Revista UIS ingenierías
ISSN: 1657-4583
ISSN: 2145-8456
Universidad Industrial de Santander

Gutiérrez-Portela, Fernando; Almenárez-Mendoza, Florina;
Calderón-Benavides, Liliana; Romero-Riaño, Efrén

Security perspective of wireless sensor networks

Revista UIS ingenierías, vol. 20, no. 3, 2021, July-September, pp. 189-202
Universidad Industrial de Santander

DOI: https://doi.org/10.18273/revuin.v20n3-2021014

Available in: https://www.redalyc.org/articulo.oa?id=553770600014

Vol. 20, n.° 3, pp. 189-202, 2021
Revista UIS Ingenierías
Página de la revista: https://revistas.uis.edu.co/index.php/revistauisingenierias

Security perspective of wireless sensor networks

Prospectiva de seguridad de las redes de sensores inalámbricos

Fernando Gutiérrez-Portela [1], Florina Almenárez-Mendoza [2], Liliana Calderón-Benavides[3], Efrén Romero-Riaño [4]

[1] Aqua, Ingeniería Civil, Universidad Cooperativa de Colombia, Colombia.
Email: fernando.gutierrez@campusucc.edu.co. Orcid: 0000-0003-3722-3809.
[2] Aplicaciones y Servicios Telemáticos, Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid, España. Email: florina@it.uc3m.es. Orcid: 0000-0002-5232-2031.
[3] Tecnologías de Información, Unidad académica, Universidad Autónoma de Bucaramanga, Colombia.
Email: mcalderon@unab.edu.co. Orcid: 0000-0001-8658-9036.
[3] Innotec, Doctorado en Ingeniería, Universidad Autónoma de Bucaramanga, Colombia.
Email: eromero21@unab.edu.co. Orcid: 0000-0002-3627-9942.

Received: 13 October 2020. Accepted: 02 February 2021. Final version: 04 June 2021.

Abstract

In Wireless Sensor Networks (WSN), nodes are vulnerable to security attacks because they are installed in a harsh environment with limited power and memory, low processing power, and medium broadcast transmission. Therefore, identifying threats, challenges, and solutions of security and privacy is a talking topic today. This article analyzes the research work that has been carried out on the security mechanisms for the protection of WSN against threats and attacks, as well as the trends that emerge in other countries combined with future research lines. From the methodological point of view, this analysis is shown through the visualization and study of works indexed in databases such as IEEE, ACM, Scopus, and Springer, with a range of 7 years as an observation window, from 2013 to 2019. A total of 4,728 publications were obtained, with a high rate of collaboration between China and India. The research raised developments, such as advances in security principles and defense mechanisms, which have led to the design of countermeasures in intrusion detection. Finally, the results show the interest of the scientific and business community in the use of artificial intelligence and machine learning (ML) to optimize performance measurements.

Keywords: wireless sensor networks; WSN attacks; security mechanisms; artificial intelligence; intrusion detection; computational resources; countermeasures; ZigBee protocol; machine learning; supervised techniques; unsupervised techniques; anomaly detection; clustering algorithms; VOSviewer; security prospective.

Resumen

En las Redes de Sensores Inalámbricos (WSN), los nodos son vulnerables a los ataques de seguridad porque están instalados en un entorno difícil, con energía y memoria limitadas, baja capacidad de procesamiento y transmisión de difusión media; por lo tanto, identificar las amenazas, los retos y las soluciones de seguridad y privacidad es un tema candente hoy en día. En este artículo se analizan los trabajos de investigación que se han realizado sobre los mecanismos de seguridad para la protección de las WSN frente a amenazas y ataques, así como las tendencias que surgen en otros países junto con futuras líneas de investigación. Desde el punto de vista metodológico, este análisis se muestra a través de la visualización y estudio de trabajos indexados en bases de datos como IEEE, ACM, Scopus

ISSN Printed: 1657 - 4583, ISSN Online: 2145 - 8456,
How to cite: F. Gutiérrez-Portela, F. Almenárez-Mendoza, L. Calderón-Benavides, E. Romero-Riaño, “Security perspective of wireless sensor networks,” *Rev. UIS Ing.*, vol. 20, no. 3, pp. 189-202, 2021, doi: 10.18273/revuin.v20n3-2021014

y Springer, con un rango de 7 años como ventana de observación, desde 2013 hasta 2019. Se obtuvieron un total de 4.728 publicaciones, con un alto índice de colaboración entre China e India. La investigación planteó desarrollos, como avances en los principios de seguridad y mecanismos de defensa, que han llevado al diseño de contramedidas en la detección de intrusiones. Por último, los resultados muestran el interés de la comunidad científica y empresarial por el uso de la inteligencia artificial y el aprendizaje automático (ML) para optimizar las medidas de rendimiento.

Palabras clave: redes de sensores inalámbricos; ataques a las WSN; mecanismos de seguridad; inteligencia artificial; detección de intrusiones; recursos computacionales; contramedidas; protocolo ZigBee; aprendizaje automático; técnicas supervisadas; técnicas no supervisadas; detección de anomalías; algoritmos de agrupamiento; VOSviewer; principios de seguridad.

1. Introduction

Wireless sensor networks (WSN) comprise large numbers of embedded sensors and transmitter nodes. Sensors are autonomous devices with limited resources, which are employed to observe and measure a certain phenomenon. They can cooperate to monitor one or more physical phenomena within an area of interest. They can also be used in a wide range of applications such as habitat environmental monitoring, health, transportation, military surveillance, climate detection, and underwater acoustics [1].

However, deployment of WSNs in hostile and/or isolated areas [2], as well as limitation of computational resources, such as memory size, sensor battery life, and storage capacity, cause data processing and wireless communication to become crucial processes that promote efficiency and security of the system. These topics pose great challenges in terms of data reliability [3] because information circulates in real-time and users can access it directly from the sensor nodes [4]. Therefore, the protection of information becomes one of the most important aspects to be considered due to security threats [5].

Several studies [6] show the different layers of vulnerabilities and attacks to WSNs. Therefore, efforts have been made to use robust and adaptable methods for data exchange [7]. Likewise, improvements in security coverage and optimization in computing resources with lighter and more effective security mechanisms that respond to these vulnerabilities are required [8], [9]. Consequently, innovation in security countermeasures that provide a high degree of reliability, detection, and prevention against various attacks are required [4].

Therefore, the proposed study aims to present a mapping of the research that is being conducted concerning security mechanisms for the protection of WSNs against threats and attacks. Furthermore, the present study put forward the trends that emerge in other countries and future investigation lines submitted by some authors regarding the WSNs security mechanisms.

2. Background

In addition to nodes, a WSN is integrated by a set of protocols and algorithms, which allow the communication and interoperability of sensor and actuator nodes. In particular, the set of IEEE 802.15 [10], which specializes in wireless personal area networks (WPAN), has evolved to turn into one of the most widely used standards in WSNs. Since 2003, such a set of protocols are responsible for communications in different layers that make it up. Within these specifications for WSNs, the following can be highlighted: 802.15.4 that allows establishing secure communications in the physical layer with low data transmission rate and maximization of battery life; and IEEE 802.15.1 and 802.15.2 (Bluetooth) with higher data rates [11], [12].

The IEEE 802.15.4 standard broadened the foundation for machine-to-machine (M2M) communications. This communication for low-speed wireless local personal area networks (LR-WPAN) leads to the emergence of wireless technologies such as IEEE 802.15.4/ZigBee, 6LoWPAN, Z-Wave, and LoRa [13]. For example, ZigBee 3.0 has been used in a variety of applications, which also include security-critical products such as door locks and intrusion alarm systems [14], WirelessHART as an extension of HART communication protocol is fulfilling the requirements of the wireless industry [15], 6LoWPAN [16], and LoRa/LoRaWAN [17]. The latter are highly targeted to specific Internet of Things (IoT) requirements.

Moreover, the IETF IPv6 standard on low power WPAN has integrated WSNs with the internet and has established communication in an adaptation layer that has been used to transmit IPv6 through IEEE 802.15.4 networks. End-to-end communication security is using the Datagram Transport Layer Security (DTLS) security protocol that provides security for UDP-based applications [18].

Moreover, low range radio (LoRa) technology is being used thanks to the low power consumption and wide range. LoRa security is ensured through symmetric and asymmetric key cryptography, which is like DTLS. However, LoRa technology has security vulnerabilities that can be exploited by intruders [19].

Thus, fundamental elements for the design of security protocols that achieve confidentiality, authentication, and integrity allow finding a trade-off between performance and cost in networks. Even more when in recent years control mechanisms have been developed for dynamic and improved access for low power networks with limited resources that prevent intrusion of false information injection, capture and node replication, Sybil, and wormhole attacks with minimum control of messages as opposed to outputs, turning them into appropriate systems for detection of intrusions in WSNs and its applications [4].

Dynamic and improved access control mechanisms comprise a) authentication scheme based on smart cards and supported by elliptic curve cryptography (ECC) in a secure way for wireless sensor networks using user password [20]; b) secret key-based user authentication schemes for heterogeneous sensor networks (HWSN) [21] and adapted to IoT environments; c) user authentication scheme using a bilinear pairing and trusted authority, which authenticates a user and also establishes secure communication between a user and sensor node [22]; d) three-factor key authentication scheme and a suitable agreement for healthcare WSNs, which is based on multiplications of light ECC points [23]; e) two-factor user authentication scheme with decoupling between a user and sensor [24] that improve the sensor registration and user authentication phase, which allows key updating and link capacity optimization, thereby greatly reducing computational costs.

3. Technological survey results

For the elaboration of this article, an adapted survey paper approach is presented based on the combination of two disciplines: (i) bibliometrics and (ii) visualization of scientific networks. Bibliometrics is the application of quantitative tools for the study of scientific communications. The phenomenon of study is the prospective of Wireless Sensor Networks, WSN, from a perspective or "meta-model" constructed from metadata extracted from the IEEE, ACM, Scopus, and Springer databases.

The study's data universe is composed of 4728 document records. The units of analysis selected are i) documents, ii) countries, and iii) keywords. The types of analysis implemented are word and countries co-occurrence. Word co-occurrence occurs when two topics appear simultaneously in different documents, within fields such as keywords, titles, or abstracts. The variables analyzed are the structure of the networks composed by the features of co-occurrence links and the relevance of the nodes (words, documents) to the research field.

3.1. Scientific publications evolution

The degree of research importance in security mechanisms for WSNs is shown by scientific publications' evolution. Our analysis revealed that with a total of 4728 publications from 2013 to 2019 (Figure 1), the years with the highest number of scientific publications were 2015, 2016, 2017, and 2018. Moreover, interest in the subject can be observed from the fact that from the year 2019 to the date of this study (September), 473 works have already been published. Therefore, it reflects the importance of the academic and business environment.

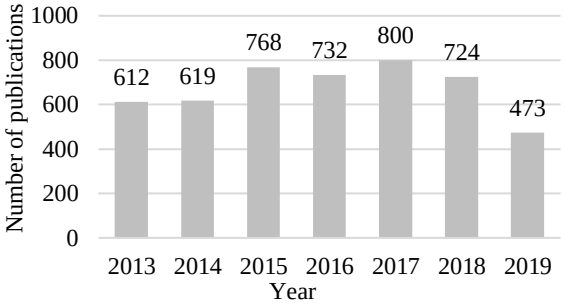

Figure 1. Scientific publications 2013–2019.

3.2. Scientific publications evolution

To identify clusters of countries leading WSN research, the results of the clustering algorithm of the VOSviewer software are used. Vosviewer identifies the similarity between units of analysis (countries, words) based on their frequency of co-occurrence within the documents [25], [26].

In that sense, the appearance of two countries in a graph with the same color reflects that author from those countries collaborates frequently [27].

The number of clusters is generated automatically by the VOSviewer algorithm using the normalization function [28]. This function compares the frequency of occurrence of a node (country, word) concerning the total occurrences of the analysed set [29], [30].

A visual graph of co-authorship networks by country can be seen in Figure 2. It is also shown that seven collaboration clusters for scientific production are present. Among the main representative countries with a high rate of collaboration are China and India, which are actively participating in the cluster with Taiwan, South Korea, Germany, Finland, France, Canada, Singapore, Spain, and the United Arab Emirates.

Moreover, the United States has a high insertion degree together with Taiwan, Morocco, Jordan, Turkey, and Italy. These two clusters are the most representative for generating a development about security mechanisms in WSNs.

4. Security principles and advances in defense mechanisms at WSNs

According to ISO/IEC 27001:2013, information security revolves around principles such as the preservation of data confidentiality, integrity, availability, and authenticity. Different security mechanisms have been designed that have allowed WSNs to process and transmit data smoothly [31], [32].

Therefore, security principles and some mechanisms in WSNs are discussed below:

DTLS protocol in wireless sensor-based networks has been suggested for data confidentiality and integrity to protect end-to-end communication between nodes.

Furthermore, security mechanisms have been developed for the establishment of random distribution of keys, trust settings, encryption schemes, and access control, and hash functions, and digital signature [33]. Studies [34] propose a hybrid key redistribution scheme (HKP-HD), which uses a hash chain based on the maximum value of an attack coefficient, to prevent an adversary from being able to extract keys cryptographic or group keys.

A WSN lightweight node protocol in TinyOS is proposed for node authentication and identification and generation of secret keys, which plays a fundamental role in guaranteeing authentication [35].

As regards the availability, security mechanisms have been proposed, such as intrusion detection systems and authentication schemes, to prevent flood attacks, interference, repetition, selective forwarding, among several others [33], [34], [6].

As regards privacy preservation in WSNs, end-to-end encryption mechanisms have been put forward for each message transmitted, symmetric key homomorphic encryption functions, time reports, cryptographic pseudonyms, and data mining with privacy recognition [36].

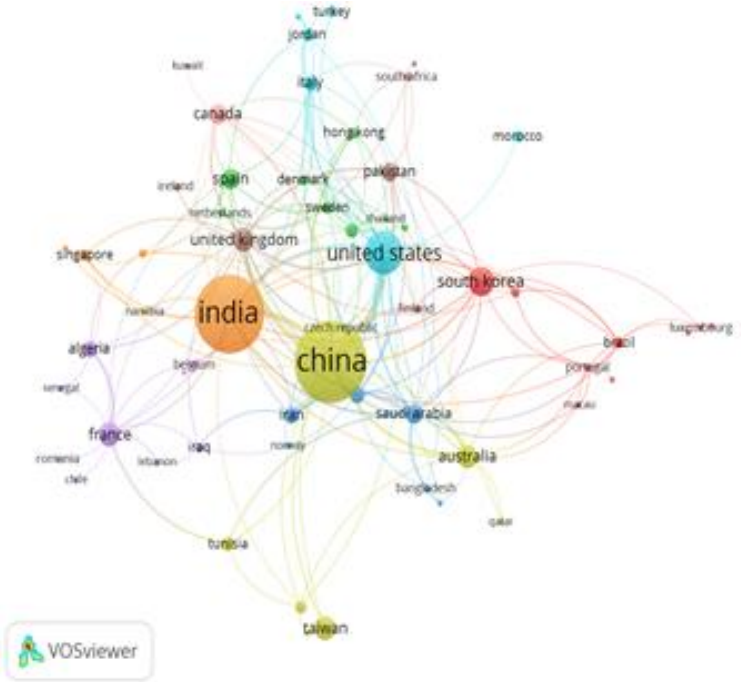

Figure 2. Visual graph of co-authorship networks.

4.1. Countermeasures against attacks

4.1.1. Flood attack

They appear in different layers of WSNs where a malicious node continuously sends data packages to a target, thereby exhausting node available resources. Attacks have been identified as denial of service (DoS) route-based and sleep deprivation attacks, which are performed at the application layer and routing layer, respectively. As an answer to this threat, a hybrid intrusion detection systems (IDS) model has been designed comprising a central agent that runs on the server and performs intensive calculations using received "alerts" [37]. As a countermeasure in a hybrid DoS attack, an energy trust-based intrusion detection method has been developed for WSNs, which predicts power consumption and increases consumption correlation calculation, thereby evaluating the security status of nodes [38].

4.1.2. Information leak/traffic capture

In traffic analysis attack events, where an intruder tries to learn the behavior of traffic, network, and nodes, patterns of a message, its length, and duration that the message remains at the central node are examined. Conversely, in advanced attack events such as controllable event triggering attack (CETA) and random event triggering attack (RETA), a collection scheme has been designed that exploit functions homomorphic encryption on efficient data collection, which makes traffic analysis and data flow tracking impossible, preserving privacy, the intractability of package flow, and confidentiality of message content [39].

As a defense strategy, three secure data aggregation schemes were deployed: a) multifunctional data aggregation scheme, b) selected random encryption based on data aggregation, and c) data aggregation based on compression [40].

By affecting data aggregation, amounts of communication and power consumption are significantly reduced [41]. Therefore, an aggregation framework called "Synoptic Diffusion" was developed, which combines multipath routing schemes with lightweight verification algorithms, whereby a base station can determine if a computed aggregate includes false information [42].

4.1.3. Constant interference attacks

The problem was addressed using the frequency hopping technique. The objective was to find an optimal frequency based on the optimal decision rule, which considers all inherent nodes' individual decision profiles for the overall well-being of a network [43].

4.1.4. Selective forwarding

Studies [44] presented a light countermeasure as regards a selective forwarding attack where a single randomly selected checkpoint node was proposed to detect the misbehavior of forwarding a malicious node. This countermeasure integrates time-delay and hop-by-hop retransmission techniques to quickly recover unexpected package losses due to forwarding misbehavior or poor channel quality.

4.1.5. Identity fraud

Phishing attacks and Sybil attacks have been analyzed by different authors [33], [45], [3]. As regards a phishing attack, an authentication protocol against all security attacks based on smart cards was proposed for a WSN restriction environment [46].

In Sybil's attack, an intruder creates multiple identities at the network layer, and packages they transmit have false identities, selectively being modified, or dropped. To mitigate this threat, the Energy Confidence System (ETS) was implemented using a confidence algorithm based on energies of each node to detect multiple identities and perform position verification [47].

4.1.6. Routing

Likewise, as part of network services that are affected when authentication fails in routing, mechanisms were created to guarantee the operation of multipath routing, base station authentication, use of directional antennas, topology check by servers, and topology check by the base station, among others, to prevent attacks such as selective forwarding, black hole, DoS, wormhole attack, false routing information, and sink attack [17], [33], [45].

To prevent wormhole attacks, the ad hoc on-demand multipath distance vector (AOMDV) routing protocol was used, which incorporates a method based on the round trip time (RTT) on each route to calculate the RTT threshold and other wormhole attack characteristics [48].

In case of a sinkhole attack, an intrusion that captures the traffic of nodes and performs operations through the compromised nodes alters the operation of a network. Hence, [49] a distributed adaptive framework based on subjective logic and abstract probabilistic timed automata extension was proposed to defend WSNs and send packages through reliable routes using the routing algorithm (ad hoc on-demand distance vector version 2, AODVv2-12), which uses the probabilistic extension, captures the traffic of nodes, and performs operations throughout the compromised nodes.

To reduce the impact of malicious nodes on the network, the routing protocol (energy-optimized secure routing, EOSR) was developed with a multi-factor routing strategic design by considering the level of trust of the node, remaining energy, and length of the path to isolate the malicious node [50]. Therefore, a protection scheme was proposed through routing algorithms [51] with other algorithms that largely aim to have efficient modules that achieve energy control and access control protocols [52].

Finally, [53] a derivation scheme and confidence calculations are required applying the semi-ring theory when selecting the route and optimizing the confidence calculation metrics, which allows defending the network against some attacks.

5. Trends and Future Lines of Work

The terms graph, which was obtained by using VOSviewer software, was developed as a strategy to verify the occurrence of topics within the group of articles related to the study. Keywords were found in the summaries of the articles examined to produce such a graph [54].

Figure 3 shows the groups of words that surround the key research topics about WSNs: security, authentication, clustering algorithms, sensor node, energy efficiency, intrusion detection, simulation, access control, ZigBee protocol, key management, biometrics, and smart cards, among others.

Around the security group, topics such as access control, sensor networks, attacks, and routing algorithms are grouped. Topics such as cryptanalysis, ECC, wasp protocol, biometrics, key establishment, and encryption algorithms were grouped around the following category.

VOSviewer enabled us to visualize the evolution and the emerging trending topics used in the WSN research field. To fulfill this objective, the overlay visualization option of the keyword co-occurrence maps [55] was used.

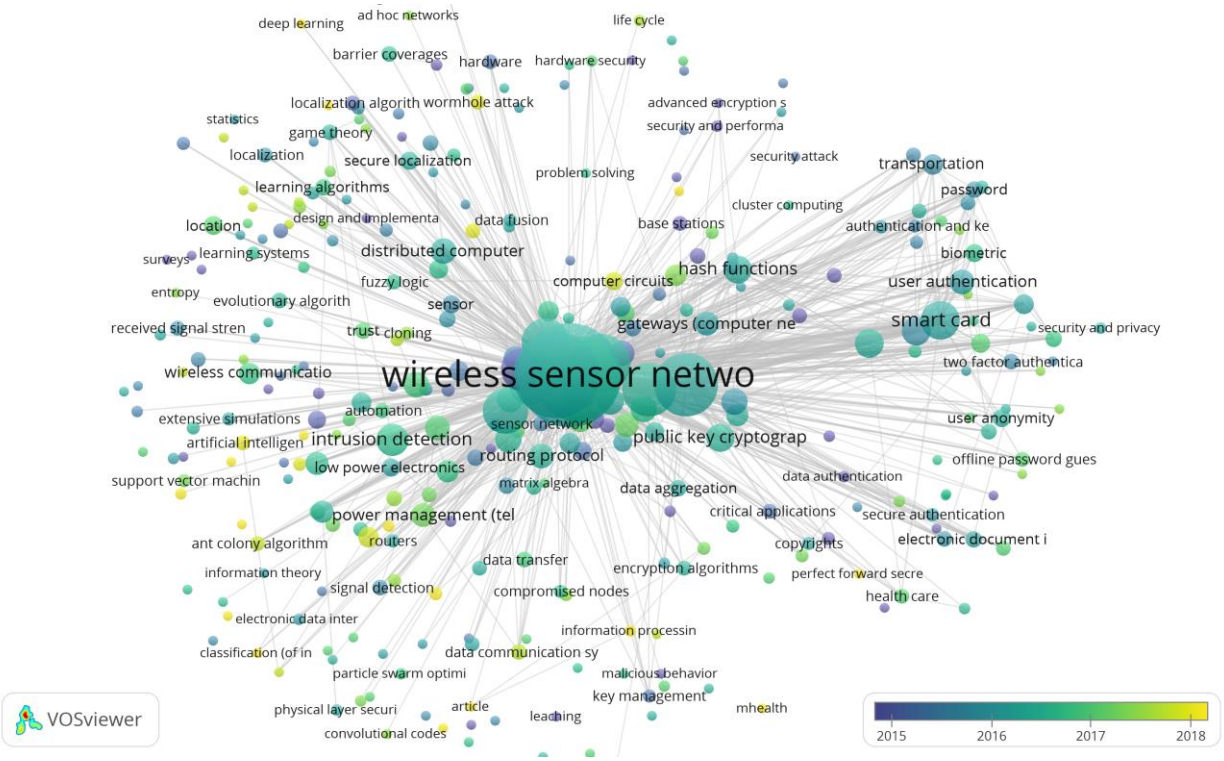

Figure 3. Visual graph of the grouping in three thematic clusters.

Figure 3 shows colored in yellow, the nodes (keywords) that appear reported in articles of the sample whose publication date is equal to or later than 2018 [56]. From the grouping of the nodes colored in yellow in related topics, four categories or fronts of study are proposed that are labeled as trending topics in WSN research.

a) The *machine learning* (ML) application and its supervised and unsupervised techniques in the design of protocols and security mechanisms for WSNs are reflected in the proposals that allow optimizing lifespans of ultra-dense WSNs, which balance energy consumption [57]. Similarly, [58] studies developed WSN middleware to provide a secure end-to-end system, which significantly decreased power consumption.

b) *Improved authentication schemes* are analyzed [59] through an improved scheme based on symmetric cryptography for IoT systems that integrated WSNs. Protocol minimizes spoofing, phishing, man-in-the-middle, desynchronization, and mutual authentication attacks. Furthermore, with an implicit certificate-based authentication protocol for WSNs and distributed IoT applications, the sensor nodes and end-users were allowed to authenticate with each other and initiate secure connections [60].

c) IDS with the use of artificial intelligence and ML with its techniques for the monitoring, detection, and prevention of attacks [61], [62]. An anomaly-based (IDS), "mIDS," with the statistical model of binary logistic regression (BLR) is submitted as a classification algorithm to identify normal and malicious data flow in detections of selective forwarding attacks and a black hole in WSNs network layer [63].

Likewise, the use of the supervised technique of a single-class vector support machine (One Class SVM) simulating with the QualNet platform a DoS attack enabled the application of the SVM algorithm in the design of IDS with an efficient way for detecting a selective forwarding attack [64]. Other authors [65] proposed a detection algorithm that dynamically runs the SVM classifier hierarchically, combining statistical-based techniques and ML, achieving intrusion detection efficiency, minimal resource overhead for WSN, and gateway security.

d) Network monitoring with attack isolation in intelligent network environments, in addition to the application of *bioinspired techniques using a neural network-based approach* to improve the cybersecurity of cyber-physical systems (CPSs) and WSNs [66], [67].

These lines are intended to conduct some future work that researchers in WSN security mechanisms have indicated:

i. Considering *multiclass classification techniques* and use of only important attributes for intrusion detection with machine learning [68].

ii. The integration of the *Taylor series into the Cat Swarm Swarm* (C-SSA) algorithm is expected to be developed to obtain high performance as a technique for routing multiple hops [69].

iii. A public key-based scheme known as effective *certificateless key management protocol* (CL-EKM) for WSNs has recently been proposed as a solution that improves the problems related to key management, in scenarios of multiple base stations and WSNs oriented to specific applications [70].

iv. Through the random key redistribution (RKP) scheme [71], under the concept of a *chameleon hash function*, building mutual trust schemes to configure a secure route that forwards the information and performs message authentication.

v. Using *IA/ML algorithms* for detection of intruders, optimization of the identification of patterns of malicious attacks [72], as well as hierarchical anomaly detection and localization (HADL), e.g., the SVM classifier in a hierarchical way [65].

vi. The *game theory* is used to delve into the design of intelligent intrusion detection models to effectively optimize the attack time and predict the next attack target with minimal energy consumption [73].

vii. It is necessary to add secure authentication systems to minimize the probability of collusion intruders in the fog-based model for the real-time monitoring of collusion attacks in IoT environments [74].

viii. An *Energy Trust System* (ETS) is proposed for WSNs in the effective detection of Sybil attacks. For this, multilevel detection based on identity and position verification is used, and then a confidence algorithm is applied supported by the energy of each sensor node. Nevertheless, it must be validated in WSN with more than two levels of hierarchy and dynamic networks such as mobile WSN and MANET [47].

6. Conclusions

WSNs lack defense lines and physical infrastructure for their protection that filters the data packages that circulate in them. Likewise, the geographical location, limitation of computational resources, and transmission medium make them vulnerable to flood attacks, information leakage, traffic capture, interference attacks, selective forwarding, identity fraud, and routing, among others. Therefore, the perspective on security mechanisms of WSNs becomes a topic of interest for scientific and business communities.

As per the publication's analysis, between the years 2013 to 2019, China is the country with the largest number of articles published with 545 issued, followed by India with 500, the US with 155, South Korea with 73, the United Kingdom with 50, France with 48, Australia with 43, Canada with 36, and Spain, Saudi Arabia, and Pakistan with 32 articles on average each. This shows that they are strong countries in the subject, with research that focuses on a) cryptographic authentication security protocols system, b) design of algorithms that have sophisticated cybersecurity barriers at the internal and external level, and c) efficient security algorithms in the use of energy.

The research identified advances in preserving confidentiality and integrity of WSNs, with the use of the DTLS protocol in protecting end-to-end communication between nodes, encryption schemes, access control, and digital signature. Similarly, progress in the availability of WSNs was identified through the development of IDS and authentication schemes. Faced with privacy protection in traffic and data flow tracking, we found that the use of end-to-end encryption for every message transmitted, symmetric key homomorphic encryption functions, and data mining with privacy recognition was viable.

Although countermeasures against flood attacks, information leakage, traffic capture, interference attacks, selective forwarding, identity fraud, and routing, among others, are present, the development of new security mechanisms is required to protect WSNs and routing protocols to ensure communications between nodes.

Finally, using overlay maps, clusters of topics or conceptual fronts that constitute trends in WSN research were identified. These topics address the development of security mechanisms based on the application of artificial intelligence and machine learning methods and tools with the use of intelligent networks.

Future studies are oriented to innovate mechanisms to minimize the probability of intelligent intrusions and optimize the consumption of computational resources.

Acknowledgment

The authors thank the research department of the Universidad Cooperativa de Colombia Ibagué - Espinal headquarters for the support provided to the development of this research, project code INV 2658.

References

[1] M. M. Shaimaa, S. . H. Haitham, A. S. Iman, "Coverage in mobile wireless sensor networks (M-WSN): A survey," *Computer Communications,* vol. 110, no. C, pp. 133-150, 2017. doi: 10.1016/j.comcom.2017.06.010

[2] J. Huang, E. Liao, Y. Chung, K. Chen, "Shielding wireless sensor network using Markovian intrusion detection system with attack pattern mining," *Information Sciences,* vol. 231, pp. 32-44, 2013. doi: 10.1016/j.ins.2011.03.014

[3] A. E. Zonouz, L. Xing, V. Vokkarane, Y. L. Sun, "Reliability-oriented single-path routing protocols in wireless sensor networks," *IEEE Sensors Journal,* vol. 14, no. 11, pp. 4059-4068, 2014. doi:10.1109/ JSEN.2014.2332296

[4] S. Chatterjee, A. K. Das, "An enhanced access control scheme in wireless sensor networks," *Ad-Hoc and Sensor Wireless Networks,* vol. 21, no. 1,pp. 121-149, 2014.

[5] S. G. Yoo, K. Park, J. Kim, "A security-performance-balanced user authentication scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks,* vol. 8, no. 3, pp. 28-38, 2012. doi: 10.1155/2012/382810

[6] I. Tomic, J. McCann, "A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols," *IEEE Internet of Things Journal,* vol. 4, no. 6, pp. 1910-1923, 2017. doi: 10.1109/JIOT.2017.2749883

[7] M. Rezvani, A. Ignjatović, E. Bertino, S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 1, pp. 98-110, 2015. doi: 10.1109/TDSC.2014.2316816

[8] A. Saipulla, C. Westphal, B. Liu, J. Wang, "Barrier coverage with line-based deployed mobile sensors," *Ad Hoc Networks*, vol. 11, no. 4, pp. 1381-1391, 2013. doi: 10.1016/j.adhoc.2010.10.002

[9] M. Abu Alsheikh, T. H. Dinh, D. Niyato, H. P. Tan, S. Lin, "Markov decision processes with applications in wireless sensor networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1239-1267, 2015. doi: 10.1109/COMST.2015.2420686

[10] IEEE Computer Society, "IEEE Standard for Low-Rate," in *IEEE*, pp. 1-709, 22 04 2016.

[11] "IEEE Standard for Low-Rate Wireless Networks," in *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011*), 2016, pp.1-709. doi: 10.1109/IEEESTD.2016.7460875

[12] "IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN - Specific Requirements - Part 15: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)," in *IEEE Std 802.15.1-2002* , 2002, pp.1-473. doi: 10.1109/IEEESTD.2002.93621

[13] A. Narmada, P. S. Rao, "Zigbee based WSN with IP connectivity," In *2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation*, 2012, pp. 178-181. doi: 10.1109 / CIMSim.2012.39.

[14] P. Morgner, S. Mattejat, Z. Benenson, C. Müller, F. Armknecht, "Insecure to the touch: attacking ZigBee 3.0 via touchlink commissioning," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017, pp. 230-240. doi: 10.1145/3098243.3098254

[15] G. Habib, N. Haddad, R. El Khoury, "Case study: Wirelesshart vs Zigbee network," in *2015 Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE)*, 2015, pp. 135-138. doi: 10.1109/TAEECE.2015.7113614

[16] M. Surendar, A. Umamakeswari, "InDReS: An Intrusion Detection and response system for Internet of Things with 6LoWPAN," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 1903-1908. doi: 10.1109/WiSPNET.2016.7566473

[17] H. Fahny, *Wireless Sensor Networks Concepts, Applications, Experimentation and Analysis.* Cairo: Springer, 2016.

[18] F. Siddiqui, J. Beley, S. Zeadally, G. Braught, "Secure and lightweight communication in heterogeneous IoT environments," *Internet of Things*, pp. 100093, 2019. doi: 10.1016/j.iot.2019.100093

[19] E. Aras, G. S. Ramachandran, P. Lawrence, D. Hu, "Exploring the Security Vulnerabilities of LoRa," in *2017 3rd IEEE International Conference on Cybernetics (CYBCONF)* , 2017, págs. 1-6. doi: 10.1109 / CYBConf.2017.7985777

[20] J. Nam, M. Kim, J. Paik, Y. Lee, D. Won, "A provably-secure ECC-based authentication scheme for wireless sensor networks," *Sensors* , vol. 14, no. 11, pp. 21023-21044, 2014. doi: 10.3390/s141121023

[21] M. Turkanović, B. Brumen, M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Redes Ad Hoc*, vol. 36, no. 1, pp. 96-112, 2016. doi: 10.1016/j.adhoc.2015.05.014

[22] C. H. Liu, Y. F. Chung,, "Secure user authentication scheme for wireless healthcare sensor networks," *Computers & Electrical Engineering*, vol. 59, pp. 250-261, 2017. doi: 10.1016/j.compeleceng.2016.01.002

[23] S. CHalla, K. A. Das, V. Odelu, N. Kumar, S. Kumar, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Computers & Electrical Enginee*, vol. 69, pp. 534-554, 2018. doi: 10.1016/j.compeleceng.2017.08.003

[24] Q. Jiang, J. Ma, X. Lu, Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 8, pp. 1070-1081, 2015. doi: 10.1007/s12083-014-0285-z.

[25] J. Gil-quintana, S. Santoveña-Casal, E. Romero Riaño, "Realfooders Influencers on Instagram : From Followers to Consumers," *Int. J. Environ. Res. Public Health*, vol. 18, no. 4, pp. 1-17, 2021. doi: 10.3390/ijerph18041624

[26] Á. M. Castro Rodríguez, L. E. Becerra Ardila, E. Romero Riaño, "Factores de éxito en proyectos de cooperación. Caso Universidad Industrial de Santander," *Rev. Ciencias Estratégicas*, vol. 24, no. 36, pp. 413-429, 2016.

[27] A. M. Beltran, E. Romero-Riaño, "Juegos y gamificación para el desarrollo la conciencia ambiental : una revisión bibliométrica the role of gamification in the environmental awareness : a bibliometric review," *Prism. Soc*, vol. 30, no. no. 3, pp. 161-185, 2020.

[28] E. Romero Riaño, L. D. Guarin Manrique, M. G. Dueñas, L. E. Becerra Ardila, "Reference framework for capabilities development in agricultural innovation systems," *Dyna*, vol. 86, no. 210, pp. 23-34, 2019. doi: 10.15446/dyna.v86n210.74475

[29] G. M. Martinez-Toro , G. C. Ariza-Zabala, D. W. Rico, E. Romero-Riaño, "Human computer interaction in transport, a systematic literature review," *Phys. Conf. Ser*, vol. 1409, no. 1, pp. 012002, 2019. doi: 10.1088/1742-6596/1409/1/012002.

[30] G. M. Martínez-Toro, D. Rico-Bautista, E. Romero-Riaño, C. J. Galeano-Barrera, C. Guerrero, J. A. Parra-Valencia, "Analysis of the intellectual structure and evolution of research in human-computer interaction: A bibliometric analysis," *Rev. Iber. Sist. E Tecnol. Informaçao*, vol. 17, pp. 363-378, 2019.

[31] N. Vlajic, D. Stevanovic, G. Spanogiannopoulos, "Strategies for improving performance of IEEE 802.15. 4/ZigBee WSNs with path-constrained mobile sink (s)," *Computer Communications*, vol. 34, no. 6, pp. 743-757, 2011. doi: 10.1016/j.comcom.2010.09.012

[32] R. Alguliyev, Y. Imamverdiyev, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212-223, 2018. doi: 10.1016/j.compind.2018.04.017

[33] B. Bhushan, G. Sahoo, "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks," *Wireless Personal Communications*, vol. 98, pp. 2037-2077., 2018. doi: 10.1007/s11277-017-4962-0

[34] P. Ahlawat, M. Dave, "An attack resistant key predistribution scheme for wireless sensor networks," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 3, pp. 268-280, 2018. doi: 10.1016/j.jksuci.2018.03.002

[35] A. H. Moom, U. Lqbal, G. M. Bhat, "Implementation of node authentication for wsn using hash chains," *Procedia Computer Science*, pp. 89, 90-98, 2016. doi: 10.1016/j.procs.2016.06.013

[36] J. Lopez, R. Rios, F. Bao, F. Wang, "Evolving privacy: From sensors to the Internet of Things," *Future Generation Computer Systems*, vol. 75, pp. 46-57, 2017. doi: 10.1016/j.future.2017.04.045

[37] C. Di Sarno, A. Garofalo, "Energy-Based Detection of Multi-layer Flooding Attacks on Wireless Sensor Network.," in *Computer Safety, Reliability, and Security vol. 8696*, Springer, Cham, 2014, pp. 339-349. doi: 10.1007/978-3-319-10557-4_37

[38] X. Jinhui, T. Yang, Y. Feiyue, P. Leina, X. Juan, H. Yao, "Intrusion Detection System for Hybrid DoS Attacks using Energy Trust in Wireless Sensor Networks," *Procedia computer science*, vol. 131, pp. 1188-1195, 2018. doi: 10.1016/j.procs.2018.04.297

[39] K. Xie, X. Ning, X. Wang, S. H, Z. Ning, Z. Liu, Z. Quin, "An efficient privacy-preserving compressive data gathering scheme in WSNs," *Information Sciences*, vol. 390, pp. 82-94., 2017. doi: 10.1016/j.ins.2016.12.050

[40] P. Zhang, J. Wang, K. Guo, F. Wu, G. Min, "Multi-functional secure data aggregation schemes for WSNs," *Ad Hoc Networks,* vol. 69, pp. 86-99., 2018. doi: 10.1016/j.adhoc.2017.11.004

[41] S. Ganesh, R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms," *Journal of Communications and Networks,* vol. 15, no. 4, pp. 422-429, 2013. doi: 10.1109/JCN.2013.000073

[42] S. Roy, M. Conti, S. Setia, S. Jajodia, "Secure data aggregation in wireless sensor networks," *IEEE Transactions on Information Forensics and Security,* vol. 7, no. 3, pp. 1040-1052, 2012. doi: 10.1109 / TIFS.2012.2189568

[43] P. Bhavathankar, S. Sarkar, S. Misra, "Optimal decision rule-based ex-ante frequency hopping for jamming avoidance in wireless sensor networks," *Computer Networks,* vol. 128, pp. 172-185., 2017. doi: 10.1016/j.comnet.2017.03.009

[44] C. Pu, S. Lim, "A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: design, analysis, and evaluation," *IEEE Systems,* pp. Journal, vol. 12, no. 1, pp. 834-842, 2018. doi: 10.1109/JSYST.2016.253573

[45] P. Ahlawat, M. Dave, "An attack resistant key predistribution scheme for wireless sensor networks," *Wireless Pers Commun*, vol. 94, pp. 3327–3353, 2017. doi: 10.1007/s11277-016-3779-6

[46] S. Kalra, S. K. Sood, "Advanced password based authentication scheme for wireless sensor networks," *Journal of information security and applications,* vol. 20, pp. 37-46, 2015. doi: 10.1016/j.jisa.2014.10.008

[47] N. Alsaedi, F. Hashim, A. Sali, F. Z. Rokhani, "Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)," *Computer Communications*, vol. 110, pp. 75-82., 2017. doi: 10.1016/j.comcom.2017.05.006

[48] P. Amish, V. P. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," *Procedia computer science,* vol. 79, pp. 700-707, 2016. doi: 10.1016/j.procs.2016.03.092

[49] G. Jahandoust, F. Ghassemi, "An adaptive sinkhole aware algorithm in wireless sensor networks," *Ad Hoc Networks,* vol. 59, pp. 24-34., 2017. doi: 10.1016/j.adhoc.2017.01.002

[50] T. Yang, X. Xiangyang, L. Peng, L. Tonghui, P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," *Procedia computer science,* vol. 131, pp. 1156-1163, 2016. doi: 10.1016/j.procs.2018.04.289

[51] Y. Li, J. Ren, J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems,* vol. 23, no. 7, pp. 1302-1311, 2012. doi: 10.1109/TPDS.2011.260

[52] S. Climent, A. Sánchez, J. V. Capella, N. Meratnia, J. J. Serrano, "Underwater acousticwireless sensor networks: Advances and future trends in physical, MAC and routing layers," *Sensors,* vol. 14, no. 2, pp. 795-833, 2014. doi: 10.3390/s140100795

[53] J. Duan, D. Yang, H. Zhu, S. Zhang, J. Zhao, "TSRF: A trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks,* vol. 10, no. 1, pp. 29-36, 2014. doi: 10.1155/2014/209436

[54] N. Eck, J. Van, L. Waltman, "VOSviewer Manual," *CWTS Meaningful metrics*, pp. 1-28, 2013.

[55] C. H. Limaymanta, E. Romero-Riaño, J. Gil-Quintana, L. Huaroto, Á. Torres Toukoumidis, R. Quiroz, "Gamificación en educación desde Web of Science. Un análisis con indicadores bibliométricos y mapas de visualización," *Rev. Conrado,* vol. 16, no. 77, pp. 339-406, 2020.

[56] E. Romero-riaño, C. D. Guerrero-Santander, H. Martínez, "Agronomy research co-authorship networks in agricultural innovation systems Redes de coautoría en investigación sobre agronomía en sistemas de innovación agrícola," *Revista UIS Ingenierías,* vol. 20, no. 1, pp. 161-175, 2021.

[57] Y. Chang, X. Yuan, B. Li, D. Niyato, N. Al-Dhah, "A Joint Unsupervised Learning and Genetic Algorithm Approach for Topology Control in Energy-Efficient Ultra-Dense Wireless Sensor Networks," *IEEE Communications Letters,* vol. 22, no. 11, pp. 2370-2373, 2018. doi: 10.1109/LCOMM.2018.2870886

[58] R. Alshinina, K. Elleithy, "A highly accurate machine learning approach for developing wireless sensor network middleware," in *2018 Wireless Telecommunications Symposium (WTS),* 2018, pp. 1-7. doi: 10.1109/WTS.2018.8363955

[59] K. Jawad, K. Mansoor, A. F. Baig, A. Ghani , "An Improved three-factor anonymous Authentication Protocol for WSN s based IoT System Using Symmetric cryptography," in *International Conference on Communication Technologies (ComTech),* 2019, pp. 53-59. doi: 10.1109/COMTECH.2019.8737799

[60] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov , "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *IEEE Wireless Communications and Networking Conference (WCNC),* 2014, pp. 2728-2733. doi: 10.1109/WCNC.2014.6952860

[61] A. Chandrasekhar, K. Raghuveer, "Intrusion detection technique by using k-means, fuzzy neural network and SVM classifiers," in *2013 International Conference on Computer Communication and Informatics,* 2013, pp. 1-7. doi: 10.1109/ICCCI.2013.6466310

[62] F. Mekelleche, B. OuldBouamam, "Monitoring of Wireless Sensor Networks: Analysis of Intrusion Detection Systems," In *2018 5th International Conference on Control, Decision and Information Technologies (CoDIT),* 2018 pp. 421-426. doi: 10.1109/CoDIT.2018.8394844, 2018.

[63] C. Ioannou, V. Vassiliou, C. Sergiou, "An Intrusion Detection System for Wireless Sensor Networks," *In 2017 24th International Conference on Telecommunications (ICT) IEEE,* 2017, pp. 1-5. doi: 10.1109 / ICT.2017.7998271

[64] L. Wang, J. Li, J. Cheng, U. Bhatti, Q. Dai, "DoS Attacks Intrusion Detection Algorithm Based on Support Vector Machine," In *International Conference on Cloud Computing and Security,* Springer, Cham, 2018, pp. 286-297. doi: 10.1007/978-3-030-00018-9_26

[65] A. Yahyaoui, T. Abdellatif, R. Attia, "Hierarchical anomaly based intrusion detection and localization in IoT," in *15th International Wireless Communications & Mobile Computing Conference (IWCMC),* 2019, pp. 108-113, doi: 10.1109/IWCMC .2019.8766574

[66] G. S. Dhunna, I. Al-Anbagi, "A low power cybersecurity mechanism for WSNs in a smart grid environment," *IEEE Electrical Power and Energy Conference (EPEC),* 2017, pp. 1-6. doi: 10.1109/EPEC.2017.8286172

[67] S. Bitam, S. Zeadally, A. Mellouk, "Bio-inspired cybersecurity for wireless sensor networks," *IEEE Communications Magazine,* vol. 54, no. 6, pp. 68-74, 2016. doi: 10.1109/MCOM.2016.7497769

[68] B. Manjula, M. Balachandra , "Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection," *Procedia Computer Science,* vol. 89, pp. 117-123, 2016. doi: 10.1016/j.procs.2016.06.016

[69] A. Vinitha, M. Rukmini, Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm," *Journal of King Saud University - Computer and Information Sciences,* pp. 1-12, 2019. doi: 10.1016/j.jksuci.2019.11.009

[70] D. Mall, K. Konaté, A. K. Pathan, "ECL-EKM: An enhanced Certificateless Effective Key Management protocol for dynamic WSN," in *International Conference on Networking, Systems and Security (NSysS), Dhaka,* 2017, pp. 150-155, doi : 10.1109/NSysS.2017.7885817

[71] A. Dahgwo Yein, C. Lin, W. Hsieh, "A secure mutual trust scheme for wireless sensor networks," in *IEEE 26th International Symposium on Industrial Electronics (ISIE),* 2017, pp. 1369-1375, doi : 10.1109/ISIE.2017.8001445

[72] X. Tan, S. Su, Z. Huang, X. Guo, Z. Zuo, X. Sun, L. Li, "Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm," *Sensors*, vol. 19, no. 1, pp. 203, 2019. doi: 10.3390/s19010203

[73] H. Lansheng Han, Z. Man , J. Wenjing , D. Zakaria, X. Xingbo, "Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model," *Information Sciences*, vol. 476, pp. 491 -504, 2019. doi: 10.1016/j.ins.2018.06.017

[74] Q. Yaseen, Y. Jararweh, M. Al-Ayyoub, M. AlDwairi, "Collusion attacks in Internet of Things: Detection and mitigation using a fog based model," *IEEE Sensors Applications Symposium (SAS), Glassboro,* 2017, pp. 1 -5. doi: 10.1109/SAS.2017.7894031