An Innovative Intrusion Detection System model aimed at Drone Nodes Networks threatened by DoS attacks

Eddy A. POLA-JIMENEZ
Computer science department, TecNM/CENIDET
Cuernavaca, Morelos 62490, México

Dr. Máximo LÓPEZ-SÁNCHEZ
Computer Science Department, TecNM/CENIDET. **(Corresponding author)**.
Cuernavaca, Morelos 62490, México

Dr. J. Gabriel GONZÁLEZ-SERNA
Computer Science Department, TecNM/CENIDET
Cuernavaca, Morelos 62490, México

Dr. Nimrod GONZÁLEZ-FRANCO
Computer Science Department, TecNM/CENIDET
Cuernavaca, Morelos 62490, México

Dr. Dante MÚJICA-VARGAS
Computer Science Department, TecNM/CENIDET
Cuernavaca, Morelos 62490, México

Dr. Guillermo SANTAMARÍA-BONFIL
Information Technology Management, Instituto Nacional de Electricidad y Energías Limpias
Cuernavaca, Morelos 62490, México

ABSTRACT[1]

A very important branch of IoT is ad-hoc mobile networks, where sensor networks move in a given space and have been created to operate without a specialized infrastructure. However, there is a branch of this technology that involves unmanned vehicles, and can be divided into two sub-branches: Vehicle Ad-hoc Networks and Flying Vehicle Ad-hoc Networks. There, end node security becomes paramount. This paper´s objective proposes detection time as a metric to measure the impact that a Denial-of-Service, (DoS), attack could have, even with an Intrusion Detection System, (IDS), operating on the network. Furthermore, the importance of developing an IDS that revolves around false positives, and how this could affect the entire network system is emphasized. Likewise, a model is proposed and described to detect DoS attacks from the security approach of the end node, whereas, instead of starting to track the attack, the supposed node being attacked is secured, protecting it without interrupting its operations and subsequently confirming the attack to be identified. In the future, we intend to explain the correlation between time detection and security.

Keywords—IoT; Intruder Detection System; machine learning; drone networks; safety before detection**.**

1. INTRODUCTION

Internet of Things (IoT) is defined as intelligent objects to perform particular tasks whilst interconnected to the internet, in so doing, they can share their resources, be managed or even monitored [1]. It is said that it is easy to obtain at least one IoT device per person, thanks to the affordable accessibility they offer, additionally, providing the user with a quick adaptation to use it.

The authors in [24] describe an exponential growth of interconnected IoT devices in Mexico, but figures are significantly high when taking into account the world around them. According to the author in [25], there were about 20.35 billion interconnected IoT devices in 2017 and a projection to date of 35.82 billion.

However, CISCO warns in [26] about sophistication levels and malware impact rendering. Cloud services and other legitimate technologies are increasingly being used as weapons to carry out cyberattacks. Many of these exploited

[1] Acknowledgement to my peer-editor Ing. Raymond A. Jones, freelance translator and native speaker of British English, for his support in the translation, revision and correction of this document. Contact: centralseac@gmail.com

vulnerabilities used by adversaries come from IoT expansion, and its use with cloud services.

Table I. A review of pragmatic researches about IoT vulnerabilities in different application contexts.

Work	Year	Type	Regarding Vulnerabilities
[27]	2019	Journal	Exposing a taxonomy of IoT attacks. Exposing security schemes on IoT. Explaining IoT trending topics for cybersecurity research.
[28]	2018	Conference	Pragmatic exposition of vulnerabilities in an IoT device within a Bring Your Own Device, (BYOD), paradigm. Tests in a user case show, that it is possible to damage a network by taking an infected smartwatch from home to work.
[29]	2017	Journal	Expose a (2015) database with registered attacks on IoT. Pragmatic vulnerability exposure on domestic IoT devices. Vulnerability tests within a Smart Metering user case with SQL and DoS injection.
[30]	2017	Magazine	Two real case presentations where DDoS attacks in 2016 reached speeds of up to 620 gbps. Botnet behavior exposure, that causes a DDoS attack. A report with more than 493,000 Mirai malware variations.
[31]	2017	Conference	This work analyses text data transmission as a clear case for use in medical IoT. Four cases were studied where sensitive information about patients was leaked.
[32]	2017	Document	Document put together by MIT which states that even rooted smartphones could be victims of personal information theft or could even be exposed to DoS attacks.
[33]	2018	Journal	This work highlights different threats for cyber-physical systems, and sensor networks, among others. It shows a comprehensive range where attacks and effects, and defensive and aggressive detection methods are displayed.

This paper presents a state-of-the-art and raises an IoT security problem focusing on Ad-hoc Mobile Networks (MANET), more specifically, a specialized MANET, as Flying Ad-hoc Networks (FANET). This process involves machine learning and attacks at network level. We have found that false positives presented in current works may present a real risk to nodes operating legitimately on an IoT network, and that detection time could play a fundamental role in real-time attacks, such as denial of service, (DoS).

Subsequently, ZigBee drone networks and DoS attacks are taken as a referential framework and a model is proposed to detect such attacks without affecting the attacked node, or the detection time as being a determining factor in this action. This proposed model is focused on detecting an anomaly in a specific node, protecting it from attack consequences without interrupting its operation, then later, specify if an attack is being carried out, as well as identifying it. The intrusion prevention section is not within this article´s scope, it is only mentioned on an illustrative basis.

2. STATE-OF-THE-ART

IoT Vulnerabilities and Costs

Table II. Cost of some attacks recorded in Mexico.

Sinister	Average cost in USD
Data Loss (up to 2 TB)	$1,057,593.00 [8]
Inactivity (every 20 hours)	$352,531.00 [8]
Phishing (per year)	$7,500,000.00* [9]
Identity theft (per year)	$126,000,000.00* [10]
Information theft (up to 100 thousand records)	$3,860,000.00 [11]
Ransomware	$133,000.00 [12]
Malware in general	$2,500,000.00 [13]

*Considering money exchange of 1 USD = 20.00 MXN

It is impending to talk about a need for IoT device security. Regardless of context or application, it has been shown that even smartphones can fall victim to data theft or even DoS attacks if the necessary conditions present themselves. Table I shows a collection of works presenting different IoT device vulnerabilities within different contexts.

In addition to the above-mentioned table, it is common place to find high impact factor journals that list, catalogue, and expose attacks concerning IoT. For example, in [2-7] they gather enough theoretical information about the attacks found for IoT.

Table II shows an investigation carried out by journalistic experts on the monetary cost of historically

recorded attacks. It focusses on Mexico, which is within the top 5 countries with the highest IoT adoption in Latin America, and which is also one of which suffers the most cyber-attacks.

Intrusion Detection Systems

Table III. Works about intrusion identification using machine learning techniques on IoT.

Work	Technique/ method	Commu-nication Protocol	Attacks addressed
[14]	Yes, but not specified	WSN	N/E
[15]	Forecasting + Chaos theory	WSN emulation	-DoS flooding attacks. -Low-rate denial of service (LDoS).
[16]	Hilbert Huang transformed + reliability assessment	Zigbee + WSN	LDoS
[17]	Naive Bayes, Bayesian networks, J48, Zero R, One Zero, simple logistic, SVM, Perceptron multi-layer, RF	WiFi + ZigBee	-Scanning attacks. -DoS/DDoS. -MITM. -Replay. -ARP y DNS spoofing
[18]	Proposed SVM, GA-SVM, A-IDS, WPS-IDS	Emulation	-DDoS
[19]	Random Forest, Linear SVM, Multinomial	Emulation	-DoS -Probe -R2L -U2R
[36]	Optimum-Path Forest, Clustering, SA-IDSs	RPL emulation with 6LowPAN	-Wormhole attack -Sinkhole attack -Rank attacks
[20]	N/A	RPL	-Sinkhole -Selective forwarding
[21]	Random Neural Networks	RF + WiFi + ZB + Bluetooth	-TCP SYN Attacks. -UDP flooding. -Sleep deprivation attack. -Broadcast attacks.
[22]	Non-symmetric Deep auto-encoder + Random Forest	Dataset	-DoS -Probe -R2L -U2R
[23]	Rough Set + SVM + Principal component analysis	Dataset	-DoS -U2R -R2L -Probing
[37]	Deep learning (Keras on Theano)	Cloud computing emulation	-DoS -Probe -R2LU2R
[34]	Based on SVM + signatures	N/A	DoS

An Intrusion Detection System, (IDS), is used in the research field to talk about techniques, algorithms or methods that identify malicious actions in cyberspace and often even in physics.

The different reviewed papers in this section are specifically directed towards the IoT threatened by cyberattacks where DoS prevails, and that, except for [20], are identified for machine learning techniques. These are summarized in Table III.

The proposal by the author in [14] is a way to perform intrusion detection from the service provider side. This task becomes important when the need for low resource consumption of the IoT end devices arises.

The author in [15] proposed a statistical method that estimates the chaotic variable changes in time series. The tests carried out in this paper were made through the emulation of static nodes, where the used communication protocol was not mentioned.

In [16], authors carried out an analysis of non-linear signals using the Hilbert Huang transform, by decomposing the network traffic in frequencies over time. The reliability assessment is combined to this to obtain the real components. The authors used static nodes Zigbee CC2530 SoC as end devices for their tests.

For their part, authors in [17] propose a 3-part architecture to carry out intrusion detection. In the first layer, data is collected, in the second, a first analysis is made to recognize and separate malicious from harmless patterns. In the last layer, the attack that is taking place is precise. Most of the shallow learning algorithms are used to evaluate a simulated network by ZigBee static nodes. The work was evaluated against 5 different attacks.

The work in [18] modified and created an algorithm for intrusion detection using a Support Vector Machine (SVM). Tests were carried out on a ZigBee static nodes emulation with NS-3 and the results compared with other

works that used SVM. DoS was the only attack investigated and evaluated in this paper.

Author in [19] used 3 shallow learning techniques for intrusion detection. The tests were done on a network behavior emulation with the NSL-KDD dataset.

The authors in [20] presented SVELTE, an anomaly detection system for traffic routes of an IoT network. Apart from performing tests in a real environment, this is one of the first intrusion detection systems that consider low consumption resources in end devices.

In [21], authors developed a paper to address some variations of DoS attacks. The tests were performed on a homogeneous network involving IoT protocols such as ZigBee, Bluetooth, RF869 and Wi-Fi. Additionally, they built their own data set to apply a neural network-based detection algorithm.

The authors in [22] proposed a deep and shallow learning combination model that is capable of analyzing a wide range of network traffic. The combined techniques used were the Non-Symmetrical Deep Auto Encoder, (NDAE), and the Random Forest Algorithm, (Random Forest). KDD Cup variant datasets were used in their tests.

The work in [23] was done by developing an intrusion detection methodology on a KD99 dataset, this means that all tests were not performed in real time or over an IoT network. Additionally, they registered the methodology detection rate through the use of major component analysis and applied security methods such as secure routing and access control.

Authors in [36] developed an intrusion detection system to route attacks such as wormhole, sinkhole and node sorting attacks. The algorithm is based on statistical analysis and decision-tree clusters of decision-making of the topology used.

The work in [37] develops a deep learning architecture to implement an Intruder Detection System that detects DoS attacks. It was not tested in simulated or real environments, with the NSL-KDD data set being the source of training and test work.

3. APPROACH TO THE PROBLEM

One of our most important research questions showed the following: How much would inactivity caused by DoS in Zigbee networks cost, more specifically, in VANET's or FANET's? If we analyze table II, we found that every 20 hours of inactivity costs up to $350,000.00 USD. DoS has been always been the cause of this loss and has become so threatening that it is probably the most studied attack on IoT.

Present research suggests the question: how probable is the aforementioned scenario? In their paper, the authors in [15] present a testbench that, when detecting DoS where the final damage is done after one minute of being started, the end node is left collapsed. Although this testbench was developed in a simulated and controlled environment, in a Smart Home context, and with a 100 Mbps bandwidth, authors note that in a real case this would take between 8 and 10 minutes to present the same result. ZigBee has a bandwidth of up to 1 Mbps, theoretically, each node is easier to harm with DoS.

The state-of-the-art section outlines a high detection rate and evaluation to developed models in reviewed papers. However, when facing a so aggressive attack like DoS it is necessary to ask: how long does an IDS take to find a DoS attack since it was started? We consider this question important if the following is analyzed to size the problem: According to [38], in the first quarter of 2020, Amazon® billed 75 billion dollars with its online sales globally. If a DoS attack was launched against its servers and the IDS found the problem after an hour of inactivity on the servers, it could have a cost of up to 26 million dollars.

Authors in [17] and [18] did the only works in 'the state-of-the-art' section that they included a training time, a testing time and a total time in their result analysis. However, they don't specify either the damage to end nodes during the course of an attack, neither the time it takes to realize an intrusion detection.

Another question is related to false positive rates of up to 60% in the state-of-the-art study, creating a new research question: How do false positive rates impact the network? Having this information would warn about risks and complications of deploying an intrusion detection system with a high false positive rate and would lead to the development of new models attempting to reduce this.

Referencing Wikipedia, a false positive means that an IDS classifies a file, node, device, traffic, etc., as malicious, and then, an intrusion prevention system (IPS) proceeds to apply a set of rules necessary to secure the network. Due of this principle, Microsoft®, CISCO®, SNORT®, among others, introduce ways of reducing false positives on their respective defense systems [41, 42]. Accordingly, false positives could negatively impact the traffic in a network, nodes or devices, programs, etc., all this according to the detection system approach developed. For example, [15] analyses data traffic for detecting anomalies. If this is the case, rules incorrectly applied due to false positives would affect legitimate packet frames. Another example is in [17] where an IDS for traffic was developed, where an intrusion would result on applying rules to the source attacking node. If false positives, benign nodes could be affected by an IPS.

4. PROPOSED MODEL

On careful analysis of table III, we found that, with the exception of [34], all documents are deployed over a hierarchical topology, which is typical for industry 4.0 or Smart Home, but not for Zigbee. This is not inherent of Zigbee and its different applications such as MANET, FANET, VANET, etc., where topology opens dynamically and the environment becomes distributed. For this reason, we have decided to concentrate on static VANET's, ensuring that the present paper revolves around Zigbee with

a distributed environment. Although our future work is to take care of false positive rates, this submission is to solve the detection time problem first. Also, this work is designed for DoS attacks by flooding.

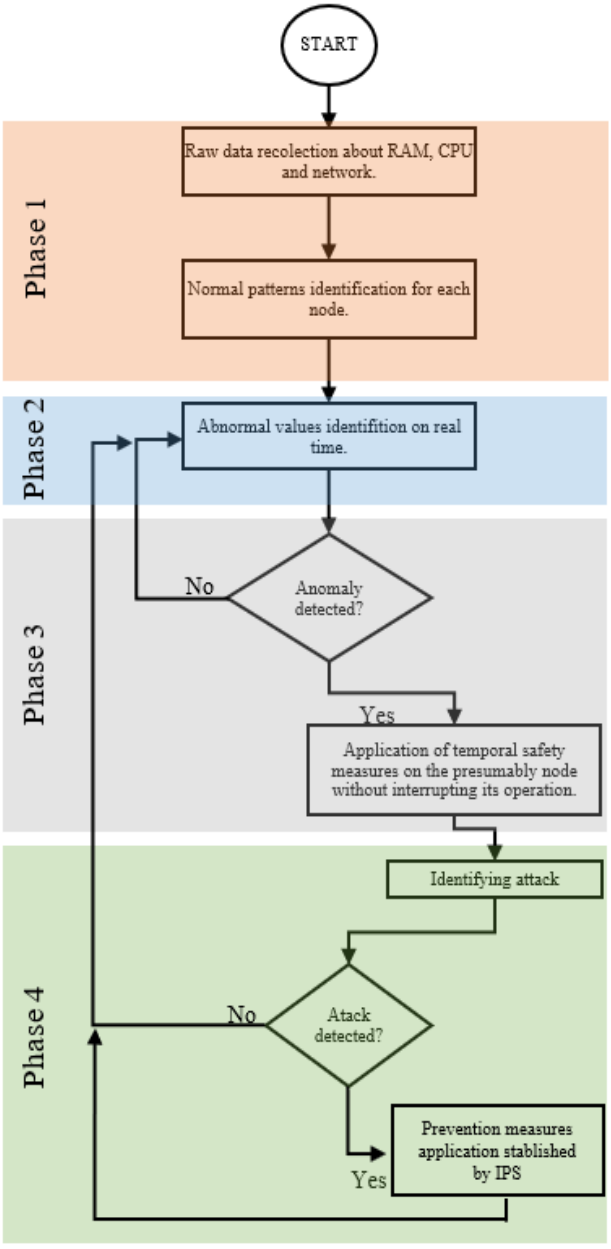

Diagram 1. Flow chart of our proposed model divided in four phases.

Deep Learning vs SVM

Deep learning with neuronal networks has proven to be a well evaluated technique, considering identification. However, papers in the state-of-art part have shown that these same techniques presented a high false positive rate. On the other hand, support machine vector techniques, (SVM), showed considerably low false positive rates without having an excellent performance in identification as neuronal networks. Thanks to these advantages, most recent papers have merged combining shallow learning with deep learning to obtain better results. This is the path to follow with this paper.

Architecture and Detection Approach

Our designed architecture comprises of 4 phases to identifying attacks and securing final nodes:

Phase 1. Profiling network devices to determine normal patterns in their behavior. Take network load measures from every node to determine a normal state. CPU/RAM loads are also taken for end devices that simulate a drone.

Phase 2. Detecting faults in real time. This phase involves training and testing of two machine learning algorithms: SVM and Neural based Networks. Input data are variables suggested in [35], later, CPU and RAM data will be added as input. The launched alert will not determine if it is exactly a DoS attack, (e.g., a false positive).

Phase 3. Applying rules designed to put the end node on an invulnerable state while a potential attack is confirmed. If an alert was launched, according to information, the IDS could determine the supposed affected node and apply a temporary rule for securing it, this could imply protocols related to virtual networks in real time.

Phase 4. Identifying the attack that is being carried out. Almost at the time the affected node is secured, the IDS will determinate exactly what attack is being carried out.

Notice that instead of detecting the source of the attack by analyzing network traffic as in every paper done, this paper proposes to analyze the attacked end node, secure it and detect, in parallel, the corresponding attack to apply the necessaries rules.

Proposed Variables

Knowing that a distributed topology is used, we propose to use a node to carry out data collection based on queries. Data collection considers network variables and two key variables for our proposed approach: CPU and RAM variables. These variables are inherent on machines as drones and are also affected when a DoS attack is carried out.

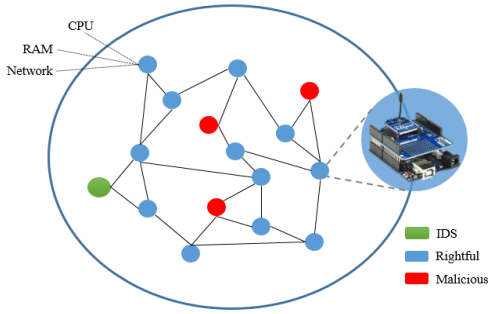

Diagram 2. A representation of nodes using a distributed topology.

In figure 1 a nodes distribution and its roles are shown. We have collected Arduino boards to simulate the

processing part of a drone and we have built-in Digi Xbee module for ZigBee communication. For data collection and processing, we will use an NVIDIA Jetson Nano tx2.

Dataset

Throughout the state-of-the-art, we see those important publications, that were developed based on a real environment, used up eight end nodes of which one to three end nodes are set as malicious nodes. This is to probe their contributions. For this paper, 15 end nodes will be used to test our model. A dataset can be collected with these nodes and from there, we can work on training and tests.

We have decided not to use existing datasets like NSL-KDD or KDD cup'99 because some papers in 'state-of-the-art' have mentioned that they are not made with IoT devices.

5. CONCLUSION AND FUTURE WORK

There are many metrics to artificially take performance measurements provided by intelligence. These metrics have been a very helpful benchmark if someone wants to choose an intrusion detection system based on specific benefits. However, despite the very good performance shown by many algorithms, we consider that detection time could be another great metric which would show if there were collateral damage on attacked devices. Adding to that, we also consider that false positive rates could have a negative impact on benign end devices and that could be vital in a drone's network. This way, we conclude that security must focus on safety devices when an indication of an anomaly has been provided by IDS, even before applying rules from an IPS.

Analyzing every node in the network, we estimate that obtaining data about CPU/RAM load would provide us with enough information to develop a profiling given by IA and detect when a node is suffering a fault. Then, we can achieve the aforementioned goal.

In our future work, we will implement two detection systems based on SVM and Neural Networks. Further on, we will test every IDS in real time, measuring when a DoS attack was detected and how long the aforementioned attacks were active. If possible, we could determine how much time the attacked device was offline correlating with the detection time of its corresponding attack. Then, we will design and implement our model where there is no collateral damage despite a DoS attack. And finally, we aim to develop an Intrusion Detection and Prevention System, (IDPS), based on the excellent accuracy shown by IA algorithms but focused on reducing False Positive Rates, (FPR).

6. ACKNOWLEDGEMENTS

Thanks to the Consejo Nacional de Ciencia y Tecnología, (CONACyT), the Tecnológico Nacional de México and the Centro Nacional de Investigación y Desarrollo Tecnológico, (CENIDET), who through the project entitled "Identificación de alteraciones en el iris del ojo para detectar patrones que permitan medir si existe correlación con personas diagnosticadas con diabetes mellitus" and which carries the number 10437.20-P, have supported current, as well as future work.

7. BIBLIOGRAPHY

[1] K. K. Goyal, A. Garg, A. Rastogi y S. Singhal, «A Literature Survey on Internet of Things (IoT),» *Int. J. Advanced Networking and Applications,* vol. 09, nº 0975-0290, pp. 3663-3668, 2018.

[2] J. Deogirikar y A. Vidhate, «Security Attacks inIoT: A Survey,» de *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2017.

[3] S. Benzarti, B. Triki y O. Korbaa, «A Survey on Attacks in Internet of Things,» de *2017 International Conference on Engineering & MIS (ICEMIS)*, Monastir, Tunisia, 2017.

[4] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray y Y. Jin, «Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice,» *Journal of Hardware and Systems Security,* vol. 2, p. 97–110, 2018.

[5] F. A. Alaba, M. Othman, I. A. T. Hashem y F. Alotaibi, «Internet of Things security: A survey,» *Journal of Network and Computer Applications,* vol. 88, pp. 10-28, 15 Junio 2017.

[6] H. HaddadPajouh, R. Parizi, A. Dehghantanha, M. Aledhari y H. Karimipour, «A Survey on Internet of Things Security: Requirements, Challenges, and Solutions,» *Internet of Things,* nº 100129, 2019.

[7] P. Williams, P. Rojas y M. Bayoumi, «Security Taxonomy in IoT – A Survey,» de *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*, Dallas, Tx, USA, 2019.

[8] R. Riquelme, «Pérdida de datos le cuesta a una empresa en México más de 1 millón de dólares: DELL EMC,» 10 Abril 2019. [En línea]. Available: https://www.eleconomista.com.mx/tecnologia/Perdida-de-datos-le-cuesta-a-una-empresa-en-Mexico-mas-de-1-millon-de-dolares-DELL-EMC-20190410-0079.html.

[9] G. Chávez, «Phishing cuesta a la banca mexicana 150 millones de pesos,» 23 Octubre 2017. [En línea]. Available: https://expansion.mx/tecnologia/2017/10/23/phishing-cuesta-a-la-banca-mexicana-150-millones-de-pesos. [Último acceso: 20 Agosto 2019].

[10] Go socket, «EL ROBO DE IDENTIDAD COSTÓ 118 MILLONES DE PESOS,» [En línea]. Available: http://iofacturo.mx/economia/el-robo-de-identidad-costo-118-millones-de-pesos. [Último acceso: 28 Agosto 2019].

[11] Computer World México, «Costos ocultos de las brechas de datos aumentan los gastos para las empresas,» 2018. [En línea]. Available: http://computerworldmexico.com.mx/costos-ocultos-de-las-brechas-de-datos-aumentan-los-gastos-para-las-empresas/. [Último acceso: 15 Agosto 2019].

[12] J. C. Wong y O. Solon, «Massive ransomware cyber-attack hits nearly 100 countries around the world,» 12 Mayo 2017. [En línea]. Available: https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs. [Último acceso: 15 Agosto 2019].

[13] D. Remírez, «Ataques de malware pueden costarle hasta 2.5 mdd a las empresas,» 06 Junio 2018. [En línea]. Available: https://www.forbes.com.mx/ataques-de-malware-pueden-costarle-hasta-2-5-mdd-a-las-empresas/. [Último acceso: 21 Agosto 2019].

[14] M. Gajewski, J. M. Batalla, G. Mastorakis y C. X. Mavromoustakis, «A distributed IDS architecture model for Smart Home systems,» *Cluster Computing*, vol. 22, p. 1739–1749, 2019.

[15] A. Procopiou, N. Komninos y C. Douligeris, «ForChaos: Real time application DDoS detection using Forecasting and Chaos Theory in Smart Home IoT Network,» *Wireless Communications and Mobile Computing*, vol. 2019, 3 Febrero 2019.

[16] H. Chen, C. Meng, Z. Shan, Z. Fu y B. K. Bhargava, «A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation,» *IEEE Access*, vol. 7, pp. 32853 - 32866, 08 Marzo 2019.

[17] E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos y P. Burnap, «A Supervised Intrusion Detection System for Smart Home IoT Devices,» *IEEE Internet of Things Journal*, vol. 6, pp. 9042 - 9053, 02 Julio 2019.

[18] S. U. Jan, S. Ahmed, V. Shakhov y I. Koo, «Toward a Lightweight Intrusion Detection System for the Internet of Things,» *IEEE Access (Volume: 7)*, pp. 42450 - 42471, 2019.

[19] M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas y J. Lloret, «Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT,» *Sensors*, 2017.

[20] S. Raza, L. Wallgren y T. Voigt, «SVELTE: Real-time intrusion detection in the Internet of Things,» *Ad Hoc Networks*, pp. 2661-2674, Noviembre 2013.

[21] O. Brun, Y. Yin y E. Gelenbe, «Deep Learning with Dense Random Neural Network for Detecting Attacks against IoT-connected Home Environments,» *Procedia Computer Science*, vol. 134, pp. 458 - 463, 2018.

[22] N. Shone, T. N. Ngoc, V. D. Phai y Q. Shi, «A Deep Learning Approach to Network Intrusion Detection,» *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 02, nº 1, pp. 41 - 50, 23 Enero 2018.

[23] L. Deng, D. Li, X. Yao, D. Cox y H. Wang, «Mobile Network Intrusion detection for IoT system based on transfer learning algorithm,» *Cluster Computing*, pp. 1-16, 31 Enero 2018.

[24] J. S. Onofre, «México entrará al Top 5 en AL del Internet de las cosas en 2020,» 05 Mayo 2017. [En línea]. Available: https://www.eleconomista.com.mx/tecnologia/Mexico-entrara-al-Top-5-en-AL-del-Internet-de-las-cosas-en-2020-20170505-0019.html. [Último acceso: 15 Agosto 2019].

[25] Statista Research Department, «Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025(in billions),» 2020. [En línea]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Último acceso: 2020].

[26] Cisco, «Cisco 2018 Annual Cybersecurity Report,» Cisco, 2018.

[27] Y. Lu y L. D. Xu, «Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics,» *IEEE Internet of Things Journal*, vol. 6, nº 18653874, pp. 2103 - 2115, 2019.

[28] S. Siboni, A. Shabtai y Y. Elovici, «Leaking data from enterprise networks using a compromised smartwatch device,» de *SAC '18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 2018.

[29] S. Tweneboah-Koduah, K. E. Skouby y R. Tadayoni, «Wireless Personal Communications,» *Wireless Personal Communications*, p. 169–185, 2017.

[30] C. Kolias, G. Kambourakis, A. Stavrou y J. Voas, «DDoS in the IoT: Mirai and Other Botnets,» *Computer*, vol. 50, nº 0018-9162, pp. 80 - 84, 2017.

[31] D. Wood, N. Apthorpe y N. Feamster, «Cleartext Data Transmissions in Consumer IoT Medical Devices,» 27 Marzo 2018. [En línea]. Available: https://arxiv.org/pdf/1803.10147.pdf.

[32] M. Ye, N. Jiang, H. Yang y Q. Yan, «ecurity analysis of Internet-of-Things: A case study of august smart lock,» de *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Atlanta, GA, USA, 2017.

[33] S. Ali, T. A. Balushi, Z. Nadir y O. K. Hussain, «WSN Security Mechanisms for CPS,» *Cyber*

Security for Cyber Physical Systems, nº 978-3-319-75879-4, pp. 65 - 87, 2018.

[34] V. Justin, N. Marathe y N. Dongre, «Hybrid IDS using SVM classifier for detecting DoS attack in MANET application,» de *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2017.

[35] K. M. A. Alheeti y K. McDonald-Maier, «Intelligent intrusion detection in external communication systems for autonomous vehicles, » Systems Science & Control Engineering, vol. 6, nº 1, pp. 48-56, 2018.

[36] A. A. Diro y N. Chilamkurti, «Distributed attack detection scheme using deep learning approach for Internet of Things,» *Future Generation Computer Systems*, vol. 82, pp. 761 - 768, 2018.

[37] Microsoft, «Solución de problemas del firewall de aplicaciones web (WAF) de Azure Application Gateway,» 14 Noviembre 2019. [En línea]. Available: https://docs.microsoft.com/es-es/azure/web-application-firewall/ag/web-application-firewall-troubleshoot. [Último acceso: 02 Agosto 2020].

[38] Statista, «Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025(in billions),» statista, 2021. [En línea]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Último acceso: 2021].