSs are among the most suitable security tools for this situation.
In this paper, we have presented a literature review on IDS research for IoT networks. In this analysis, we used a division based on features such as placement strategy, detection method and implementation. We focused on the techniques used to develop IDS, in particular classical and learning methods.
We concluded that IDS research in the field of IoT is still in its infancy. Existing work does not cover a large number of IoT technologies and cannot detect a wide variety of attacks.

REFERENCES

[1] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, **"A vision of IoT: Applications, challenges, and opportunities with China Perspective,"** *IEEE Internet of Things Journal*. 2014.

[2] S. Li, L. Da Xu, and S. Zhao, **"The internet of things: a survey,"** *Inf. Syst. Front.*, 2015.

[3] M. M. Patel and A. Aggarwal, **"Security attacks in wireless sensor networks: A survey,"** in *2013 International Conference on Intelligent Systems and Signal Processing, ISSP 2013*, 2013.

[4] L. Clemmer, **"Information Security Concepts: Authenticity."** [Online]. Available: http://www.brighthub.com/computing/smb-security/articles/31234.aspx.

[5] . K. and R. Khan, **"Review on Network Security and Cryptography,"** *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 8, no. 6, p. 21, 2018.

[6] M. V. U. Chezhian, D. Ramar, and M. Z. U. Khan, **"Security Requirements in Mobile Ad Hoc Networks,"** *nternational J. Adv. Res. Comput. Commun. Eng.*, vol. 1, no. 2, 2012.

[7] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, **and Open Problems in the Internet of Things,"** in *Proceedings - 2015 IEEE World Congress on Services, SERVICES 2015*, 2015.

[8] A. Anand, **"An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols,"** *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, 2012.

[9] N. A. Alrajeh, S. Khan, and B. Shams, **"Intrusion detection systems in wireless sensor networks: A review,"** *International Journal of Distributed Sensor Networks*. 2013.

[10] Y. Zhang, W. Lee, and Y. A. Huang, **"Intrusion detection techniques for mobile wireless networks,"** *Wirel. Networks*, 2003.

[11] A. S. Ashoor and S. Gore, **"Importance of Intrusion Detection System (IDS),"** *Int. J. Sci. Eng. Res. 2011*, 2011.

[12] J. Pacheco and S. Hariri, **"IoT security framework for smart cyber infrastructures,"** in *Proceedings - IEEE 1st International Workshops on Foundations and Applications of Self-Systems, FAS-W 2016*, 2016.

[13] N. Maharaj and P. Khanna, **"A Comparative Analysis of Different Classification Techniques for Intrusion Detection System,"** *Int. J. Comput. Appl.*, 2014.

[14] K. Scarfone and P. Mell, **"Guide to Intrusion Detection and Prevention Systems (IDPS),"** *Natl. Inst. Stand. Technol.*, 2007.

[15] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han, and L. Shu, **"Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks,"** in *2014 IEEE International Conference on Communications, ICC 2014*, 2014.

[16] E. J. Cho, J. H. Kim, and C. S. Hong, **"Attack model and detection scheme for botnet on 6LoWPAN,"** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5787 LNCS, pp. 515–518, 2009.

[17] A. Bamou, M. Khardioui, M. D. El Ouadghiri, and B. Aghoutane, **"Implementing and Evaluating an Intrusion Detection System for Denial of Service Attacks in IoT Environments,"** in *Lecture Notes in Networks and Systems*, 2020.

[18] D. H. Summerville, K. M. Zach, and Y. Chen, **"Ultra-lightweight deep packet anomaly detection for Internet of Things devices,"** in *2015 IEEE 34th International Performance Computing and Communications Conference, IPCCC 2015*, 2016.

[19] P. Pongle and G. Chavan, **"Real Time Intrusion and Wormhole Attack Detection in Internet of Things,"** *Int. J. Comput. Appl.*, 2015.

[20] I. Butun, S. D. Morgera, and R. Sankar, **"A survey of intrusion detection systems in wireless sensor networks,"** *IEEE Commun. Surv. Tutorials*, 2014.

[21] A. Mishra, K. Nadkarni, and A. Patcha, **"Intrusion Detection in Wireless Ad Hoc Networks,"** *IEEE Wireless Communications*. 2004.

[22] A. Le, J. Loo, Y. Luo, and A. Lasebae, **"Specification-based IDS for securing RPL from topology attacks,"** *IFIP Wirel. Days*, vol. 1, no. 1, pp. 4–6, 2011.

[23] W. Ikram, S. Petersen, P. Orten, and N. F. Thornhill, **"Adaptive multi-channel transmission power control for industrial wireless instrumentation,"** *IEEE Trans. Ind. Informatics*, 2014. https://doi.org/10.1109/TII.2014.2310594

[24] K. Wang, Y. Shao, L. Shu, G. Han, and C. Zhu, **"LDPA: A local data processing architecture in ambient assisted living communications,"** *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 56–63, 2015.

[25] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, **"Network Intrusion Detection for IoT Security Based on Learning Techniques,"** *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[26] K. Kim, M. E. Aminanto, and H. C. Tanuwidjaja, ***SPRINGER BRIEFS ON Network Intrusion Detection using Deep Learning A Feature Learning***. 2018.

[27] W. N. Hussein, L. M. Kamarudin, H. N. Hussain, N. A. Ishak, A. Zakaria, and K. J. Jadaa, **"Discovering the Implementation Success Factors for IoT and Big Data Analytics in Transportation System,"** in *IOP Conference Series: Materials Science and Engineering*, 2019.

[28] N. Chandra Sekhar Reddy, P. C. R. Vemuri, and A. Govardhan, **"An implementation of novel feature subset selection algorithm for IDS in mobile networks,"** *Int. J. Adv. Trends Comput. Sci. Eng.*, 2019.

[29] H. Bostani and M. Sheikhan, **"Modification of supervised OPF-based intrusion detection systems using unsupervised learning and social network concept,"** *Pattern Recognit.*, 2017.

[30] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, **"Network Intrusion Detection for IoT Security Based on Learning Techniques,"** *IEEE Commun. Surv. Tutorials*, 2019.

[31] H. Liu and B. Lang, **"Machine learning and deep learning methods for intrusion detection systems: A survey,"** *Appl. Sci.*, vol. 9, no. 20, 2019.

[32] J. Bassey, D. Adesina, X. Li, L. Qian, A. Aved, and T. Kroecker, **"Intrusion detection for IoT devices based on RF fingerprinting using deep learning,"** *2019 4th Int. Conf. Fog Mob. Edge Comput. FMEC 2019*, pp. 98–104, 2019.

[33] S. Byun, **"Gateway-based resource control for reliable iot environments,"** *Int. J. Adv. Trends Comput. Sci. Eng.*, 2019. https://doi.org/10.30534/ijatcse/2019/11852019

[34] H. Li, K. Ota, and M. Dong, **"Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing,"** *IEEE Netw.*, vol. 32, no. 1, pp. 96–101, 2018.

[35] P. M. Comar, L. Liu, S. Saha, P. N. Tan, and A. Nucci, **"Combining supervised and unsupervised learning for zero-day malware detection,"** *Proc. - IEEE INFOCOM*, pp. 2022–2030, 2013.