American Journal of Electrical and Computer Engineering
2022; 6(1): 24-29
http://www.sciencepublishinggroup.com/j/ajece
doi: 10.11648/j.ajece.20220601.13
ISSN: 2640-0480 (Print); ISSN: 2640-0502 (Online)

An Efficient Intrusion Detection Approach for Wireless Sensor Networks

Fuad Abu Owaimer[1], Ayman Tanira[1], Mohammed Abu Hatab[2], Mohammad Mikki[3]

[1]Computer Department, Palestine Technical College, Deir ElBalah, Palestine

[2]Engineering Department, Palestine Technical College, Deir ElBalah, Palestine

[3]Computer Engineering Department, Islamic University, Gaza, Palestine

Email address:

fowaimer@ptcdb.edu.ps (F. A. Owaimer), atanira@ptcdb.edu.ps (A. Tanira), mabuhatab@ptcdb.edu.ps (M. A. Hatab), mmikki@iugaza.edu.ps (M. Mikki)

To cite this article:

Fuad Abu Owaimer, Ayman Tanira, Mohammed Abu Hatab, Mohammad Mikki. An Efficient Intrusion Detection Approach for Wireless Sensor Networks. *American Journal of Electrical and Computer Engineering*. Vol. 6, No. 1, 2022, pp. 24-29.
doi: 10.11648/j.ajece.20220601.13

Received: March 26, 2022; **Accepted**: April 16, 2022; **Published**: May 10, 2022

Abstract: Wireless Sensor Networks (WSNs) are vulnerable to various kinds of security attacks that can compromise many nodes and therefore the performance of the network may be degraded. Failures to prevent intrusions could also decrease the credibility of security services, e.g., data confidentiality, integrity, and availability. Traditional Intrusion Detection Systems (IDS) suffer from many issues in performance and increased overhead which are considered the main challenge in WSNs. The common architecture of WSN is that nodes are organized into a set of clusters; each one contains a set of nodes with a specialized node called Cluster Head (CH) node which is responsible for managing activities through the cluster and communicating with other nodes and a Base Station (BS). The CH plays a critical role in the case attacking WSN in the two cases; signature-based and anomaly-based. This paper proposes an efficient hybrid IDS to analyze and secure WSN in multiple phases because it combines the best features of two different approaches to achieve better performance. In the proposed approach, BS evaluates and updates attacks information for the entire network which is the main advantage where BS doesn't suffer from any limitations in sensor nodes. Moreover, BS selects CH among other nodes based on power capabilities and computational resources. The efficiency and adaptability of the proposed method have been tested by simulation experiments deployed on JiST/Swans simulation. The experimental results show that the proposed system is efficient with acceptable performance in comparison with other hybrid IDSs. The experimental evaluation also expresses that the proposed technique reduces the communication costs on the cluster head (CH) which improves the lifetime of the entire WSN.

Keywords: Intrusion Detection System (IDS), Wireless Sensor Networks (WSN), Cluster Head (CH), Base Station (BS)

1. Introduction

Wireless sensor networks (WSNs) consist of a large number of small sensor devices with sensing, computational and communication capabilities. Sensor nodes are infrastructure-less; distributed and dynamic nature, monitoring some physical phenomena in their environment, recording values from surrounding environment, and sending them using wireless transmission toward network sink such as a BS. WSNs become increasingly popular in many environmental, business, engineering, healthcare, military, surveillance, and other applications [1, 3]. While the natural properties of sensor nodes are considered limited, serious security issues make them vulnerable to many security threats. To secure a WSN from different threats, it requires many authentications and management tasks.

Limited sensor nodes capacities such as energy, memory, bandwidth, and other computational resources make WSNs security is main challenge. Consequently, progress in WSN research has yielded many major advances against threats. Particularly, IDS still the most effective mechanism to detect and analyze suspicious activities that occur in WSNs [2, 9]. An IDS automates the detection of intrusion activities that can compromise the confidentiality, availability, and integrity of WSN through bypassing the security mechanisms [15, 18].

IDS agent performs an important task for securing network from intrusive attacks. Researchers use three different ways of installing IDS agent in WSNs. These are purely distributed, purely centralized, and distributed-centralized [8, 17].

1.1. Purely Distributed Approaches

Each wireless sensor node has its main components like memory unit, sensing unit, communication unit, and processing unit. In this approach, each sensor node gets its own IDS agent to analyze all data that is sensed from the surrounding environment using its own sensing capabilities. It also processes and communicates these data directly with the BS using hop-by-hop techniques. Purely distributed IDS techniques are not energy-efficient because IDS agent is installed in every node. It increases computation or power consumption at node level. [8, 10, 19].

1.2. Purely Centralized Approaches

In these techniques BS or sink take the responsibility to collect, evaluate and analyze some specific information gathered from sensor nodes. They use routing protocol to detect intrusions, then the BS analyzes the gathered information and determines if there is an intruder node or not. Finally, BS sends back the intrusion analysis report to each sensor node. Purely centralized IDS approaches are power-efficient because BS or sink takes the responsibility of intrusion detection process which saves the power consumption in other nodes. On the other hand, these techniques are complex and require some specialized routing protocols that collect data from each sensor node to BS or sink for anomaly detection [8, 10].

1.3. Distributed-Centralized Approaches

These approaches are also called hybrid approaches, since they combine characteristics of both distributed and centralized techniques. In particular, intrusion detection agent is installed mainly on selected monitor node called CH. CH is selected carefully based on both power resources and good computational resources. This node monitors activities and collects all information in its range and send the misbehavior activities to the BS to take its decision about malicious activity and backs it to sensor node through CH node. Distributed-centralized IDS approach suits WSNs in accordance with energy consumption and complexity, but it has its own constraints. WSNs are vulnerable to a number of inside attacks that affect the overall performance of the network. These attacks result in wrong interpretation of the sensed information. There is a requirement of an energy-efficient IDS that works in distributed manner and cooperates with other nodes to identify the abnormal behavior of the nodes in a WSN [16]. Figure 1 shows a WSN that consists of a set of sensor nodes that arranged to groups where each cluster managed by a specific node called CH which is responsible to connect nodes to BS.

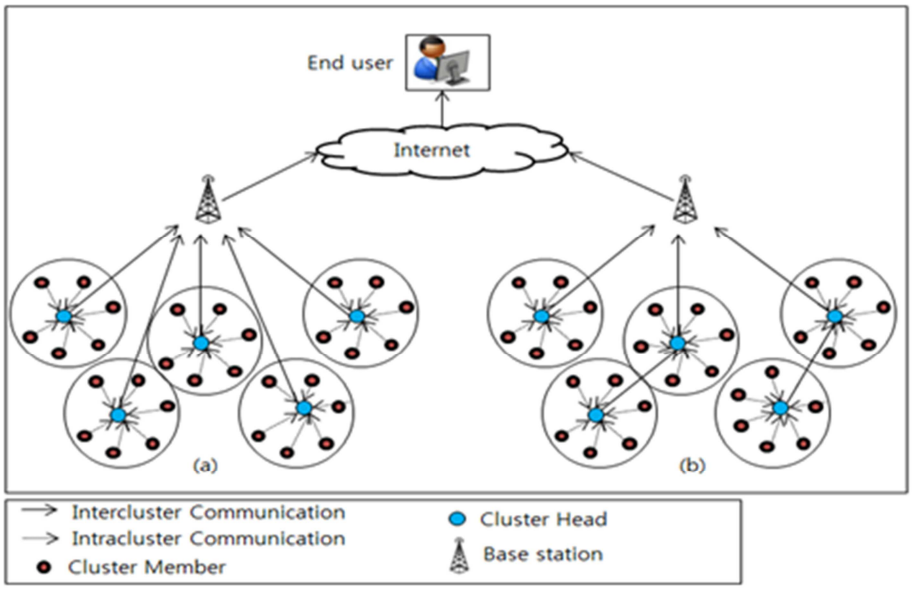

Figure 1. *Wireless sensor network.*

This paper has the following main contributions:

1. IDS is formulated into an adequate framework.
2. An efficient hybrid IDS is introduced which reduces the workload and overhead on CH by forwarding the anomaly detection threats to BS; making more stability to WSN with an acceptable level of security.
3. Finally, the paper conducts a series of experiments by using simulated environment, and the results demonstrate the advantage of the proposed method.

The rest of this paper is organized as follows: section II presents a review of the related work in the literature. Section III describes statement of the problem. Section IV focuses on a proposed method for solving the problem. Section V presents the results of the experimental evaluation. Finally, conclusion is given in Section VI.

2. Related Work

In this section, a simple survey for IDS for WSNs is presented. The authors in [5] propose a hierarchical IDS based on cluster design and install on each cluster-head an IDS agent to detect anomaly intrusion based on the rules and decision-making module. Simulation results show that this model has a high detection rate and lower false positive rate. But, the main disadvantage of this scheme is CH because the mechanism requires many calculations and intruder can attack this node.

The researchers in [6] introduce a Lightweight Intrusion Detection based on cluster-based architecture which divides the sensor network into groups of clusters, and elects a node to become a CH. In this architecture, every node belongs to only one of the clusters. CH is used to reduce energy consumption and amount of data in the entire network. It is used to increase network lifetime by collecting the information gathered from sensor node and to process it without the need for every node to communicate directly with BS. The disadvantage of this scheme is the same issue; CH because the method allows an intruder to focus attack on CH.

A Hybrid Intrusion Detection System for WSNs is investigated in [4] by using anomaly detection based on SVM technique and a set of predefined fixed signature attacks' rules, which are designed to validate the malicious behavior of a target identified by anomaly detection technique. The proposed techniques based on CH which works to forward the collected sensor node data to the BS instead of sending directly to BS by every node. The disadvantage of this model is that all intrusion detection decisions are done in the BS and CH. There is an overhead in the CH to forward all packets from the sensor node to the BS and back which consumes a lot of resources.

The proposed Hybrid Intrusion Detection System based on anomaly and misuse detection techniques in a cluster wireless sensor topology is discussed in [11]. The scheme allows a high detection rate with low level of energy consumption. However, this scheme is unable to detect most network attacks.

The authors in [12] implement a lightweight Framework for securing wireless sensor networks by combining the advantages of both cryptography and IDS technology to detect the most dangerous network attacks. The scheme performs well in terms of detection rate, but introduces high overhead and energy consumption.

3. Statement of Problem

Given a WSN that consists of a main Base Station BS and connects a set of clusters C= $\{c_1, c_2,.., c_n\}$. Each one consists of a set of nodes N_i= $\{n_{i1}, n_{i2},.., n_{im}\}$ where i is a specific cluster in the network. Every cluster has a Cluster Head CH_i, which is responsible of all traffic in his cluster and communicates with the BS. Each node n_{ij} communicates with other nodes and CH_i of the cluster that it belongs to and stores an updated blacklist of the compromised nodes. Intuitively, each CH_i communicates with BS in the situation of detecting a new anomaly. In the case that node nij is compromised of some attack it directly sends to the CHi which tries to defense the attack. Consequently, there are two cases. First case, CH copes with attack that means it is found in the signature-based blacklist of CH. Second case, it cannot deal with the attack so it sends all details to the BS. In this case the BS becomes responsible to overcome the attack and broadcast attack's information to the whole entire network for future concerns.

Choosing the CH depends on both power resources and available computational resources. A CH is responsible of security for all cluster nodes by collecting the data and sending it to the BS which analyzes the security features and sends it back to CH which update the security plane to each node in his cluster based on that information. CH plays critical rules for many reasons; first the computational needs will consume a lot of power to send request and replay it back to all nodes, second intruder may intend to attack this node which leads to fall down, and finally the node may stop working for any other sudden reasons. Due to the critical role of the CH as mentioned above, and the availability needed to the network, the BS is responsible to select alternative node as new CH. The goal is providing a mechanism that assures the availability of the network against any malicious behavior, particularly intruders.

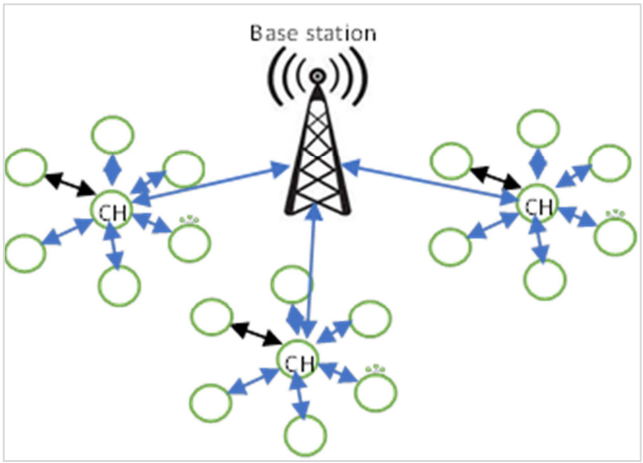

Figure 2. *Wireless sensor network (WSN) Structure.*

The natural properties of sensor nodes make choosing of a certain IDS technique is very difficult; some authors choose a complete centralized model for sensor network which is not the best choice [16], others use hybrid model which is more suitable for the characteristic of WSN as discussed earlier in this paper. Again, CH is responsible for security of cluster nodes by collecting the data and sending it to the BS which analyzes the security features and sends it back to CH which update the security plan to each node in his cluster.

4. Proposed Method

This paper proposes an efficient intrusion detection

approach for WSN that provides more stability to WSN and reduces the communication overhead on CH node. BS takes the responsibility of evaluating and updating attacks information for the entire WSN which is a main advantage where BS doesn't suffer from limitations in sensor nodes. BS is responsible of selecting CH which is chosen based on power and computational resources of that node. The mechanisms of IDS implemented in our work is a hybrid intrusion detection system paradigm because it combines the best features of two different approaches to achieve better performance. The system relies on both signature-based model and anomaly-based model.

The overall process is explained in the following steps:

Step 1: BS is responsible to manage IDS and group sensor nodes in clusters by choosing CH for each cluster based on power and computational resources.

Step 2: Sensor nodes are installed in the environment then grouped based on location and sensing range by BS.

Step 3: Each sensor node has its IDS analyzing agent to monitor information traffic and sends the suspicions to the CH which works as a local BS.

Step 4: CH monitors local member nodes' activities and any data transmitted through them.

Step 5: CH has a local agent that is responsible to make a decision to all request received and decides whether it is normal or malicious using his signature-based IDS technique.

Step 6: Any unknown event that CH can't manage is reported to BS.

Step 7: BS analyzes the data to determine the suspiciousness of events.

Step 8: BS alerts the CHs about the pattern of threat events. Then CHs take action upon such alerts by updating their signature base.

Step 9: BS copes suspicious node and updates blacklist nodes and broadcasts the new information to all CHs and nodes in the whole WSN.

Figure 2 shows a network structure design that consists of sensor nodes grouped into clusters. A master node is selected as CH based on power and computational resources by BS. It is clear from the figure that a communication process in the WSN. If any node has a security suspicion event it communicates with CH directly then CH communicates with BS according to the threat.

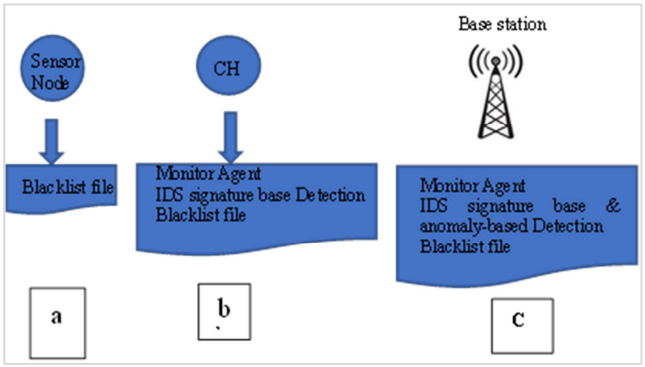

Figure 3. *IDS Architecture Model.*

Figure 3 shows the architecture of the model used in our project. Figure 3(a) shows that each sensor node has its own blacklist file of all malicious nodes updated by CH or BS. Figure 3(b) shows that CH has a monitor agent to detect any malicious activity, IDS signature base detection engine mode and blacklist file. Figure 3(c) shows that BS contains the main parts of IDS of both signature and anomaly-based detection engine.

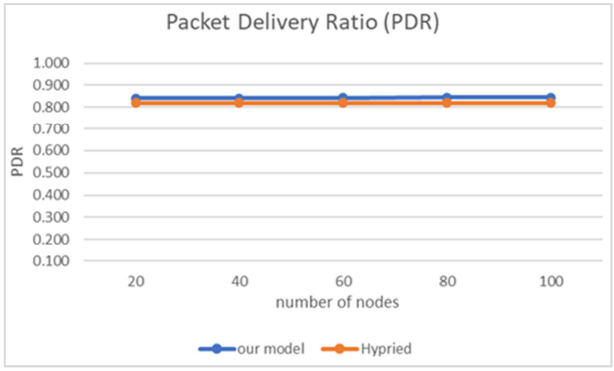

Figure 4. *Work load on CH in proposed model vs hybrid model.*

The main advantage of our approach reduces the workload and overhead on CH node by forwarding the anomaly detection threats to BS intrusion detection engine also the BS will alert all nodes and CH of the suspicion nodes or alerts in network which reduce numbers of packets and process needed by CH making more stability to wireless sensor network and keep security level the same with other models.

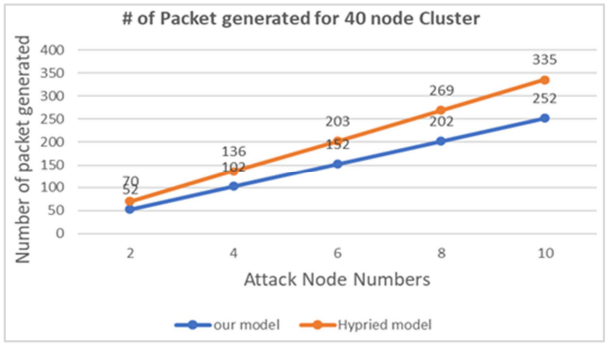

Figure 5. *Number of Packets generated in CH for 40 nodes Cluster under attack.*

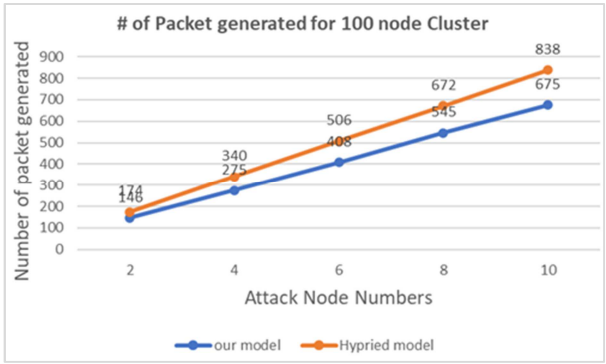

Figure 6. *Number of Packet generated in CH for 100 node Cluster under attack.*

5. Experimental Evaluation

The empirical work has been simulated in JiST/Swans simulation under windows operating system. JiST/Swans is a new Java-based discrete-event simulation engine with a number of novel and unique design features and is specific for both Ad hoc Networks and WSN [13, 14].

The simulation is done by comparing both the proposed model described previously with default hybrid IDS system (every sensor node sends a suspicion request to CH then the CH forwards the traffic to BS and replies the results to inform member nodes if there is an attack event.). In our experiments, the simulated WSN is organized as shown in Table 1.

A WSN of different sizes is implemented including the following number of nodes: 20, 40, 60, 80 and 100, with CH in each cluster and a single BS for the whole network. Firstly, the Packet Delivery Ratio (PDR) of the proposed model is compared with a hybrid model in free attack mode where there isn't any attack case. Figure 4 shows that the proposed model is the same with hybrid model for PDR in this case.

Table 1. *Simulation parameters.*

Parameters	Value
Number of nodes	100
Number of clusters	2
Number of node per cluster	40-50
Protocols	Adhoc/WSN
Field (area)	100*100m
Antenna type	Omni
Number of BS	1

Secondly, attack nodes are created by generating ICMP ping as DoS attack which classified as signature-based attack to specific sensor nodes in the network and create different behavioral attack to be classified as anomaly-based attack then measure those effects on both models. The percentage of signature-based attacks is 80% of all attacks happened and 20% is anomaly-based attacks.

The proposed model performance is evaluated by changing the number of both nodes in each cluster and the number of attack nodes respectively then the system measures the packet related to security suspicion sent by compromised nodes to CH to report it.

Table 2 summarizes all cases investigated for this experiment. The proposed model is investigated in different scenarios of WSN according to different number of nodes which varies from 20 sensor nodes in each cluster to 100 sensor nodes. Moreover, the number of attack nodes is set to vary from 2 to 10 nodes. All packet generated for security related is shown in Table 2. For example, in the case of 40 node cluster, It is clearly, that the number of packets generated by CH in the proposed model is less that the hybrid model and the difference of packets increases with respect to the number of anomaly attack. It is obvious from Table 2 that the proposed model is less than the hybrid one which means that the overhead is transferred from CH to BS.

Figure 5 and Figure show the differences of the number of packets generated by the proposed model and hybrid model for scenario of 40 and 100 sensor nodes member in the cluster. The results show that number of packets generated in CH in the proposed model is less than the number of packets of the hybrid model which means the performance of the proposed model increases. It is also clearly from figures that the overhead of the number of packets sent by CH increases as the number of nodes increases in the case of existing of attack nodes but it is obvious that the proposed model is better than the hybrid model even when WSN contains a large number of nodes which means a better performance is achieved.

Table 2. *Number of Packets Generated in CH.*

Attack Nodes Number	Number of packets generated in CH									
	20 Nodes Cluster		40 Nodes Cluster		60 Nodes Cluster		80 Nodes Cluster		100 Nodes Cluster	
	proposed model	hybrid model	proposed model	hybrid model	proposed model	hybrid model	proposed model	hybrid model	proposed model	hybrid model
2	35	35	52	70	87	105	112	139	146	174
4	52	70	102	136	170	204	210	272	275	340
6	87	105	152	203	253	304	310	405	408	506
8	105	139	202	269	336	403	408	538	545	672
10	139	174	252	335	419	503	509	671	675	838

Finally, Let's discuss the power consumption comparison between the proposed model and hybrid model [7]. Firstly, let's define the power consumption equation for CH node by:

$$CH_{Power\_Consumption} = P_{tr} + P_{rec} + P_{idle} + P_{pro} \quad (1)$$

where,

P_{tr}: Packet Transmision Power Consumption

P_{rec}: Packet Received Power Consumption

P_{idle}: Idle time power Consumption

P_{pro}: Processing Time Power Consumption

Let's assume that the processing time and idle time is equals in both the proposed and hybrid model and its clears that the number of packets send and received by our model by CH is less than the hybrid model as previous discussion in the proposed model so,

$$(P_{tr} + P_{rec})_{Proposed\_Model} < (P_{tr} + P_{rec})_{Hybrid_{model}} \quad (2)$$

which leads to that the power performance of the proposed model is better than the hybrid model which can be defined by the following equation:

$$CH_{saved\_power} = CH_{current\_power} - CH_{consumed_{power}} \quad (3)$$

So mathematically the conclusion is that the power consumed by CH node in the proposed model is less than the power consumed by the hybrid model and the overall overhead is transferred to BS which improve the stability of the WSN and insure long lifetime for the entire WSN.

6. Conclusion

Wireless sensor networks (WSNs) consist of a large number of small sensor devices special capabilities. Sensor nodes are infrastructure-less; distributed and dynamic nature, that are used to monitor the surrounding environment. Recently, the spread of WSN increases more and more in many areas such as industry, IoT, health, surveillance and other fields. This spread requires more attention to secure WSN from numerous threats.

The paper surveyed the current approach of Intrusion Detection Systems and discuss the characteristics of the three main approaches in the literature; purely centralized, purely distributed and hybrid approaches.

This paper introduced an efficient intrusion detection approach for wireless sensor networks, based on modified hybrid Intrusion Detection System (IDS) with both anomaly-based and signature-based detection. The proposed approach is presented in details. The experimental evaluation expresses that the proposed technique reduces the communication costs on cluster head (CH) which improves the lifetime of the entire WSN.

As a future work, a lot of research issues can be considered with Intrusion Detection System (IDS) based on machine learning approaches and Reinforcement Learning techniques to improve both the accuracy of detection engine with low overhead.

References

[1] Akyildiz, W., Sankarasubramaniam, Y., & Cayirci., E. (2002) A survey on sensor networks. In IEEE Communication Magazine, vol. 40 (8). doi: 10.1109/MCOM.2002.1024422.

[2] Khudadad, M., & Huang, Z. (2018). Novel intrusion detection methods for security of wireless sensor network. Journal of Fundamental and Applied Sciences, 10 (2S), 173-189. ISSN: 1112-9867.

[3] Mishra, A., & Srivastava, A. K. (2013). A Survey on Intrusion Detection System for Wireless Network. International Journal of Computer Applications, 73 (21), 37-40. doi: 10.5120/13021-0221.

[4] Maleh, Y., Ezzati, A., Qasmaoui, Y., & Mbida, M. (2015). A global hybrid intrusion detection system for wireless sensor networks. Procedia Computer Science, 52, 1047-1052. https://doi.org/10.1016/j.procs.2015.05.108.

[5] Yan, K. Q., Wang, S. C., Wang, S. S., & Liu, C. W. (2010, July). Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network. In 2010 3rd international conference on computer science and Information Technology, China, pp. 114-118. doi: 10.1109/ICCSIT.2010.5563886.

[6] MALEH, Y., & Ezzati, A. (2015). Lightweight Intrusion Detection Scheme for Wireless Sensor Networks. IAENG International Journal of Computer Science, 42 (4).

[7] Sutaria, T., Mahgoub, I., Humos, A., & Badi, A. (2007, April). Implementation of an energy model for JiST/SWANS wireless network simulator. In Sixth International Conference on Networking (ICN'07) (pp. 24-24). IEEE. https://doi.org/10.1109/ICN.2007.47

[8] Farooqi, A., & Khan, F., (2009). Intrusion Detection Systems for Wireless Sensor Networks: A Survey. Conference Paper in International Journal of Ad Hoc and Ubiquitous Computing. DOI: 10.1504/IJAHUC.2012.045549.

[9] Butun, I., Morgera, S. D., & Sankar, R. (2013). A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16 (1), 266-282. doi: 10.1109/SURV.2013.050113.00191.

[10] Farooqi, A. H., & Khan, F. A. (2012). A survey of intrusion detection systems for wireless sensor networks. International Journal of Ad Hoc and Ubiquitous Computing, 9 (2), 69-83.

[11] Abduvaliyev, A., Lee, S., & Lee, Y. K. (2010, August). Energy efficient hybrid intrusion detection system for wireless sensor networks. In 2010 International Conference on Electronics and Information Engineering (Vol. 2, pp. V2-25). IEEE. doi: 10.1109/ICEIE.2010.5559708.

[12] Sedjelmaci, H., & Senouci, S. M. (2014, June). A lightweight hybrid security framework for wireless sensor networks. In 2014 IEEE international conference on communications (ICC) (pp. 3636-3641). IEEE. doi: 10.1109/ICC.2014.6883886.

[13] Barr, R., Haas, Z., & Renesse, R. (2004, March). Scalable Wireless Ad Hoc Network Simulation.

[14] Barr, R. (2004, March). JiST–Java in Simulation Time "http://JiST.ece.cornell.edu/".

[15] Singh, G., & Khare, N. (2021). A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques. International Journal of Computers and Applications, 1-11. doi: 10.1080/1206212X.2021.1885150.

[16] Ozcelik, M. M., Irmak, E., & Ozdemir, S. (2017, May). A hybrid trust based intrusion detection system for wireless sensor networks. In 2017 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE. doi: 10.1109/ISNCC.2017.8071998.

[17] Abbood, Z. A., Atilla, D. Ç., Aydin, Ç., & Mahmoud, M. S. (2021, December). A Survey on Intrusion Detection System in Ad Hoc Networks Based on Machine Learning 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI), 2021, pp. 1-8, doi: 10.1109/MTICTI53925.2021.9664776.

[18] Elbahadır, H., & Erdem, E., (2021). Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks. In 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021, pp. 401-406, doi: 10.1109/UBMK52708.2021.9558928.

[19] Amaran, S., & Mohan, R., (2021). Intrusion Detection System using Optimal Support Vector Machine for Wireless Sensor Networks. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), pp. 1100-1104, doi: 10.1109/ICAIS50930.2021.9395919.