Section A-Research paper
ISSN 2063-5346

A COMPREHENSIVE ANALYSIS OF INTRUSION DETECTION SYSTEMS IN WIRELESS SENSOR NETWORKS

D.Govindaraj, (Ph.D)., Research Scholar, Department of Computer Science (PG), Kongu Arts and Science College (Autonomous), Erode- 638 107.
Dr.B.Jayanthi, Associate Professor & Head, Department of Computer Science (PG), Kongu Arts and Science College (Autonomous), Erode- 638 107.

Abstract

WSN is a dispersed sensor network having sensors as its endpoints that can sense and detect the external environment. Numerous routing, power management, and data dissemination protocols are tailored specifically for WSNs, prioritizing power economy in their architecture. The routing protocols used in WSNs might vary depending on the application and the network's design. Detecting and responding to a broad range of security threats in WSNs is possible with an IDS. WSN Intrusion Detection Systems (IDS) are discussed in this article. The inquiry and connection of each arrangement and the favorable conditions and burdens associated with them decide this. "intrusion" refers to any unauthorized or illegal activity inside a network or system. An IDS is a combination of technologies, methods, and resources that are used to detect, analyze, and report intrusions. In wireless sensor networks, trust-based routing methods are prevalent (WSNs). Following a brief discussion of trust models in WSNs, the focus shifts to routing techniques and cluster-based trust management. The pros and downsides of each routing method are also discussed. Because of this, intrusion detection systems (IDSs) exist to stop unauthorized access to a system's resources. There is a common perception that IDSs constitute the second line of defense for data protection.

Keywords: WSN, Routing, Trust, Intrusion Detection System (IDS), Attacks, Security

I INTRODUCTION

WSNs are rapidly gaining popularity as a means of providing ubiquitous computing environments for various applications [1]. Energy constraint is the most critical issue in all of these environments. Due to the high energy consumption associated with radio transmission and reception, one of the critical issues in wireless sensor networks is the inherently limited battery capacity of network sensor nodes. As a result, battery power is a critical parameter in designing algorithms that extend the life of network nodes [2]. Any reasonably unauthorized or unapproved activities in a network or a system are referred to as intrusions. In [5], Techniques for interfering with intrusions2 (such as coding, authentication, restriction of access, secure routing, etc.) are supplied as the first defense against invasions. It's hard to prevent intrusions altogether, even

with the best security measures available. Security keys in the form of steers are made available to the attackers after an intrusion or breach of a node. As a result, the mechanism designed to avoid such an occurrence fails [6-13].

Dense node deployment, dynamic network architecture, limited battery life, and multi-hop communication are only a few of the distinguishing features of a WSN [14-19]. In WSNs, the sensor nodes may be homogeneous or heterogeneous, and the self-configurable sensor nodes may be mobile or stationary. Dispersed sensors in a hostile environment are in danger of many destructive attacks because of their broadcast nature. An attacker may, for example, look at the network's traffic flow and decide to act quickly [20-29].

WSNs are susceptible to several dangers. The resource reliability and performance of any WSN with clustered The value of WSNs cannot be overstated. As well as in industrial automation, agriculture, healthcare, and robotics, WSNs are employed in various other industries. When it comes to route-finding challenges, WSNs face the bulk of them in terms of the placement and security of nodes, the consumption of energy, the range of communication, the level of fault tolerance, and the quality of the service. Economic loss and privacy concerns have heightened interest in WSN security [30-41].

The Wireless Sensor Network (WSN) is a large network of hundreds to tens of thousands of tiny devices. Wireless sensor networks, or WSNs, are used in various industries, including military, healthcare, and smart homes. WSN security is an essential research subject since WSN applications have serious security problems. As a second-line network security device, an Intrusion Detection System is critical to the network's integrity, confidentiality and availability [42-48].

Security systems for wireless sensor networks must be redesigned to reduce network resources while allowing the network's most trustworthy devices, such as routers, to engage only in routing. Trust-based security (TBS) is a new way to protect WSNs.

WSNs' limitations on cyber security approaches and attack types make intrusion detection in WSNs unique from wired and non-energy-constrained wireless networks. WSN intrusion detection systems have been the target of several attacks, summarised in this article [49-52].

System and user behavior are monitored by an Intrusion Detection System, which may identify suspicious network activity and establish attack patterns. Network intrusions are central to the IDS concept. Even so, physical damage to sensor equipment is a possibility with WSN. Detection of sensor degradation is critical to ensuring reliability and fault tolerance.

II **LITERATURE SURVEY**

2.1 INTRUSION DETECTION

Amaran, S., & Mohan, R. M. [2] This study has developed an effective OSVM-based IDS paradigm (WSN) in wireless sensor networks. Preprocessing, categorization, and kernel selection are part of the OSVM model's intrusion detection process. The supplied network data is

mostly transformed into a format that may be used. The invasions are classified using the OSVM model, which uses the best possible support vector machines. IDS in WSN uses a new, more efficient version of the optimal support vector machine. To round things up, the OSVM technique suggests that the whale optimization algorithm (WOA) be used to discover the best kernels in the SVM model. The NSLKDDCup 99 dataset has been used to evaluate the OSVM model's performance. The OSVM model's improved accuracy and detection rate of 95.02 percent were evident in the simulation results, which showed the model's beneficial effects. The WOA may be replaced with hybrid metaheuristic algorithms as a future update.

Ashraf, S., & Ahmed, T. [3] Several intelligent methods have been presented as intrusion detection tools to monitor DoS attempts from the corpus. Upon applying KNN, Logistic regression, SVM, Nave Bayes, and ANN, it was shown that ANN and KNN performed much better at 98 and 97 percent, respectively than all other methods. A comparison with the existing research from which the recommended method was derived reveals similar results, indicating that our experiment was conducted using a typical and adequate setting. The chosen approach is appropriate for this kind of data corpus since the data is collected using the LEACH methodology. These methods may, however, also be utilized for data sets collected from other protocols for routing. We may utilize KNN and ANN algorithms in real time for wireless network intrusion detection and raise the alarm to begin the preventive action. For this reason, we also show how to categorize the Unbalance dataset and use it for analysis. The study's results indicated that the algorithms could predict attacks intelligently after utilizing SMOTE.

The award, S., & Joshi, S. [4] Utilize acknowledgment schemes such as TWOACK, ACK, AACK, and EAACK to prevent the fault. Packet loss detection is essential for securing MANETs. EAACK provides superior performance compared to other schemes. EAACK's use of digital signatures causes routing delays. This study suggests using hybrid cryptography to reduce routing costs to detect malicious pathways. Using a shared key, the source and destination nodes verify the authenticity of the data they send back and forth.

Jiang, S.et al. [27]. Preparation of the data is done using the SBS approach. Through feature extraction from the original data, this strategy may effectively reduce dimensionality and eliminate data redundancy to the maximum extent feasible. Using LightGBM, measurements, including accuracy and recall, may be improved. Research has proven that this approach not only has a high detection rate but also involves few computations and a low false alarm rate, which experiments and comparative analyses have shown. To detect intrusions, it may be integrated into real-world wireless sensor networks.

Meng, W et al. [37] IoT applications rely heavily on wireless sensor networks (WSNs), which allow networked things to be sensed and controlled by merging the physical world and computer systems

through the Internet of Things (IoT). Trust-based intrusion detection technologies are often used to protect networks from threats, including insider attacks. It is, however, inefficient to use packet-based trust management due to packet loss and overhead traffic in the age of big data. We propose a solution to this issue by merging Bayesian trust management with traffic sampling for wireless intrusion detection.

Kurniawan, M. T., & Yazid, S [34] The DoS mitigation technique for WSN networks was successfully implemented. DoS detection with signature-based IDS is the first step. Detection successfully calculated RREQ RATELIMIT; if it exceeds a specified threshold, it may signal a DoS assault. IDS has little influence on DoS assaults since it solely functions as a notification system. DDoS attacks diminish the performance of WSN networks. Scenario I depicts a WSN in a normal, unattacked state with excellent performance, Scenario II depicts a WSN under a DoS attack with a degraded quality of service performance, and Scenario III depicts a WSN under a DoS assault with a mitigation mechanism and an impending system shutdown. When IDS identifies a DoS assault, the system approach shutdown is used to drop all packets originating from the attacker. IDS will produce a system approach shutdown on each node that detects the attacker and conducts a packet drop action originating from the attacker.

Borkar, G. M., & Patil, L. H. [13]. Samples are not utilized in regular CSO. Hence the ACSO approach minimizes the amount of time it takes. Reduce the amount of sensor node properties that aren't necessary—an adaptive SVM classifier supervised-learning classification method using the RRF approach. In contrast to a two-stage technique, the classifier methodology relies on an anomaly-based IDS that uses the acknowledgment method to detect the presence of an attack. Packets traveling between sensor networks may be sent safely with a High-LevelSecurity Mechanism. The effectiveness of the proposed technique is compared to current security measures; It takes 0.17476 seconds to encrypt and 0.17472 seconds to decrypt. The results are striking when the proposed two-stage classification strategy is compared to prior techniques that yielded a detection rate of 0.50. Our proposed approach outperforms existing techniques regarding specificity, sensitivity, FPR, and FDR accuracy outcomes.

2.2 TRUST-BASED WIRELESS SENSOR NETWORK

Cheng, X. et al.[14] The capture of a node in a wireless sensor network represents a lethal danger to the whole network since many nodes are in an uncontrolled environment. It is possible for a single node, or even the whole network, to be the cause of a failure. As a result, figuring out whether or not a given network node can be trusted is critical. This research presents a trust management approach for wireless sensor networks. To overcome the difficulty of evil nodes not being able to recognize each other, a simple mathematical approach is utilized to calculate the integrated trust value of each node. In addition, the model's

accuracy in detecting harmful nodes is dramatically increased, the false detection rate is minimized, and the network security performance is improved by building the credibility of direct trust.

Gautam, A. K., & Kumar, R [17] WSNs provide several security challenges regarding internal vulnerabilities, external threats, node deployment, energy consumption, communication range, fault tolerance, and quality of service. We have proposed a robust trust architecture to secure a cluster-based network against collusion assaults. Our solution is lightweight since the direct trust is calculated using elementary mathematical processes. The trust is continuously updated, and greater weight is placed on recent transactions. The trust calculation relies only on packet exchanges between nodes. We presume that the environmental aspect of the transaction stays unaltered. The cluster head functions as a manager of recommendations, computing the indirect trust of each node. The proposed technique provides an effective and robust trust architecture to defend WSN against insider attacks.
The suggested approach may be used to identify and avoid intrusion detection and other forms of assaults.

Ozcelik, M. M. et al. [47] WSNs have limited resources. As a result, standard network security measures cannot be used directly on these applications. We propose a new trust-based IDS for WSNs and a preliminary system evaluation in this study's findings. The proposed system combines an abuse detection method with a functional reputation-based trust evaluation. Additional control packet costs are small. Therefore, the technology can be used according to simulation results.

2.3 WSN PACKET LOSS

Hentati, A.et al. [24] In this study, a point-to-point wireless energy harvesting transmission mechanism is analyzed, considering the information's age and packet loss metrics. Data gathering, channel evaluation, and data transfer are all included in our research. To avoid the additional delay caused by retransmissions, they predict the channel's condition before transmission. Information age terms and packet loss losses are determined using a known energy arrival approach. According to analytical and simulation results, obtaining the channel status, as employed by the proposed transmission method, reduces information age and packet loss.

Li, H. et al. [35] To reduce packet loss, it is advised that LEACH-M be used. The method's performance is compared to that of LEACH-M and AODV using the NS3 simulator. The improved packet loss rate technique outperforms leach-m for a certain network architecture model. There will be an increase in energy usage for certain nodes, requiring the network to do extra energy-saving processes. It's time to work on the selection process for cluster leaders and the scope of a given cluster. Using the LEACH-M mobile model and the clustering network idea in the domain of mobile intelligent devices will be the focus of future research. By preserving the node gap, we can reduce packet loss and improve

data accuracy if we keep researching the node cluster clustering determination approach.

2.4 PACKET DROPPING IN WSN

Joseph, C. et al. [28] Homomorphic Linear Authenticator (HLA)-based public auditing architecture efficiently solved security concerns caused by malicious attacks. The network's efficiency is enhanced.

Table 1: comparative analysis of Attacks

Authors	Defense Approach	Attacks Considered	Technique Used	Dataset
Nannan et al.[40]	Centralized	Dos User to root Remote to local Probe	GNP	NSL-KDD
Hidoussi et al.[23]	Centralized	Black hole Selective Forwarding	Reception and delay rule sub-list of C.H. member's nodes rule information loss rule	Collected from NS2 Network simulator
Cho et al.[16]	Distributed			Collected from NS2 Network simulator
Berjab et al. [8]	Distributed	No specific attack defined	STA correlation MVA correlations	Real-world dataset
Han et al.[22]	Centralized	Malicious	Auto aggressive Game theory	MAT Lab
Ioannou et al.[25]	Distributed	Selective forwarding blackhole	BLR	Collected from cooja network simulator
Osanaiye et al.[44]	Distributed	Jamming	EWMA	CRAWDA
Shafiei et al.[44]	Distributed	Sinkhole	Geo-statistical	Castalia simulator

Section A-Research paper
ISSN 2063-5346

				(OMNeT++)
J.W.Ho et al.[30]	Distributed	DoS	SPRT	
Ballarini et al.[9]	Distributed	DoS	GSPN	Collected from NS2 network simulator

Authors	Defense Approach	Attacks Considered	Technique Used	Dataset
Ahmad et al.[1]	Centralized	Black hole Misdirection	Improved K-means	Collected from NS2 network simulator
Kaur et al.[31]	Centralized	Black hole	K-means J48	Collected from NS2 network simulator
Almomani et al.[7]	Centralized	Flooding Gray hole Black hole Scheduling	Navie Bayes Decision Trees RF SVM J48 ANN KNN Bayesian Networks	WSN-DS
Li et al.[35]	Centralized	Flooding	KNN	Testbed
Coppolino et al.[15]	Distributed	Sinkhole Sleep Deprivation	Decision Tree	Collected from NS3 network simulators

Authors	Defense Approach	Attacks Considered	Technique Used	Dataset

Almomani et al.[7]	Centralized	Flooding Gray hole Black hole Scheduling	ANN	Collected from NS2 network simulator (WSN-DS)
Qu et al.[48]	Centralized	Blackhole Flooding	FCM One class SVM Sliding Window	EXata network simulator
Qtoum et al.[45]	Centralized	DoS User to Root Remote to Local Probe	RFt E-DBSCAN	Collected From NS2network simulator
Qtoum et al.[46]	Centralized	DoS User to root Remote to local probe	RBM	Collected from NS2 network simulator
Garofalo et al.[20]	Distributed	Sinkhole	Decision tree	Collected from NS2 network Simulator

Authors	Defense Approach	Attacks Considered	Technique Used	Dataset
Mansouri et al.[38]	Centralized	Command injections Response DoS Reconnaissance	GWO ANN	Gas Pipeline
Nithiyanandam et al.[41]	Centralized	Sinkhole	ACO PSO	Collected from NS2 network Simulator
Bitam et al.[10]	Distributed	Cyber	Swarm intelligence	Theoretical Analysis

Authors	Defense Approach	Attacks Considered	Technique Used	Dataset

Yan et al.[6]	Distributed	DoS User to root Remote to local Probe Attack	Anomaly-based (BPN)+signature based	KDDCup'99

Table 2: An overview of network layer schemes

Network layer scheme	Description
SMECN [48] Flooding	Creates a subgraph of the sensor network that contains the M.E. path. Broadcasts data to all neighbor nodes regardless if they receive it before or not
Gossiping [32]	Sends data to one randomly selected neighbor
SPIN [35]	Sends data to sensor nodes only if they are interested; has three types of messages, i.e., ADV, REQ, and DATA
LEACH [34]	Forms clusters to minimize energy dissipation
Directed diffusion [39]	Sets up gradients for data to flow from source to sink during interest dissemination

Bhakthavatsalam, P. et al. [12] The problem of safely transmitting provenance data across sensor networks have previously been addressed by providing a lightweight provenance encoding and decoding solution. Preserved privacy, integrity, and purity are hallmarks of Provenance in the present method. Congestion-based data-provenance binding may assist in identifying AODV protocol packet loss concerns in this technique. Congestion or purposeful packet drop by an attacker may be used to identify a node as either legitimate or an attacker using the Packet Drop Due to Attacker Congestion (PDAC) approach, which improves the detection of packet-dropping attacks. Provenance's security is enhanced by this strategy, which prevents packet-dropping attacks when the network is congested.

Ghugar, U., & Pradhan, J. [18] The author has developed a black hole attack technique to identify the rogue node in a network. Detection accuracy (DA) rises as node density increases, and false alarm rate (FAR) lowers, according to the results and explanation. It implies that our system will be a superior model for black hole attacks.

In the future, we want to construct a more efficient intrusion detection system and more network layers.

Kalnoor, G., & Agarkhed, J. [32] In the event of an intrusion, the sensor network's performance is improved by considering all Quality of Service (quality of service) attributes. The multipath routing protocol calculates all feasible routes from the source to the destination. A custom IDS monitors the WSN once an algorithm finds the cheapest path. Even after a sinkhole attack, it is considered that WSN's service requirements improve performance. This protocol may detect and avoid a wide range of WSN-based attacks.

Nobar, S. et al. [43] The author investigated an energy-harvesting TDMA sensor network with linear physical topology. Energy causality, data queue stability, and minimum packet production rate limitations have reduced the overall packet loss probability across all nodes. The problem was turned into a time-average optimization problem using the Lyapunov drift plus penalty theorem. For example, the suggested technique asymptotically achieves the desired goal function by transmitting at an optimal power level, retaining a packet, or rejecting a packet. The average delay in packet delivery is determined by the tradeoff between the value of the goal function and the stable queue size, which is controlled by the network operator-selected parameter V. For a particular monitoring quality (Qom) restriction in the network's stability zone; we may obtain almost the same objective function value at a larger queue size price if the energy harvesting rate is sufficiently high. Our proposed method may be implemented in networks that are tolerant of delays.

Reddy, V. et al. [52] Trust is critical to enhancing system performance and identifying rogue nodes. Safe routing, data aggregation, cluster head selection, and trustworthy key exchange are just a few of the many uses of this technology. As trust grows in interpersonal relationships, this study gives a framework for understanding how trust develops through time. This system's unique approach to evaluating trust increases and decreases delivers more reliable trust values. The hysteresis curve is seen in this diagram. Many systems often assume initial trust values of 0 or 0.50, or 1. The trustworthiness values of these systems are unstable when first investigated. On the other hand, the hysteresis model takes longer to show the effect and is less vulnerable to packet loss.

3 CONCLUSION

In the early stages of sensor network routing, there is currently just a small but growing body of study. In this study, we evaluate WSN trust-based routing algorithms published in the scientific surveys taken with 52 papers in recent years. IDS is also an important part of the network security community. Energy-efficient intrusion detection systems are ideal for wireless device networks. Centralized intrusion detection systems (IDS) are energy-efficient due to the most powerful network neighborhood (the sink or B.S.) detecting intrusions. But these advanced techniques need a particular routing protocol

that gathers information from each device node and transfers it to a source or sinks for anomaly identification. Because the IDS agent is installed on every node, purely distributed IDS systems are inefficient. Extra processing or power consumption at the node level will result. Based on energy consumption and complexity, the distributed-centralized IDS technique is appropriate for WSNs, notwithstanding its drawbacks. The tradeoffs between energy and communication overhead reductions inherent in many routing paradigms and the advantages and downsides of each routing technique are also addressed. Sensor networks confront extra challenges despite some of these promising routing techniques.

4. REFERENCES

1. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network. IEEE Sensors Journal, 15(12), 6962–6972. doi:10.1109/jsen.2015.2468576
2. Amaran, S., & Mohan, R. M. (2021). Intrusion Detection System using Optimal Support Vector Machine for Wireless Sensor Networks. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS). doi:10.1109/icais50930.2021.9395919
3. Ashraf, S., & Ahmed, T. (2020). Sagacious Intrusion Detection Strategy in Sensor Network. 2020 International Conference on UK-China Emerging Technologies (UCET). doi:10.1109/ucet51115.2020.9205412
4. Awatade, S., & Joshi, S. (2016). Improved EAACK: Develop a secure intrusion detection system for MANETs using hybrid cryptography. 2016 International Conference on Computing Communication Control and Automation (ICCUBEA). doi:10.1109/iccubea.2016.7860076
5. B. Ahmad, W. Jian, Z. Anwar Ali, S. Tanvir, M. Sadiq Ali Khan, "Hybrid Anomaly Detection by Using Clustering for Wireless Sensor Network," Wireless Personal Communications, Vol. 106, No. 4, pp. 1841–1853, 2018.***
6. V. T. Alaparthy and S. D. Morgera, "A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory," IEEE Access, Vol. 6, pp. 47364-47373, 2018.******
7. I. Almomani, Bassam Al-Kasasbeh and Mousa AL-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," Journal of Sensors, Vol. 2016, 16 pages, 2016. *****
8. N. Berjab, H. H. Le, C. Yu, S. Kuo, and H. Yokota, "Hierarchical Abnormal-Node Detection Using Fuzzy Logic for ECA Rule-Based Wireless Sensor Networks," 2018

IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan 2018, pp. 289-298. ****

9. P. Ballarini, L. Mokdad, and Q. Monnet, "Modeling Tools for Detecting DoS Attacks in WSNs," Security and Communication Networks, Vol. 6, No. 4, pp. 420–436, Apr. 2013.****
10. S. Bitam, S. Zeadally and A. Mellouk, "Bio-Inspired Cybersecurity for Wireless Sensor Networks," IEEE Communications Magazine, Vol. 54, No. 6, pp. 68-74, 2016.****
11. Berrachedi, A., & Boukala-Ioualalen, M. (2016). Evaluation of the Energy Consumption and the Packet Loss in WSNs Using Deterministic Stochastic Petri Nets. 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA). doi:10.1109/waina.2016.86
12. Bhakthavatsalam, P. K., & Malarkodi, B. (2016). Securing Provenance by avoiding packet drop attacks due to congestion in wireless sensor networks. 2016 International Conference on Inventive Computation Technologies (ICICT). doi:10.1109/inventive.2016.7824890
13. Borkar, G. M., & Patil, L. H. (2019). A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. Sustainable Computing: Informatics and Systems. doi:10.1016/j.suscom.2019.06.002
14. Cheng, X., Luo, Y., & Gui, Q. (2018). Research on Trust Management Model of Wireless Sensor Networks. 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC). doi:10.1109/iaeac.2018.8577648
15. L. Coppolino, S. DAntonio, A. Garofalo and L. Romano, "Applying Data Mining Techniques to Intrusion Detection in Wireless Sensor Networks," 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Compiegne, pp. 247-254, 2013.**********
16. E. J. Cho, C. S. Hong, S. Lee, and S. Jeon, "A Partially Distributed Intrusion Detection System for Wireless Sensor Networks," Sensors, vol. 13, no. 12, pp. 15863-15879, 2013.*****
17. Gautam, A. K., & Kumar, R. (2018). A Robust Trust Model for Wireless Sensor Networks. 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON). doi:10.1109/upcon.2018.8597072

18. Ghugar, U., & Pradhan, J. (2018). NL-IDS: Trust-Based Intrusion Detection System for Network layer in Wireless Sensor Networks. 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). doi:10.1109/pdgc.2018.8745870
19. Gul, M. (2016). Intrusion detection for Wireless Sensor Networks using ant colony. 2016 24th Signal Processing and Communication Application Conference (SIU). doi:10.1109/siu.2016.7496024
20. A. Garofalo, C. Di Sarno, V. Formicola, "Enhancing Intrusion Detection in Wireless Sensor Networks through Decision Trees," In Vieira M., Cunha J.C. (eds) Dependable Computing. Lecture Notes in Computer Science, Vol 7869. Springer, Berlin, Heidelberg, EWDC 2013.***
21. Guo, Q., Li, X., Feng, Z., & Xu, G. (2015). MPOID: Multi-protocol Oriented Intrusion Detection Method for Wireless Sensor Networks. 2015 IEEE 17th International Conference on High-Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems. doi:10.1109/hpcc-css-icess.2015.283
22. L. Han, M. Zhou, W. Jia, Z. Dalil, and X. Xu, "Intrusion Detection Model of Wireless Sensor Networks based on Game Theory and an Autoregressive Model," Inf. Sci., Vol. 476, pp. 491–504, 2018.****
23. F. Hidoussi, H. Toral-Cruz, D. Boubiche, K. Lakhtaria, A. Mihovska, and M. Voznak, "Centralized IDS Based on Misuse Detection for Cluster-Based Wireless Sensors Networks," Wireless Personal Communications, Vol. 85, No. 1, pp. 207-224, 2015.*****
24. Hentati, A., Frigon, J.-F., & Ajib, W. (2018). Information Age and Packet Loss Performance Analysis of Energy Harvesting WSNs. 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall). https://doi.org/10.1109/vtcfall.2018.8690610
25. C. Ioannou, V. Vassiliou, and C. Sergiou, "An Intrusion Detection System for Wireless Sensor Networks," 2017 24th International Conference on Telecommunications (ICT), Limassol, pp. 1-5, 2017****
26. C. Ioannou and V. Vassiliou," An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression," In Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM '18). ACM, New York, NY, USA, pp. 259-263, 2018.***

27. Jiang, S., Zhao, J., & Xu, X. (2020). SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments. IEEE Access, 8, 169548–169558. doi:10.1109/access.2020.3024219
28. Joseph, C., Swaroop, P., & Reddy, Y. S. (2017). Prevention of packet dropping in wireless Ad Hoc networks using HLA algorithm. 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). doi:10.1109/iciiecs.2017.8275898
29. Justus, J. J., & Sekar, A. C. (2016). Energy efficient priority packet scheduling with delay and loss constraints for wireless sensor networks. 2016 International Conference on Inventive Computation Technologies (ICICT). doi:10.1109/inventive.2016.7830076
30. J. W. Ho, M. Wright, and S. K. Das, "Distributed Detection of Mobile Malicious Node Attacks in Wireless Sensor Networks," Ad Hoc Networks, Vol. 10, No. 3, pp. 512–523, 2012.*****
31. G. Kaur and M. Singh, "Detection of Blackhole in Wireless Sensor Network based on Data Mining," 2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), Noida, pp. 457-461, 2014.*****
32. Kalnoor, G., & Agarkhed, J. (2016). QoS-based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks. 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT). doi:10.1109/iccpct.2016.7530341
33. Kumar, S., Lal, N., & Chaurasiya, V. K. (2019). An energy-efficient IPv6 packet delivery scheme for industrial IoT over G.9959 protocol-based Wireless Sensor Network (WSN). Computer Networks, 154, 79–87. doi:10.1016/j.comnet.2019.03.001
34. Kurniawan, M. T., & Yazid, S. (2020). Mitigation and Detection Strategy of DoS Attack on Wireless Sensor Network Using Blocking Approach and Intrusion Detection System. 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). doi:10.1109/icecce49384.2020.9179255
35. Li, H., He, X., & Ding, S. (2019). Routing Algorithm for Reducing Packet Loss in Mobile WSN. 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA). doi:10.1109/iccnea.2019.00057

36. T. Le, T. Park, D. Cho, and H. Kim, "An Effective Classification for DoS Attacks in Wireless Sensor Networks," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, pp. 689-692, 2018.****
37. Meng, W., Li, W., Su, C., Zhou, J., & Lu, R. (2018). Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data. IEEE Access, 6, 7234–7243. doi:10.1109/access.2017.2772294
38. A. Mansouri, B. Majidi and A. Shamisa," Metaheuristic Neural Networks for Anomaly Recognition in Industrial Sensor Networks with Packet Latency And Jitter for Smart Infrastructures," International Journal of Computers and Applications, 2018.****
39. T. Ma, F. Wang, J. Cheng, Y. Yu, and X. Chen, "A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks," Sensors, Vol. 16, No. 10, p. 1701, 2016.****
40. Nannan Lu, Yanjing Sun, Hui Liu, and Song Li, "Intrusion Detection System Based on Evolving Rules for Wireless Sensor Networks," Journal of Sensors, vol. 2018, Article ID 5948146, 8 pages, 2018. *****
41. N. Nithiyanandam, P. Latha Parthiban, B. Rajalingam, "Effectively Suppress the Attack of Sinkhole in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique," International Journal of Pure and Applied Mathematics, Vol. 118, No. 9, pp. 313-329, 2018. ****
42. Nirupama A., Vijaya Bhaskar, S. C., & Jena, S. (2015). An efficient protocol to identify packet droppers and modifiers to improve QoS in Wireless Sensor Network (WSN). 2015 International Conference on Communications and Signal Processing (ICCSP). doi:10.1109/iccsp.2015.7322632
43. Nobar, S. K., Mansourkiaie, F., & Ahmed, M. H. (2020). Packet Dropping Minimization in Energy Harvesting-Based Wireless Sensor Network with Linear Topology. IEEE Access, 1–1. doi:10.1109/access.2020.2975489
44. O. Osanaiye, A.S. Alfa and G.P. Hancke," A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks," Sensors, Vol. 18, No. 6, p. 1691, 2018. ****
45. S. Otoum, B. Kantarci and H. T. Mouftah, "Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications," IEEE Sensors Letters, Vol. 1, No. 5, pp. 1-4, Oct. 2017****
46. S. Otoum, B. Kantarci and H. T. Mouftah," On the Feasibility of Deep Learning in Sensor Network Intrusion Detection," IEEE Networking Letters, 2019.***

47. Ozcelik, M. M., Irmak, E., & Ozdemir, S. (2017). A hybrid trust-based intrusion detection system for wireless sensor networks. 2017 International Symposium on Networks, Computers, and Communications (ISNCC). doi:10.1109/isncc.2017.8071998
48. H. Qu, L. Lei, X.Tang, and P. Wang, "A Lightweight Intrusion Detection Method Based on Fuzzy Clustering Algorithm for Wireless Sensor Networks," Advances in Fuzzy Systems, Vol. 2018, 12 pages, 2018.****
49. Rahmadhani, M. A., Yovita, L. V., & Mayasari, R. (2018). Energy Consumption and Packet Loss Analysis of LEACH Routing Protocol on WSN Over DTN. 2018 4th International Conference on Wireless and Telematics (ICWT). doi:10.1109/icwt.2018.8527827
50. Rani, JayaKumar, & Divya. (2015). Trust aware systems in Wireless Sensor Networks. 2015 International Conference on Computing and Communications Technologies (ICCCT). doi:10.1109/iccct2.2015.7292741
51. Raza, F., Bashir, S., Tauseef, K., & Shah, S. I. (2015). Optimizing nodes proportion for intrusion detection in uniform and Gaussian distributed heterogeneous WSN. 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST). doi:10.1109/ibcast.2015.7058571
52. Reddy, V. B., Negi, A., & Venkataraman, S. (2018). Trust Computation Model Using Hysteresis Curve for Wireless Sensor Networks. 2018 IEEE SENSORS. doi:10.1109/icsens.2018.8589697